Juniper Networks | Engineering Simplicity

SRX5800 Firewall Hardware Guide

Published
2024-09-16

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

SRX5800 Firewall Hardware Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to install hardware and perform initial software configuration, routine maintenance, and troubleshooting for the SRX5800 Firewall.

After completing the installation and basic configuration procedures covered in this guide, refer to the Junos OS documentation for information about further software configuration.

RELATED DOCUMENTATION

- Getting Started Guide for the SRX5800 Firewall
- SRX5400, SRX5600 and SRX5800 Firewall Card Reference
- Safety Guide
- Transceivers Supported on SRX5800 Firewalls

CHAPTER 1

Overview

SRX5800 Firewall System Overview

IN THIS SECTION

SRX5800 Firewall Description

The SRX5800 Firewall is a high-performance, highly scalable, carrier-class security device with multi-processor architecture.

The firewall provides 12 slots that you can populate with 2 or 3 Switch Control Boards (SCBs) and up to 12 additional cards of the following types:

- Services Processing Cards (SPCs) provide the processing capacity to run integrated services such as firewall, IPsec, and IDP.
- Modular PIC Concentrators (MPCs) provide Ethernet interfaces that connect the firewall to your network.
- I/O cards (IOCs) provide Ethernet interfaces that connect the firewall to your network.
- Flex IOCs are similar to IOCs, but have slots for port modules that allow you greater flexibility in adding different types of Ethernet ports to your firewall.

For detailed information about the cards supported by the firewall, see the *SRX5400, SRX5600, and SRX5800 Firewall Card Reference* at www.juniper.net/documentation/.

Benefits of the SRX5800 Firewall

- The SRX5800 Firewall is the market-leading security solution supporting up to 1.2 Tbps firewall throughput and latency as low as 32 microseconds for stateful firewall, 395 million concurrent sessions, and 1 Tbps IPS.

Equipped with the full range of advanced security services, massive performance, scalability, and flexibility make the SRX5800 ideal for securing large enterprise, hosted, or colocated data centers, mobile operator environments, densely consolidated processing environments, cloud and managed service providers.

- IPS Capabilities - Juniper Networks IPS capabilities offer several unique features such as Protocol decodes, Zero-day protection, Active/active traffic monitoring, and packet capture logging per rule assure the highest level of network security.
- Content Security Content Security Capabilities - The Content Security services offered on the SRX5000 line of Firewalls include industry-leading antivirus, antispam, content filtering, and additional content security services.

  The Content Security services provide sophisticated protection from:

  - Antivirus experts against malware attacks that can lead to data breaches and lost productivity.
  - Advanced persistent threats perpetrated through social networking attacks and the latest phishing scams with sophisticated e-mail filtering and content blockers.
  - Lost productivity and the impact of malicious URLs and extraneous or malicious content on the network to help maintain bandwidth.
- Advanced Threat Prevention (ATP) - Juniper ATP Cloud, a SaaS-based service, and the Juniper ATP Appliance, an on-premises solution:
  - Protects enterprise users from a spectrum of advanced malware that exploits “zero-day” vulnerabilities.
  - Proactively blocks malware communication channels.
  - The Juniper ATP Appliance includes support for cloud-based e-mail services such as Office 365 and Google Mail, and detects threats in SMB traffic.
  - Single pane-of-glass management with Security Director and JSA Series integration.

SRX5800 Firewall Field-Replaceable Units

Field-replaceable units (FRUs) are firewall components that can be replaced at the customer site. The firewall uses the following types of FRUs:

Table 1 on page 4 lists the FRUs of the firewall and the action to perform to install, remove, or replace an FRU.

Table 1: Field-Replaceable Units

Field-Replaceable Units (FRUs)	Action
Air filter	You need not power off the firewall to install, remove, or replace any of these FRUs.
Fan tray	
Craft interface	
AC and DC power supplies (if redundant)	
SFP and XFP transceivers	
IOCs	Power off the firewall to install, remove, or replace any of these FRUs.
Flex IOCs	
Port modules of the Flex IOCs	
Routing Engine	
SCBs	
SPCs	
MPCs	
MICs	

SRX5800 Firewall Component Redundancy

The following major hardware components are redundant:

- Switch Control Boards (SCBs)—The SRX5800 Firewall has two SCBs installed and you can install a third SCB for switch fabric redundancy. The SCB of the host subsystem functions as the primary and the others function as backup. If the SCB of the host subsystem fails, one of the other SCBs takes over as the primary.

  NOTE: The SRX5800 Firewall supports a redundant SCB, provided the SCB is a SRX5K-SCBE (SCB2) running Junos OS Release 12.1X47-D15 and later, or a SRX5K-SCB3 (SCB3) running Junos OS Release 15.1X49-D10 and later.
  The SRX5800 Firewall does not support a redundant SCB (third SCB) card if SRX5K-SPC-4-15-320 (SPC2) is installed with SCB1 (SRX5K-SCB). If you have installed a SPC2 on a SRX5800 Firewall with a redundant SCB1 card, make sure to remove the redundant SCB1 card.

- Power supplies—When powered by standard-capacity AC power supplies, a minimum of three power supplies are required to supply power to a fully configured firewall. All AC power supplies share the load evenly. The addition of a fourth power supply provides full power redundancy. If one power supply fails in a redundant configuration, the three remaining power supplies provide full power.

  When powered by DC power supplies or high-capacity AC power supplies, two power supplies are required to supply power to a fully configured firewall. One power supply supports approximately half of the components in the firewall, and the other power supply supports the remaining components. The installation of two additional power supplies provides full power redundancy. If one or two power supplies fail, the remaining power supplies can provide full power to the firewall.

- Cooling system—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 firewall indefinitely.

SRX5800 Chassis

IN THIS SECTION

SRX5800 Firewall Chassis

The firewall chassis is a rigid sheet metal structure that houses all the other firewall components (see Figure 1 on page 7, Figure 2 on page 8, and Figure 3 on page 9). The chassis measures 27.75 in. (70.49 cm) high, 17.37 in. (44.11 cm) wide, and 23.0 in. (58.42 cm) deep (from the front-mounting flanges to the rear of the chassis). The chassis installs in 19-in. equipment racks or telco open-frame racks.

The chassis can be installed in standard 800-mm (or deeper) enclosed cabinets when powered by standard-capacity power supplies, or in 1000-mm (or deeper) enclosed cabinets when powered by high-capacity power supplies.

Up to three firewalls can be installed in one standard (48 U) rack if the rack can handle their combined weight, which can be greater than 1,134 lb (515 kg). See "SRX5800 Firewall Physical Specifications" on page 9 for physical specifications for the SRX5800 Firewall.

Mounting hardware includes front-mounting flanges on the front of the chassis, and two center-mounting brackets attached to the center of the chassis.

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power. See "Grounding the SRX5800 Firewall" on page 252 for instructions.

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

Figure 1: Front View of a Fully Configured Firewall Chassis

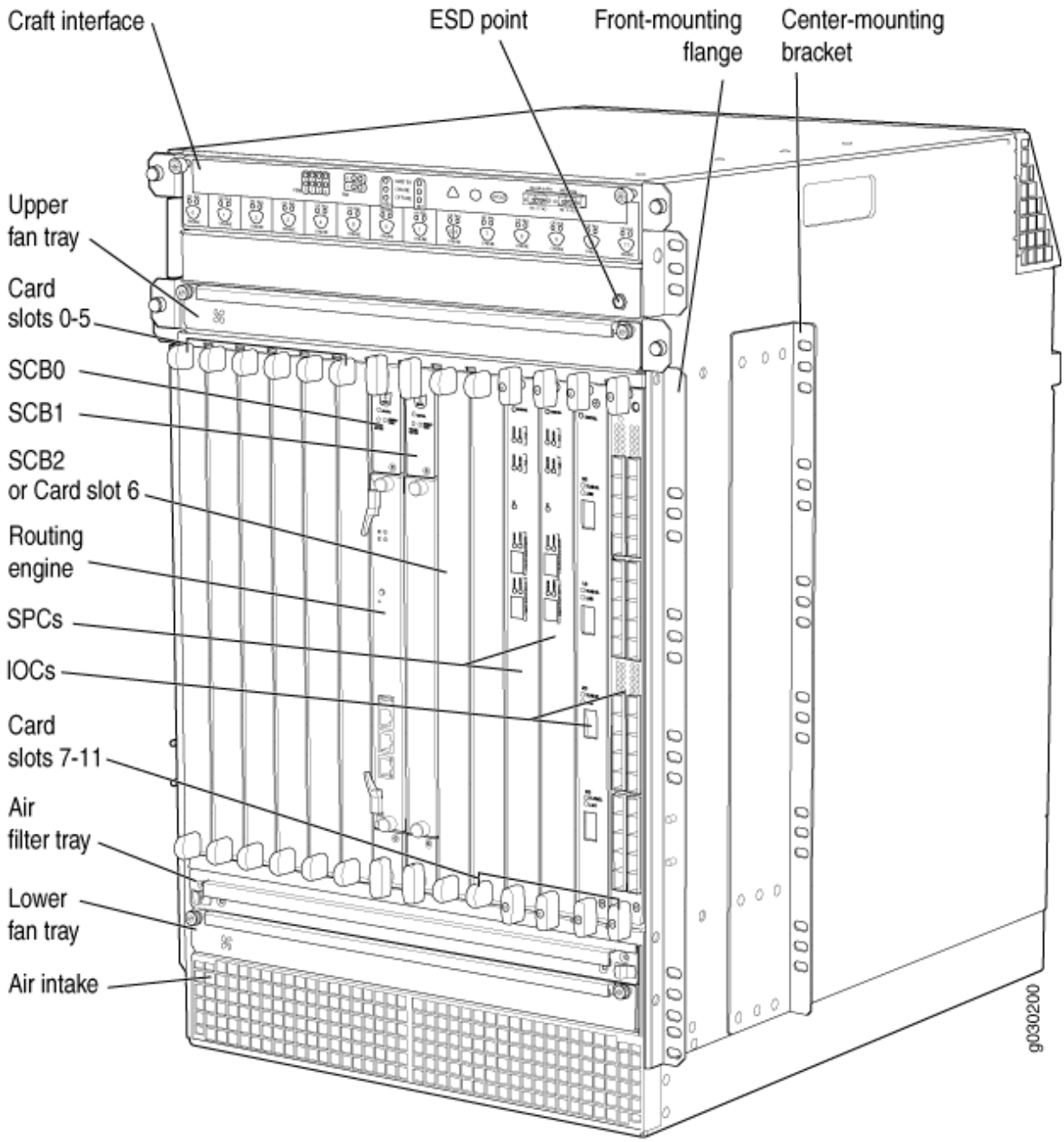


Figure 2: Rear View of a Fully Configured AC-Powered Firewall Chassis

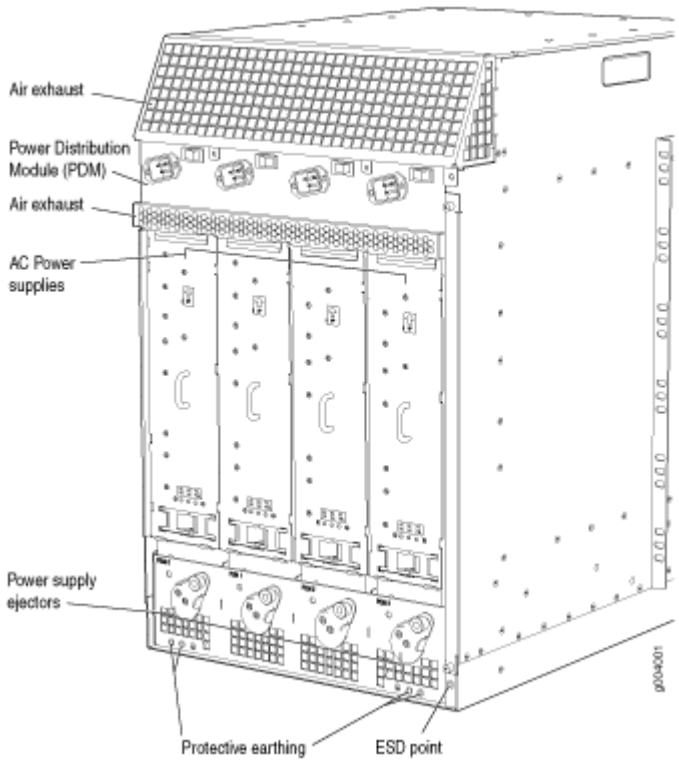
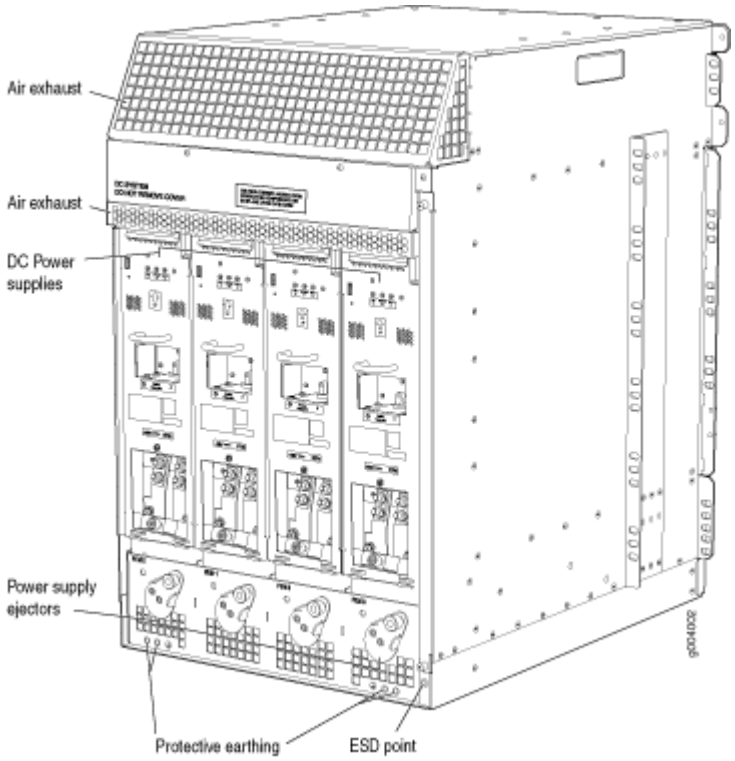


Figure 3: Rear View of a Fully Configured DC-Powered Firewall Chassis



SRX5800 Firewall Physical Specifications

Table 2 on page 9 summarizes the physical specifications for the firewall chassis.

Table 2: Physical Specifications

Description		Value
Chassis dimensions	Height	27.75 in. (70.5 cm) high
	Width	17.37 in. (44.1 cm) wide

Table 2: Physical Specifications *(Continued)*

Description		Value
	Depth, with standard-capacity power supplies	23.0 in. (58.4 cm) deep from front-mounting bracket to chassis rear 27.8 in. (70.6 cm) total depth including cable management system
	Depth, with high-capacity AC power supplies	25.5 in. (64.8 cm) deep from front-mounting bracket to chassis rear 30.3 in. (77.0 cm) total depth including cable management system
	Depth, with high-capacity DC power supplies	27.8 in. (70.6 cm) deep from front-mounting bracket to chassis rear 32.6 in. (82.8 cm) total depth including cable management system
Firewall weight		Chassis with midplane, fan tray, air filter, and cable manager: 150 lb (60.4 kg) Maximum configuration: 400 lb (182 kg)
Routing Engine weight		SRX5K-RE-13-20: 2.4 lb (1.1 kg) SRX5K-RE-1800X4: 2.4 lb (1.1 kg)
SCB weight		SRX5K-SCB: 9.6 lb (4.4 kg) SRX5K-SCBE: 9.6 lb (4.4 kg) SRK5K-SCB3: 10.14 lb (4.6 kg)
MPC weight (with two MICs)		13.1 lb (5.9 kg)
IOC weight		13.1 lb (5.9 kg)
Craft interface weight		1.1 lb (0.5 kg)

Table 2: Physical Specifications *(Continued)*

Description	Value
Fan tray weight	4.2 lb (1.9 kg)
Air filter weight	1.0 lb (0.5 kg)
Cable management weight	0.3 lb (0.14 kg)
Standard-capacity DC power supply weight (only supported on devices with SRX5K-SCB and SRX5K-RE-13-20)	3.8 lb (1.7 kg)
High-capacity DC power supply weight	12.0 lb (5.5 kg)
Standard-capacity AC power supply weight (only supported on devices with SRX5K-SCB and SRX5K-RE-13-20)	5.0 lb (2.3 kg)
High-capacity AC power supply weight	12.0 lb (5.5 kg)

NOTE: For the weights of specific cards, Routing Engines, or port modules, see the *SRX5400, SRX5600, and SRX5800 Firewall Card Guide* at www.juniper.net/documentation/.

SRX5800 Firewall Midplane Description

The midplane is located toward the rear of the chassis and forms the rear of the card cage (see Figure 4 on page 13). IOCs, SPCs, and SCBs install into the midplane from the front of the chassis, and the power supplies install into the midplane from the rear of the chassis. The cooling system components also connect to the midplane.

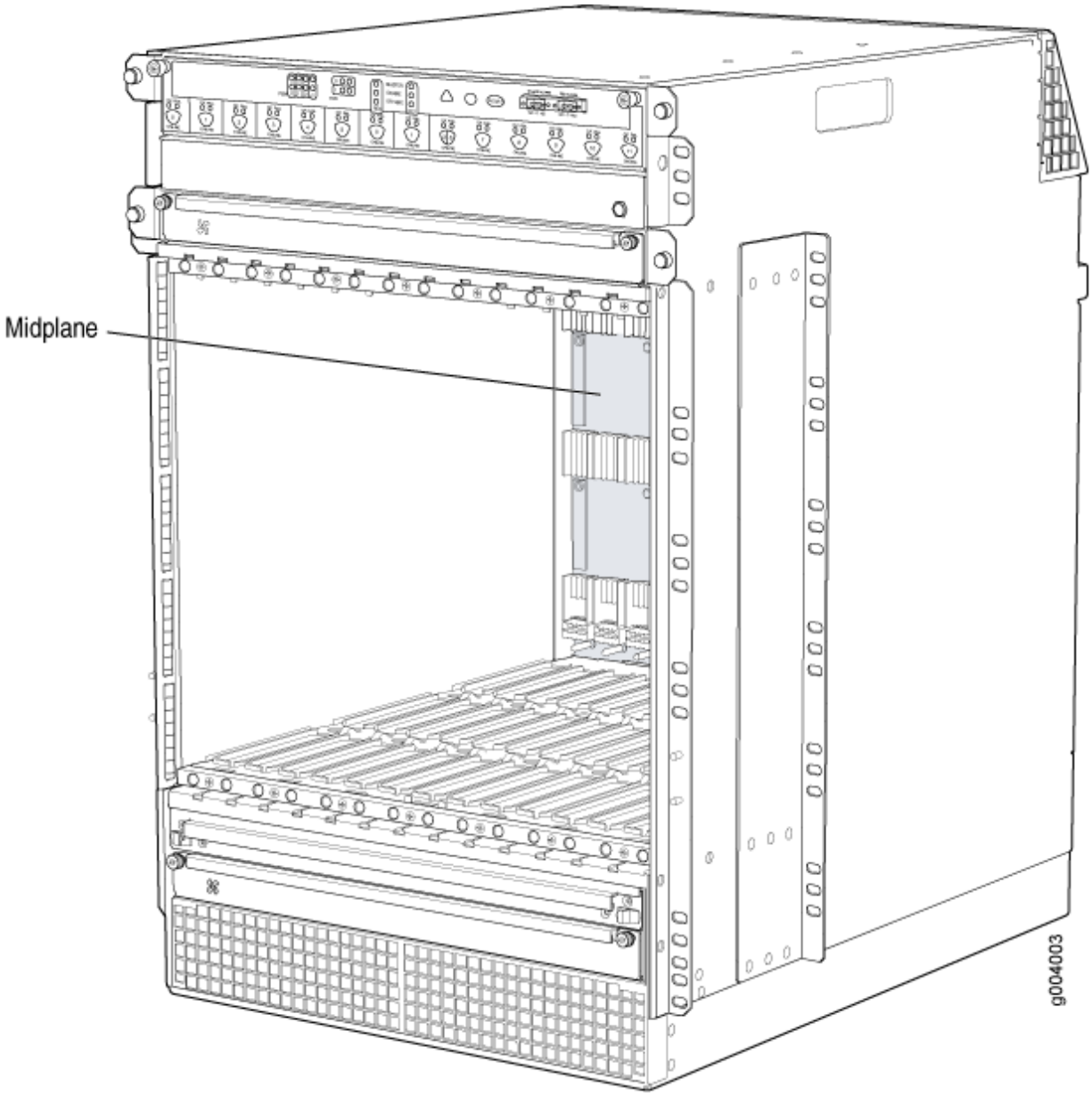
The midplane performs the following major functions:

- Data path—Data packets are transferred across the midplane between the IOCs and SPCs through the fabric ASICs on the SCBs.

- Power distribution—The power supplies are connected to the midplane, which distributes power to all the firewall components.
- Signal path—The midplane provides the signal path to the IOCs, SCBs, SPCs, Routing Engine, and other system components for monitoring and control of the system.

The enhanced midplane supports Junos OS Release15.1X49-D10. It provides greater per-slot fabric performance and signal integrity, along with error-free high speed data transfer, and it reduces cross-talk. The midplane supports link speeds up to 10 Gbps and is not field replaceable.

Figure 4: Midplane

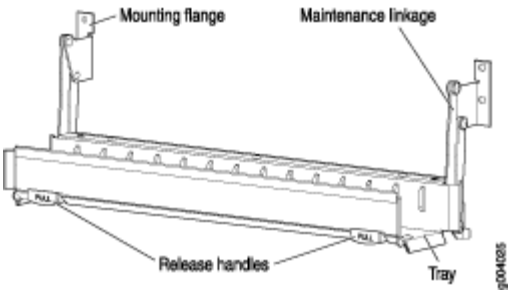


SRX5800 Firewall Cable Manager Description

The cable management system (see Figure 5 on page 14) is a tray located below the card cage that has a row of fourteen dividers for securing the cables for each card. Features in the cable management tray allow you to gently secure the cables with cable strips or other ties. To secure the cables in place, loop the tie through the cable anchor and secure the tie.

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 air filter.

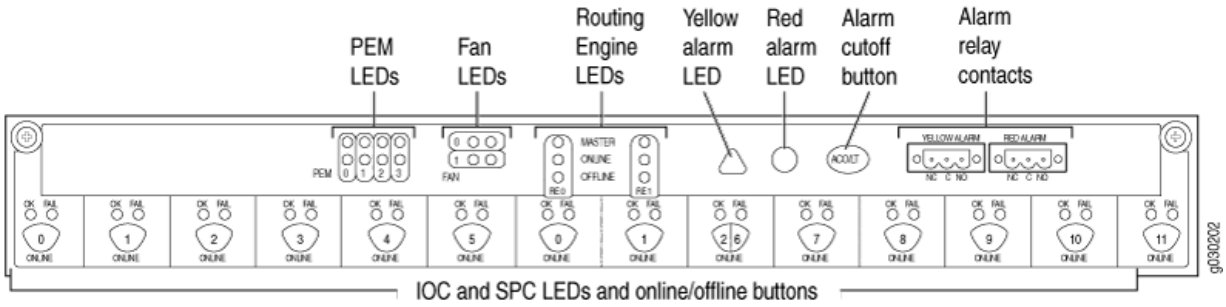
Figure 5: Cable Management System



SRX5800 Firewall Craft Interface Overview

The craft interface shows you status and troubleshooting information at a glance and lets you perform many system control functions (see Figure 6 on page 14). It is hot-insertable and hot-removable. The craft interface is located on the front of the firewall above the upper fan tray.

Figure 6: Front Panel of the Craft Interface



NOTE: The craft interface draws its power from the SCBs installed in the SCB slots 0, 1, and 2 at the center of the card cage. At least one SCB must be installed in the firewall for the craft interface to obtain power.

SRX5800 Firewall Craft Interface Alarm LEDs and Alarm Cutoff/Lamp Test Button

Two large alarm LEDs are located at the upper right of the craft interface. The circular red LED lights to indicate a critical condition that can result in a system shutdown. The triangular yellow LED lights to indicate a less severe condition that requires monitoring or maintenance. Both LEDs can be lit simultaneously. A condition that causes an LED to light also activates the corresponding alarm relay contact on the craft interface.

To deactivate the red and yellow alarms, press the button labeled **ACO/LT** (for "alarm cutoff/lamp test"), which is located to the right of the alarm LEDs. Deactivating an alarm turns off both LEDs and deactivates the device attached to the corresponding alarm relay contact on the craft interface.

Table 3 on page 15 describes the alarm LEDs and alarm cutoff button in more detail.

Table 3: Alarm LEDs and Alarm Cutoff/Lamp Test Button

Shape	Color	State	Description
	Red	On steadily	Critical alarm LED—Indicates a critical condition that can cause the device to stop functioning. Possible causes include component removal, failure, or overheating.
	Yellow	On steadily	Warning alarm LED—Indicates a serious but nonfatal error condition, such as a maintenance alert or a significant increase in component temperature.
	–	–	Alarm cutoff/lamp test button—Deactivates red and yellow alarms. Causes all LEDs on the craft interface to light (for testing) when pressed and held.

SRX5800 Firewall Craft Interface Host Subsystem LEDs

The host subsystem has three LEDs, located in the middle of the craft interface, that indicate its status. The LEDs labeled **RE0** show the status of the Routing Engine and SCB in slot **0** .

The LEDs labeled **RE1** show the status of the Routing Engine and SCB in slot **1**. Table 4 on page 16 describes the functions of the host subsystem LEDs.

Table 4: Host Subsystem LEDs

Label	Color	State	Description
MASTER	Green	On steadily	Host is functioning as the master.
ONLINE	Green	On steadily	Host is online and is functioning normally.
OFFLINE	Red	On steadily	Host is installed but the Routing Engine is offline.
		Off	Host is not installed.

SRX5800 Firewall Craft Interface Power Supply LEDs

Each power supply has two LEDs on the craft interface that indicate its status. The LEDs, labeled **0** through **3**, are located near the middle of the craft interface next to the **PEM** label. Table 5 on page 16 describes the functions of the power supply LEDs on the craft interface.

Table 5: Power Supply LEDs on the Craft Interface

Label	Color	State	Description
PEM	Green	On steadily	Power supply is functioning normally.
	Red	On steadily	Power supply has failed or power input has failed.

SRX5800 Firewall Craft Interface Card OK/Fail LEDs

Each slot in the card cage has a pair of LEDs on the craft interface that indicates the status of the card installed in it. The card LEDs are located along the bottom edge of the craft interface and are labeled as follows:

- **0** through **5** on the left

- **0** and **1** for the two center slots reserved for SCBs
- **2/6** and **7** through **11** on the right

Table 6 on page 17 describes the functions of the **OK** and **Fail** LEDs.

Table 6: Card OK/Fail LEDs

Label	Color	State	Description
OK	Green	On steadily	The card is functioning normally.
		Blinking	The card is transitioning online or offline.
		Off	The card is not online.
FAIL	Red	On steadily	The card has failed.

SRX5800 Firewall Craft Interface Fan LEDs

Each fan LED is located on the top left of the craft interface. Table 7 on page 17 describes the functions of the fan LEDs.

Table 7: Fan LEDs

Label	Color	State	Description
OK	Green	On steadily	Fan tray is functioning normally.
FAIL	Red	On steadily	Fan tray has failed.

SRX5800 Firewall Craft Interface Online Buttons

The craft interface has a row of Online/Offline buttons along its lower edge. Each button corresponds to one slot in the card cage. The Online/Offline buttons are only supported for slots containing MPC interface cards. You can install MPCs into slots:

- SRX5400–Any slot except bottom slot **0**
- SRX5600–Any slot except bottom slots **0** or **1**
- SRX5800–Any slot except center slots **0** or **1**

NOTE: The Online/Offline buttons are not supported for removal and replacement of SPCs or SCB.

CAUTION: While traffic is passing through the Firewall, particularly if the device is configured as part of a high availability (HA) cluster, we strongly recommend that you do not push any of the Online/Offline buttons.

To take an MPC offline using the Online/Offline buttons:

1. Press and hold the corresponding card's Online/Offline button on slot **1** on the craft interface. The green **OK/FAIL** LED next to the button begins to blink. Hold until both the button's LED and the MPC's LED are off.
2. Issue the CLI `show chassis fpc` command to check the status of installed MPCs. As shown in the sample output, the value *Offline* in the column labeled *State* indicates that the MPC in slot **1** is now offline:

```
user@host> show chassis fpc

Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online           35      4          0       1024       13         25
  1  Online           47      3          0       1024       13         25
  2  Online           37      8          0       2048       18         14
```

An MPC can also be taken offline via CLI command:

```
user@host> request chassis fpc slot 2 offline
node0:
```

```
--------------------------------------------------------------------------
Offline initiated, use "show chassis fpc" to verify

{primary:node0}
```

```
user@host> show chassis fpc
node0:
--------------------------------------------------------------------------
                     Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online            35      7          0       1024       13         25
  1  Online            46      4          0       1024       13         25
  2  Offline         ---Offlined by cli command---

After pushing MPC online button:
```

```
user@host> show chassis fpc
                     Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online            34      5          0       1024       13         25
  1  Online            46      3          0       1024       13         25
  2  Offline         ---Offlined by button press---
```

To bring an MPC back online using the Online/Offline buttons:

1. Press and hold the corresponding card's Online/Offline button on slot **1** on the craft interface. The green **OK/FAIL** LED next to the button and the MPC's LED begins to blink. Hold until both the button's LED and the MPC's LED are green and steady.

2. Issue the CLI `show chassis fpc` command to check the status of installed MPCs. As shown in the sample output, the value *Online* in the column labeled *State* indicates that the MPC in slot **1** is functioning normally:

   Verify if the MPC is offline:

```
user@host> show chassis fpc
node0:
--------------------------------------------------------------------------
                     Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
```

```
  0  Online            37     23          0       2048       19         14
  1  Offline         ---Offlined by cli command---
  2  Online            49     37          0       1024       14         25
```

The command output indicates the MPC is offline.

Bring the MPC online for the first time by using the following CLI command:

```
user@host> request chassis fpc slot 1 online
node0:
--------------------------------------------------------------------------
Online initiated, use "show chassis fpc" to verify
```

Verify that the MPC is online:

```
user@host> request chassis fpc slot 1 online
node 0
node0:
--------------------------------------------------------------------------
FPC 1 already online
```

The command output indicates the MPC is online.

Confirm that the MPC in the chassis is online:

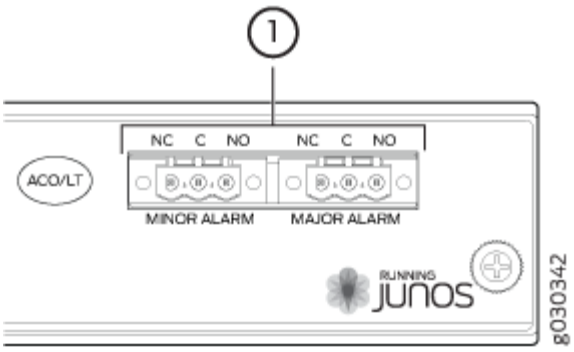
```
user@host> show chassis fpc
node0:
--------------------------------------------------------------------------
                     Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online            37      6          0       2048       19         14
  1  Online            44     11          0       1024       23         29
  2  Online            49     22          0       1024       14         25
```

SRX5800 Firewall Craft Interface Alarm Relay Contacts

The craft interface has two alarm relay contacts for connecting the device to external alarm devices (see Figure 7 on page 21). Whenever a system condition triggers either the major or minor alarm on the

craft interface, the alarm relay contacts are also activated. The alarm relay contacts are located on the upper right of the craft interface.

Figure 7: Alarm Relay Contacts



The alarm relay contacts consist of two sets of connectors, one set for each of the two alarms (major and minor). For each alarm color there are three connectors. Table 8 on page 21 describes the functions of the connectors.

Table 8: Alarm Relay Contact Functions

Contact Label	Contact Name	Function
NC	Normally Closed	Connects the alarm relay to an external alarm-reporting device that activates when the circuit between C and NC is closed.
C	Current In	Connects the alarm relay to the current source for the external alarm-reporting device.
NO	Normally Open	Connects the alarm relay to an external alarm-reporting device that activates when the circuit between C and NC is open.

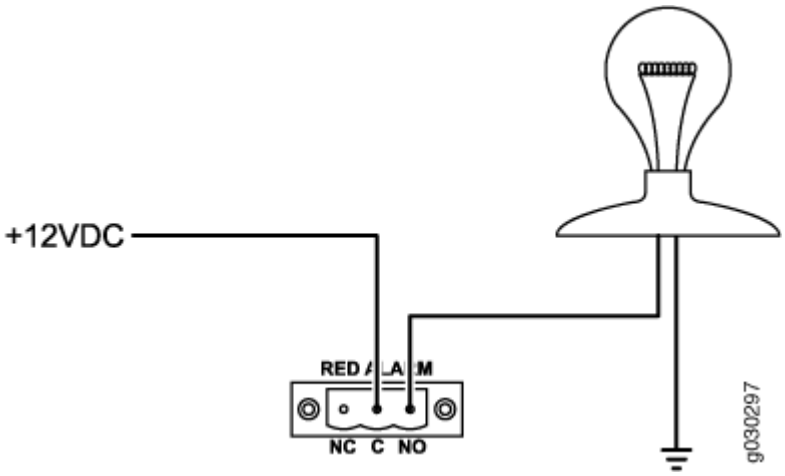
Table 9 on page 22 shows the electrical specifications for the alarm relay contacts.

Table 9: Alarm Relay Contact Electrical Specifications

	Current Type	
	AC	DC
Maximum Voltage	250	30
Maximum Current	8 A	

Figure 8 on page 22 shows an example wiring diagram for a simple alarm reporting device. In this case the device is a 12-volt light bulb that illuminates when the device encounters a condition that activates the major alarm LED and relay contacts. The alarm relay contacts can also be used to activate other devices such as bells or buzzers.

Figure 8: Example Alarm Reporting Device



SRX5800 Firewall Cooling System

The cooling system consists of the following components:

- Upper fan tray
- Bottom fan tray

- Air filter tray and air filter

The cooling system components work together to keep all firewall components within the acceptable temperature range (see Figure 9 on page 23, Figure 10 on page 24, Figure 11 on page 24, Figure 12 on page 24, and Figure 13 on page 25). The firewall has two fan trays located in the front of the device that install horizontally above and below the card cage.

NOTE: In the Junos OS command-line interface (CLI):

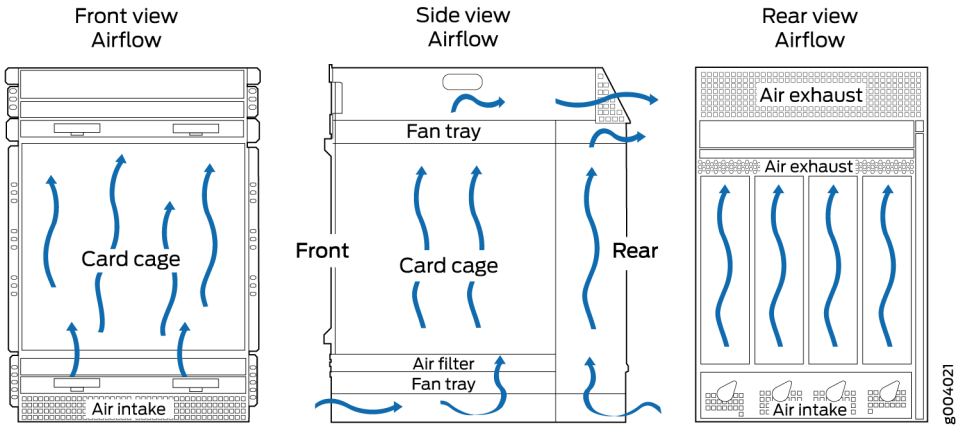
- The `show chassis hardware` command output displays the fan trays as `Fan Tray 0` for the upper fan tray and `Fan Tray 1` for the bottom fan tray.
- The `show chassis environment` command output displays the fan trays as `Upper Fan Tray` and `Bottom Fan Tray`.

Two different types of fan trays are available:

- The standard capacity fan tray has six fans that operate at 728 cubic feet per minute (CFM) at full speed and is adequate for firewalls in which standard-capacity power supplies are installed.
- The high-capacity fan tray has 12 fans that operate at 976 cubic feet per minute (CFM) at full speed and is required when high-capacity power supplies are installed. When high-capacity fan trays are installed, you must also install the high-capacity air filter tray.

The fan trays are interchangeable and are hot-insertable and hot-removable.

Figure 9: Airflow Through the Chassis



The host subsystem monitors the temperature of the device components. When the device 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 the system by disabling output power from each PEM.

There is a single air intake in the front of the firewall. Air is pushed up through an air filter, through the card cage, and then through the upper fan tray where it combines in a common exhaust plenum and is exhausted out the upper rear of the system.

Figure 10: Standard-Capacity Fan Tray (Same Upper and Bottom)

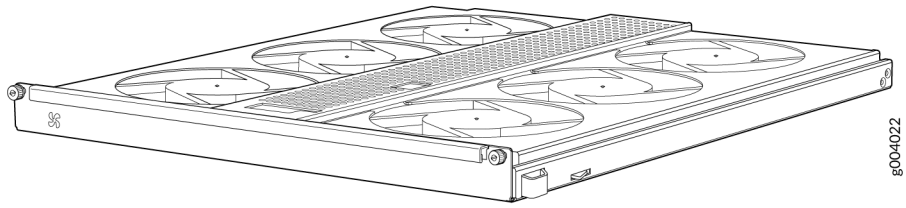


Figure 11: High-Capacity Fan Tray (Same Upper and Bottom)

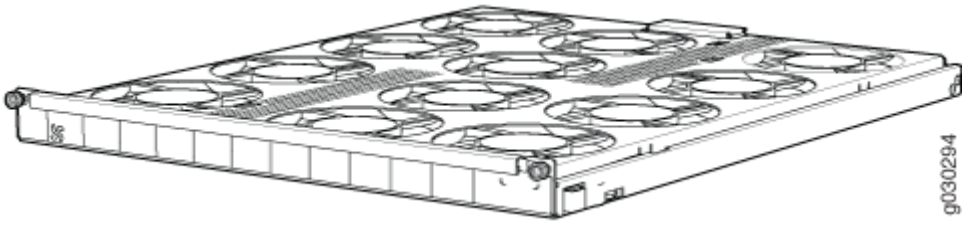


Figure 12: Air Filter

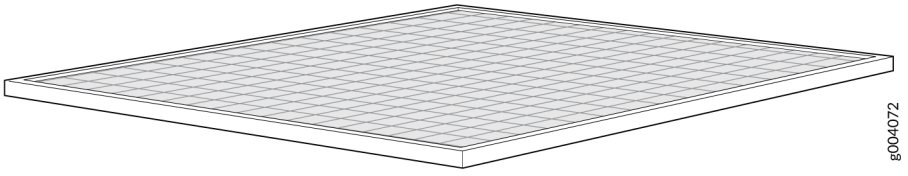


Figure 13: Standard-Capacity Air Filter Tray

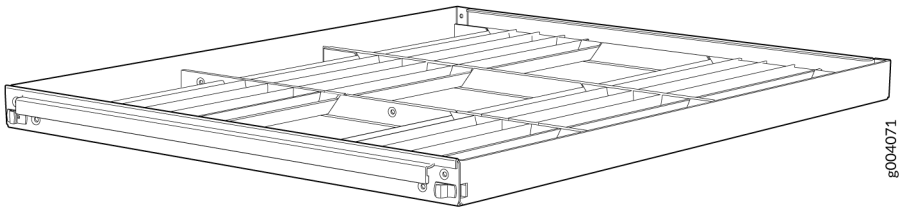
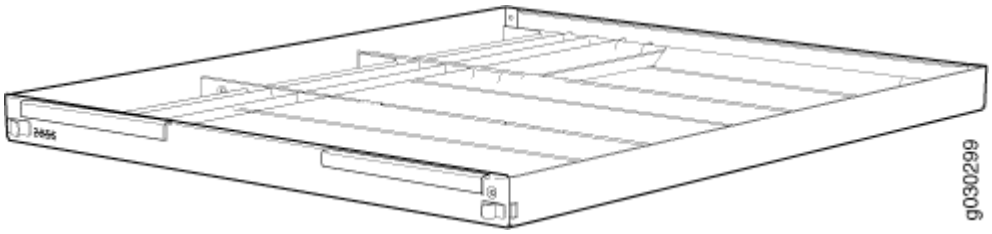


Figure 14: High-Capacity Air Filter Tray



SRX5800 Power System

IN THIS SECTION

SRX5800 Firewall Power System Overview

The SRX5800 Firewall uses either AC or DC power supplies. The firewall is configurable with two to four AC power supplies or two or four DC power supplies. The power supplies connect to the midplane, which distributes the different output voltages produced by the power supplies to the firewall components, depending on their voltage requirements.

Table 10 on page 27 describes the different types of power supplies available.

Table 10: Power Supply Type Summary

Power Supply Type	Juniper Model Number	Input Condition (If Any)	Maximum Output	Redundancy	Power Distribution
AC standard-capacity	SRX5800-PWR-AC		1700 W	3+1	Shared
AC high-capacity	SRX5800-PWR-4100-AC	One AC input	1700 W	2+2	Zoned
		Two AC inputs	4100 W		
High-Capacity Second-Generation AC Power Supply	SRX5800-HPWR-AC	One AC input	2550 W		
		Two AC inputs	5100 W		
High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supply	MX960-PSM-HV		5100 W		
DC standard-capacity	SRX5800-PWR-DC		1700 W		
DC high-capacity	SRX5800-PWR-4100-DC	One DC input	1700 W		
		Two DC inputs	4100 W		

NOTE: The firewall must be running Junos OS Release 10.4 or later in order to use high-capacity AC power supplies. The firewall must be running Junos OS Release 12.1X44-D10 or later in order to use high-capacity DC power supplies.

The firewall must be running Junos OS Release 21.4R1 or later in order to use high-capacity second-generation AC and high-voltage second-generation universal (HVAC or HVDC) power supplies.

Redundant power supplies are hot-removable and hot-insertable. Each power supply is cooled by its own internal cooling system.

NOTE: Devices configured from the factory with DC power supplies are shipped with a blank panel installed over the power distribution modules. Devices configured with AC power supplies have no blank panel.

CAUTION: The firewall cannot be powered from AC and DC power supplies simultaneously. The first type of power supply detected by the firewall when initially powered on determines the type of power supply allowed by the firewall. All installed power supplies of the other type are disabled by the firewall. If you install a power supply of the other type while the firewall is operating, the firewall disables the power supply and generates an alarm.

When the firewall is powered by standard-capacity AC power supplies, the firewall contains either three or four AC power supplies, located at the rear of the chassis in slots **PEM0** through **PEM3** (left to right). Each power supply provides power to all components in the firewall. When three power supplies are present, they share power almost equally within a fully populated system. Four power supplies provide full power redundancy. If one power supply fails or is removed, the remaining power supplies instantly assume the entire electrical load without interruption. Three power supplies provide the maximum configuration with full power for as long as the firewall is operational.

When the firewall is powered by either standard- or high-capacity DC power supplies, or high-capacity AC power supplies, or by high-capacity second-generation AC power supplies, or high-voltage second-generation universal (HVAC or HVDC) power supplies power distribution within the chassis is divided into zones, as described in Table 11 on page 28.

Table 11: SRX5800 Firewall Power Distribution (DC, or High-Capacity AC, or High-Capacity Second-Generation AC, or High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supplies)

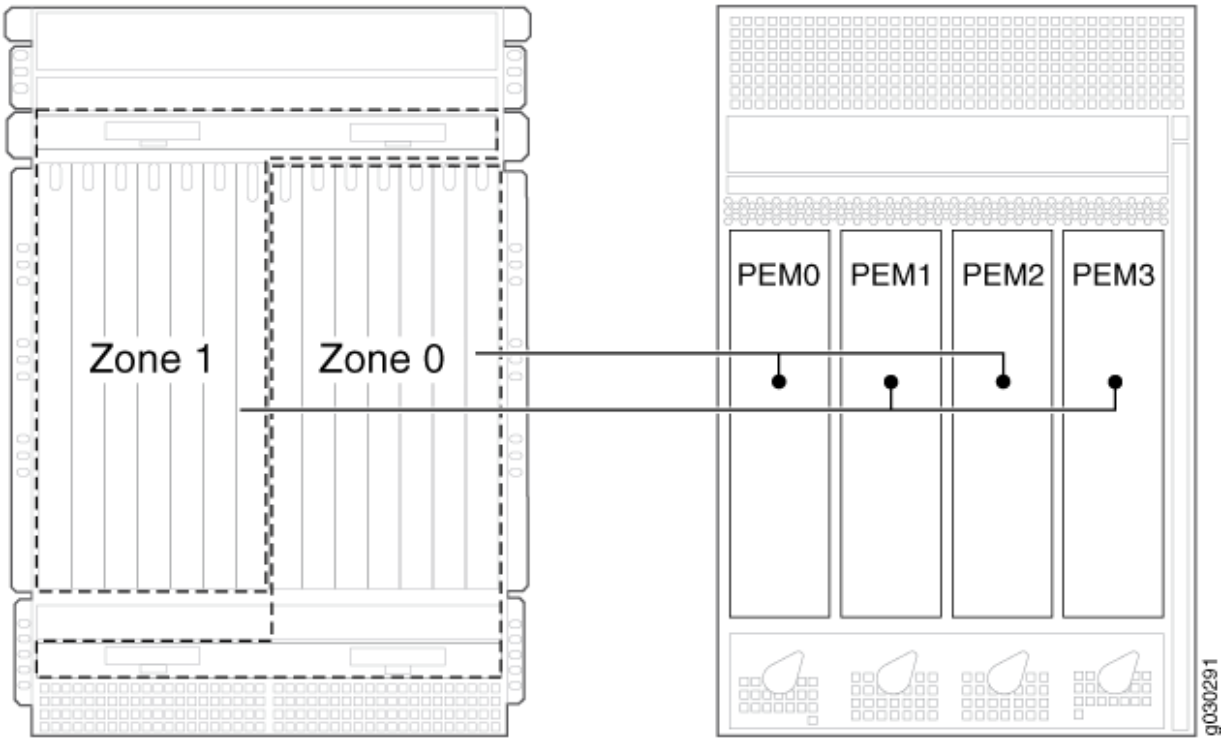
Zone	Power Supplies	Provide Power To:
Zone 0	• PEM0 • PEM2	• Bottom fan tray • IOC or SPC slots 6 through 11 • SCB slots 1 and 2

Table 11: SRX5800 Firewall Power Distribution (DC, or High-Capacity AC, or High-Capacity Second-Generation AC, or High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supplies) ***(Continued)***

Zone	Power Supplies	Provide Power To:
Zone 1	• PEM1 • PEM3	• Upper fan tray • IOC or SPC slots 0 through 5 • SCB slot 0

Figure 15 on page 29 shows the distribution of power from the power supplies to the chassis components in an SRX5800 Firewall chassis powered by DC power supplies, or high-capacity AC power supplies, or high-capacity second-generation AC, or high-voltage second-generation universal (HVAC or HVDC) power supplies.

Figure 15: Power Distribution from DC, or High-Capacity AC, or High-Capacity Second-Generation AC, or High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supplies in the SRX5800 Firewall Chassis



NOTE: The craft interface draws its power from the SCBs installed in the SCB slots 0, 1, and 2 at the center of the card cage. In the standard configuration, with SCBs in slots 0 and 1, the craft interface is powered on even when one of the two zones loses power. But if the chassis only has one SCB installed, the craft interface draws all of its power from that card, and consequently is powered off if the zone in which that SCB is installed loses power.

You can install either two or four DC power supplies, or high-capacity AC power supplies, or high-capacity second-generation AC, or high-voltage second-generation universal (HVAC or HVDC) power supplies. Two power supplies are required to power the two zones, while four power supplies provide full redundancy for both zones. The power supplies in slots **PEM0** and **PEM2** form a redundant pair, as do the power supplies in slots **PEM1** and **PEM3**. When two power supplies are installed for a zone, they share the load. If a power supply fails, its redundant power supply assumes the full load of that zone without interruption.

If you do install only two power supplies, they must be installed so that one is in an odd-numbered slot and the other is in an even-numbered slot. For example, you can install one high-capacity AC power supply in each of the slots **PEM0** and **PEM1**.

SRX5800 Firewall Standard-Capacity AC Power Supply—SRX5800-PWR-AC

Each standard-capacity AC power supply (SRX5800-PWR-AC) has a corresponding AC appliance inlet located in the chassis directly above the power supply. Each inlet requires a dedicated AC power feed and a dedicated 15 A (250 VAC) circuit breaker. See Figure 16 on page 31.

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, the firewall chassis must be adequately grounded before power is connected. See "Grounding the SRX5800 Firewall" on page 252 for instructions.

Figure 16: Standard-Capacity AC Power Supply

SRX5800 Firewall Standard-Capacity AC Power Supply LEDs

Each standard-capacity AC power supply faceplate contains three LEDs that indicate the status of the power supply (see Table 12 on page 31). The power supply status is also reflected in two LEDs on the craft interface. In addition, a power supply failure triggers the red alarm LED on the craft interface.

Table 12: Standard Capacity AC Power Supply LEDs

Label	Color	State	Description
AC OK	Green	Off	AC power applied to power supply is not within the normal operating range.
		On	AC power applied to power supply is within the normal operating range.
DC OK	Green	Off	DC power outputs generated by the power supply are not within the normal operating ranges.
		On	DC power outputs generated by the power supply are within the normal operating ranges.
PS FAIL	Red	Off	Power supply is functioning normally.

Table 12: Standard Capacity AC Power Supply LEDs *(Continued)*

Label	Color	State	Description
		On	Power supply is not functioning normally. Check **AC OK** and **DC OK** LEDs for more information.

SRX5800 Firewall High-Capacity AC Power Supply—SRX5800-PWR-4100-AC

High-capacity AC power supplies (SRX5800-PWR-4100-AC) provide a maximum of 4100 W of power each. Two high-capacity power supplies are required, and you can install four high-capacity power supplies for redundancy. Each high-capacity AC power supply has two corresponding AC appliance inlets: one located in the chassis directly above the power supply and one located near the top edge of the power supply itself. For each power supply, you connect one power cord to the inlet on the chassis above the power supply and one power cord to the inlet on the power supply itself. Each inlet you connect requires a dedicated AC power feed and a dedicated 15 A (250 VAC) circuit breaker. See Figure 17 on page 34.

NOTE: The firewall cannot be powered from standard-capacity and high-capacity AC power supplies simultaneously. The one exception is during the process of replacing standard-capacity AC power supplies with high-capacity AC power supplies, when it is permissible to have both types installed briefly.

NOTE: The high-capacity power supply will operate with only one of its two AC inlets connected to an AC power feed. However, its DC output will be limited to a maximum of 1700 W. We recommend that you connect two AC power feeds to each high-capacity AC power supply.

NOTE: The firewall must be running Junos OS Release 10.4 or later in order to use high-capacity AC power supplies.

Each high-capacity AC power supply has an input mode switch, covered by a small metal plate. The input mode switch tells the system the number of AC power feeds it should expect. The input mode switch settings are described in Table 13 on page 33. The default setting is 1.

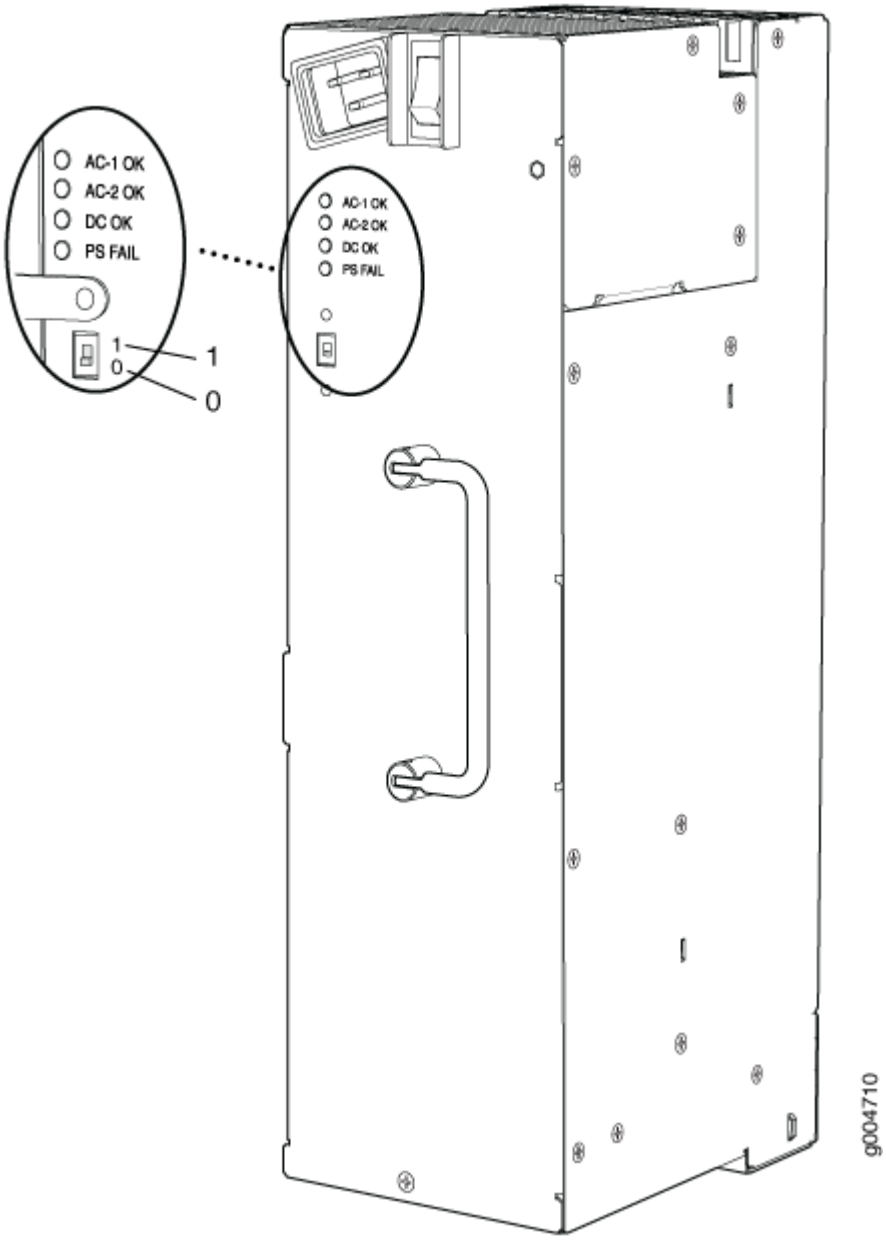
Table 13: High-Capacity AC Power Supply Input Mode Switch Settings

Mode Switch Setting	AC Inputs	Result
1	Both AC inlets powered	AC output of 4100 W **AC OK** LED lights
	Only one AC inlet powered	AC output of 1700 W **AC OK** LED lights
0	Both AC inlets powered	AC output of 4100 W **AC OK** LED lights
	Only one AC inlet powered	AC output disabled **AC OK** LED unlit

NOTE: We recommend that you set the input mode switch to **1** and connect two AC input feeds to each high-capacity AC power supply.

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, the firewall chassis must be adequately grounded before power is connected. See "Grounding the SRX5800 Firewall" on page 252 for instructions.

Figure 17: High-Capacity AC Power Supply



SRX5800 Firewall High-Capacity AC Power Supply LEDs

Each high-capacity AC power supply faceplate contains four LEDs that indicate the status of the power supply (see Table 14 on page 35). The power supply status is also reflected in two LEDs on the craft interface. In addition, a power supply failure triggers the red alarm LED on the craft interface.

Table 14: High-Capacity AC Power Supply LEDs

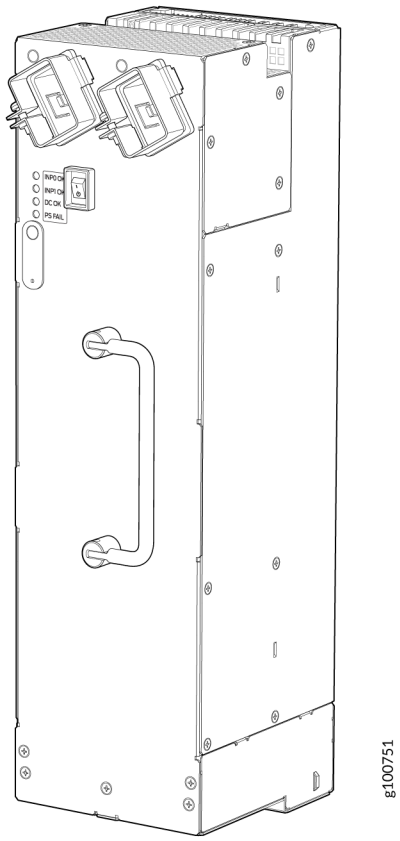
Label	Color	State	Description
AC-1 OK	Green	Off	AC power applied to power supply at the upper appliance inlet is not within the normal operating range.
		On	AC power applied to power supply at the upper appliance inlet is within the normal operating range.
AC-2 OK	Green	Off	AC power applied to power supply at the lower appliance inlet is not within the normal operating range.
		On	AC power applied to power supply at the lower appliance inlet is within the normal operating range.
DC OK	Green	Off	DC power outputs generated by the power supply are not within the normal operating ranges.
		On	DC power outputs generated by the power supply are within the normal operating ranges.
PS FAIL	Red	Off	Power supply is functioning normally.
		On	Power supply is not functioning normally. Check the **AC-1 OK**, **AC-2 OK**, and **DC OK** LEDs for more information.

SRX5800 Firewall High-Capacity Second-Generation AC Power Supply—SRX5800-HPWR-AC

IN THIS SECTION

The SRX5800 Firewall can also be powered by four High-Capacity Second-Generation AC power supplies (SRX5800-HPWR-AC). The high-capacity second-generation power supplies must be installed in adjacent slots in the chassis. They can operate in either one-feed mode or two-feed mode. The maximum inrush current per feed for a high-capacity AC power supply is 38 A per feed at 264 VAC.

Figure 18: SRX5800 Firewall High-Capacity Second-Generation AC Power Supply



In the one-feed mode, the power supplies provide power at a reduced capacity (2550 W). In the two-feed mode, the power supplies provide power at full capacity (5100 W). To operate the SRX5800 at full capacity, you must use the two-feed mode. High-capacity second-generation AC power supplies require one power cord per feed. Therefore, to operate the SRX5800 Firewall at full capacity, you need eight power cords.

Each high-capacity second-generation AC power supply accepts two AC feeds in two C19/C20 AC receptacles, both receptacles are located on the power supply. Do not use the receptacle located on the chassis. For supported power cables, see "AC Power Cord Specifications for the SRX5800 Firewall" on page 40.

When using the high-capacity second-generation AC power supplies in one-feed mode, plug one end of the power cord into the corresponding AC receptacle directly on the power supply and the other end into an AC outlet. When using the high-capacity second-generation AC power supply in two-feed mode, you need two power cords. Plug both power cords into the AC receptacles on the power supply the other ends of the cable into AC outlets.

In high-capacity second-generation AC power supply configurations, there are two zones that provide power to specific components in the SRX5800 Firewall. Redundancy is 1+1 per zone. Table 15 on page 37 lists the components that receive power for each zone in a high-capacity AC power supply configuration.

Table 15: Zoning for High-Capacity Second-Generation Power Supplies in an SRX5800 Firewall

Chassis Power Configuration	Zone	Power Supply (PEM)	Provide Power To
High-capacity second-generation AC power supplies	Zone 0	• PEM0 • PEM2	• Bottom fan tray • IOC or SPC slots 6 through 11 • SCB slots 1 and 2
High-capacity second-generation AC power supplies	Zone 1	• PEM1 • PEM3	• Upper fan tray • IOC or SPC slots 0 through 5 • SCB slot 0

SRX5800 Firewall High-Capacity Second-Generation AC Power Supply LEDs

Each high-capacity second-generation AC power supply faceplate contains four LEDs that indicate the status of the power supply (see Figure 19 on page 38 and Table 16 on page 38).

Figure 19: High-Capacity Second-Generation AC Power Supply LEDs

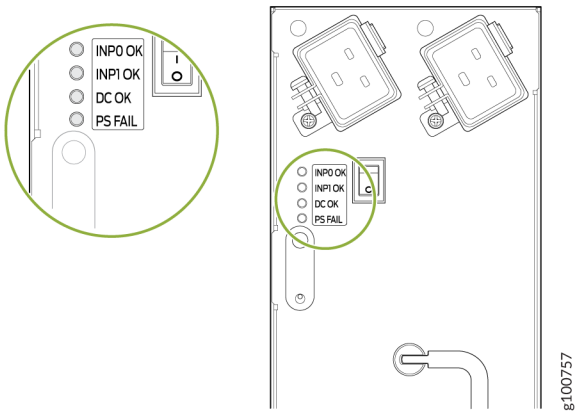


Table 16: High-Capacity Second-Generation AC Power Supply LEDs

Label	Color	State	Description
INP0 OK	Green	Off	AC power applied to power supply is not within the normal operating range.
		On	AC power applied to power supply is within the normal operating range.
INP1 OK	Green	Off	AC power applied to power supply is not within the normal operating range.
		On	AC power applied to power supply is within the normal operating range.
DC OK	Green	Off	DC power outputs generated by the power supply are not within the normal operating ranges.
		On	DC power outputs generated by the power supply are within the normal operating ranges.
PS FAIL	Red	Off	Power supply is functioning normally.

Table 16: High-Capacity Second-Generation AC Power Supply LEDs *(Continued)*

Label	Color	State	Description
		On	Power supply is not functioning normally. Check **AC OK** and **DC OK** LEDs for more information.

SRX5800 Firewall AC Power Supply Specifications

Table 17 on page 39 lists the AC power supply electrical specifications for both the standard-capacity, high-capacity, and high-capacity second-generation AC power supply. Table 18 on page 40 lists the AC power system electrical specifications.

Table 17: AC Power Supply Electrical Specifications

Item	Specification		
	Standard-Capacity	High-Capacity	High-Capacity Second-Generation
Maximum output power	1700 W	4100 W (two AC inputs) 1700 W (one AC input)	5100 W (two AC inputs) 2550 W (one AC input)
AC input current rating	11 A @ 240 VAC maximum	13 A @ 240 VAC maximum per AC input (26 A per power supply when two AC inputs are used)	16 A @ 200 VAC maximum per AC input (32 A per power supply when two AC inputs are used)
AC input voltage	Operating range: 200 to 240 VAC		Operating range: 180 to 264 VAC
AC input line frequency	50 to 60 Hz		47 to 63 Hz

Table 17: AC Power Supply Electrical Specifications *(Continued)*

Item	Specification		
	Standard-Capacity	High-Capacity	High-Capacity Second-Generation
Efficiency	~88% **NOTE**: This value is at full load and nominal voltage.		~91% **NOTE**: This value is at full load and nominal voltage.

Table 18: AC Power System Specifications

Item	Normal-Capacity	High-Capacity		High-Capacity Second-Generation	
		Two AC inputs for each power supply	One AC input for each power supply	Two AC inputs for each power supply	One AC input for each power supply
Redundancy	3+1	2+2	2+2	2+2	2+2
Output power (maximum) per supply	1700 W	4100 W	1700 W	5100 W	2550 W
Output power (maximum) per system	5100 W	8200 W	3400 W	1.2 KW	5100 W

AC Power Cord Specifications for the SRX5800 Firewall

Each AC power supply has a single AC appliance inlet located in the chassis directly above the power supply that requires a dedicated AC power feed. Most sites distribute power through a main conduit that leads to frame-mounted power distribution panels, one of which can be located at the top of the rack that houses the firewall. An AC power cord connects each power supply to the power distribution panel.

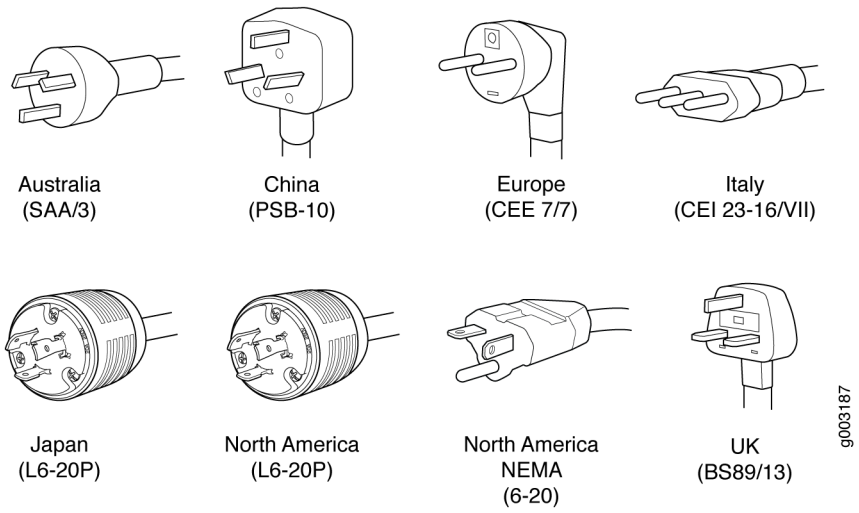
The firewall is not shipped with AC power cords. You must order power cords separately using the model number shown in Table 19 on page 41. The C19 appliance coupler end of the cord inserts into the AC appliance inlet coupler, type C20 (right angle) as described by International Electrotechnical Commission (IEC) standard 60320. The plug end of the power cord fits into the power source receptacle that is standard for your geographical location.

Table 19 on page 41 provides specifications and Figure 20 on page 42 depicts the plug on the AC power cord provided for each country or region.

Table 19: AC Power Cord Specifications

Country	Model Number	Electrical Specification	Plug Type
Australia	CBL-M-PWR-RA-AU	240 VAC, 50 Hz AC	SAA/3
China	CBL-M-PWR-RA-CH	220 VAC, 50 Hz AC	PSB-10
Europe (except Denmark, Italy, Switzerland, and United Kingdom)	CBL-M-PWR-RA-EU	220 or 230 VAC, 50 Hz AC	CEE 7/7
Italy	CBL-M-PWR-RA-IT	230 VAC, 50 Hz AC	CEI 23-16/VII
Japan	CBL-M-PWR-RA-JP	220 VAC, 50 or 60 Hz AC	NEMA L6-20P
North America	CBL-M-PWR-RA-TWLK-US	250 VAC, 60 Hz AC	NEMA L6-20P
United Kingdom	CBL-M-PWR-RA-UK	240 VAC, 50 Hz AC	BS89/13

Figure 20: AC Plug Types



Each high-capacity second-generation (MX960-PSM-5K-AC) power supply has two AC appliance inlets located in the power supply itself. Each receptacle requires a dedicated AC power feed and a dedicated breaker. Table 20 on page 42 provides specifications for the high-capacity second-generation PSM.

CAUTION: The bend radius for the power cord cables is 7 inches. Avoid bending the cable beyond it's bend radius when dressing the cables into the cable channels on the rack.

Table 20: AC Power Cord Specifications for the MX960-PSM-5K-AC PSM

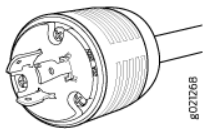
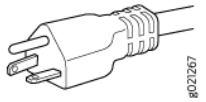
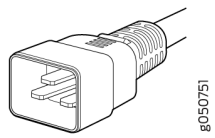
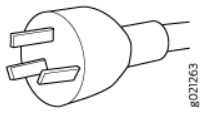
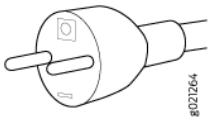
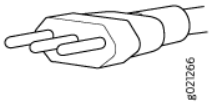
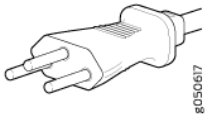
Country	Model Number	Electrical Specification	Plug Type	Graphic
North America	CBL-M-PWR-RA-JP	250 VAC, 20 A, 50 or 60 Hz AC	NEMA L6-20P Type NEMA Locking	
North America	CBL-M-PWR-RA-US	250 VAC, 20 A, 60 Hz	NEMA 6-20, Type N6/20	

Table 20: AC Power Cord Specifications for the MX960-PSM-5K-AC PSM *(Continued)*

Country	Model Number	Electrical Specification	Plug Type	Graphic
Worldwide (Except U.S.A)	CBL-MX-PWR-C19-C20	250 VAC, 16 A, 50 Hz	EN 60320-2-2/1	 g050751
China	CBL-PWR-C19S-162-CH	250 VAC, 16 A, 50Hz	GB 1002 Type PRC/3/16	 g021263
Continental Europe	CBL-PWR-C19S-162-EU	250 VAC, 16 A, 50 Hz	CEE (7) VII Type VIIG	 g021264
Italy	CBL-PWR-C19S-162-IT	250 VAC, 16 A, 50 Hz	CEI 23-16 Type I/ 3/16	 g021266
Switzerland	CBL-MX-PWR-C19-SZ	250 VAC, 16 A, 50 Hz	SEV 5934/2 Type 23G	 g050617

WARNING: The AC power cord for the firewall is intended for use with the firewall only and not for any other use.

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power. See "Grounding the SRX5800 Firewall" on page 252 for instructions.

CAUTION: Power cords and cables must not block access to firewall components or drape where people could trip on them.

NOTE: In North America, AC power cords must not exceed 4.5 m (approximately 14.75 ft) in length, to comply with National Electrical Code (NEC) Sections 400-8 (NFPA 75, 5-2.2) and 210-52, and Canadian Electrical Code (CEC) Section 4-010(3). The cords listed in Table 19 on page 41 are in compliance.

Understanding Input Mode Switch (DIP Switch) Settings

Each High-Capacity AC Power Supply and High-Capacity Second-Generation AC Power Supply has two input mode switches (DIP switches) on the faceplate. The DIP switches provide critical information to the power management subsystem to help generate alarms in case of a feed failure or a wrong connection. Each PSM has an LED per feed indicating whether the feed is active and whether the feed is properly connected. You must set the DIP switch on each high-capacity AC or high-capacity second-generation AC power supply according to how many feeds are connected. When one feed is connected, the system is running in reduced capacity mode. When two feeds are connected the system is running in full-capacity mode. Use these DIP switch settings:

- **Position-0** indicates one AC feed is present
- **Position-1** indicates two AC feeds are present

Refer to Figure 21 on page 45 and Figure 22 on page 45.

Figure 21: Setting the Input Mode Switch (DIP Switch)

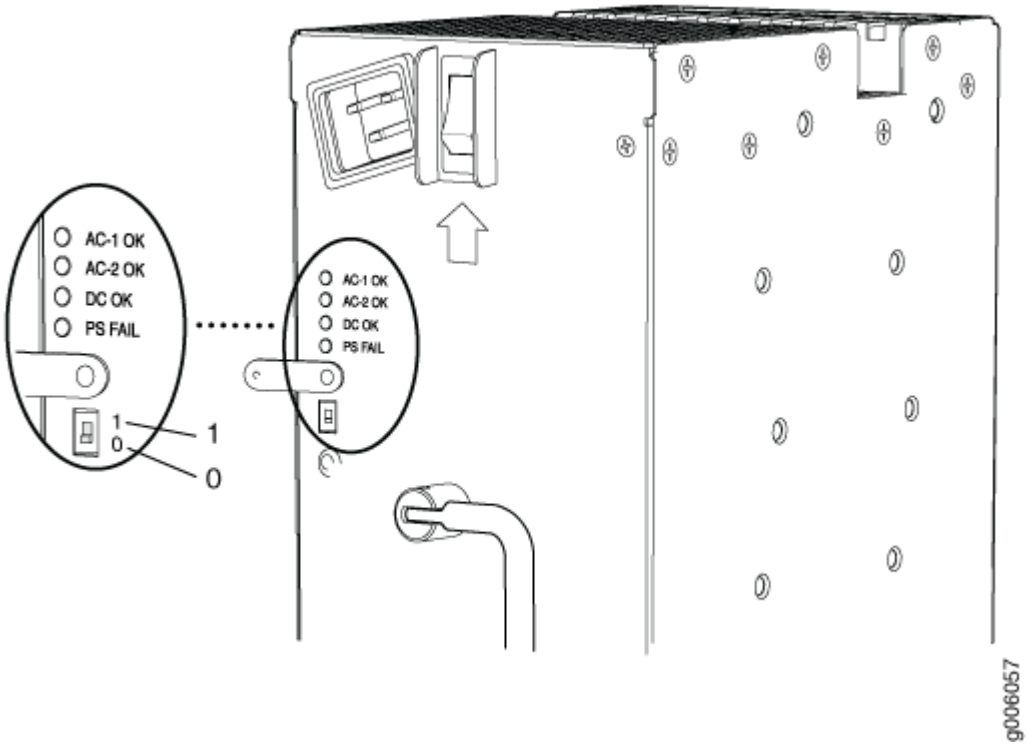
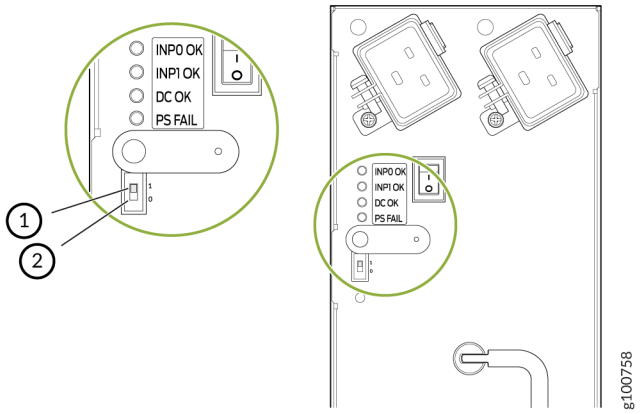


Figure 22: Setting the Input Mode Switch (DIP Switch) on High-Capacity Second-Generation AC PSM



1– Position **1** indicates two AC feeds are present	2– Position **0** indicates one AC feeds is present

Use the `show chassis power` command to verify that the DIP switch settings on the high-capacity AC power supplies are set to the correct position. Here are examples of the command output:

Example 1: Proper setting of the DIP switch

```
user@host>show chassis power
PEM 0:
  State:     Online
  AC input:  OK (2 feed expected, 2 feed connected)
  Capacity:  5100 W (maximum 5100 W)
  DC output: 171 W (zone 0, 3 A at 57 V, 3% of capacity)

PEM 1:
  State:     Online
  AC input:  OK (2 feed expected, 2 feed connected)
  Capacity:  5100 W (maximum 5100 W)
  DC output: 342 W (zone 1, 6 A at 57 V, 6% of capacity)

PEM 2:
  State:     Online
  AC input:  OK (1 feed expected, 1 feed connected)
  Capacity:  2550 W (maximum 2550 W)
  DC output: 114 W (zone 0, 2 A at 57 V, 4% of capacity)

PEM 3:
  State:     Online
  AC input:  OK (2 feed expected, 2 feed connected)
  Capacity:  5100 W (maximum 5100 W)
  DC output: 399 W (zone 1, 7 A at 57 V, 7% of capacity)

System:
  Zone 0:
      Capacity:          5100 W (maximum 5100 W)
      Allocated power:   595 W (4505 W remaining)
      Actual usage:      285 W
  Zone 1:
      Capacity:          5100 W (maximum 5100 W)
      Allocated power:   1180 W (3920 W remaining)
      Actual usage:      741 W
  Total system capacity: 10200 W (maximum 10200 W)
  Total remaining power: 8425 W

root@cland03> show chassis alarms
No alarms currently active
```

In Example 1, **PEM 0** is running at full capacity (5100 W) with two AC feeds expected and two AC feeds connected. This indicates that the DIP switch is properly set to **Position 1** since two AC feeds are connected. The example also shows that **PEM 2** is running at reduced capacity (2550 W) with one AC feed expected and one AC feed connected. This indicates that the DIP switch is correctly set to **Position 0** since one feed is present.

Example 2 shows the `show chassis power` command output when the DIP switch is set improperly:

Example 2: Improper Setting of the DIP Switch

```
user@host>show chassis power
PEM 0:
  State:     Online
  AC input:  OK (2 feed expected, 2 feed connected)
  Capacity:  5100 W (maximum 5100 W)
  DC output: 114 W (zone 0, 2 A at 57 V, 2% of capacity)

PEM 1:
  State:     Online
  AC input:  OK (2 feed expected, 2 feed connected)
  Capacity:  5100 W (maximum 5100 W)
  DC output: 342 W (zone 1, 6 A at 57 V, 6% of capacity)

PEM 2:
  State:     Present
  AC input:  Check (2 feed expected, 1 feed connected)
  Capacity:  2550 W (maximum 2550 W)
  DC output: 114 W (zone 0, 2 A at 57 V, 4% of capacity)

PEM 3:
  State:     Online
  AC input:  OK (2 feed expected, 2 feed connected)
  Capacity:  5100 W (maximum 5100 W)
  DC output: 399 W (zone 1, 7 A at 57 V, 7% of capacity)

System:
  Zone 0:
      Capacity:          5100 W (maximum 5100 W)
      Allocated power:   595 W (4505 W remaining)
      Actual usage:      228 W
  Zone 1:
      Capacity:          5100 W (maximum 5100 W)
      Allocated power:   1180 W (3920 W remaining)
```

```
      Actual usage:      741 W
  Total system capacity: 10200 W (maximum 10200 W)
  Total remaining power: 8425 W

root@cland03> show chassis alarms
1 alarms currently active
Alarm time               Class  Description
2021-10-27 13:15:14 PDT  Major  PEM 2 Not OK
```

The `PEM 0` status indicates the system is `Online`, the `AC Input` is `OK`, is running at full capacity (5100 W) with two AC feeds expected and two AC feeds connected. But notice the status for `PEM 2`. The `State` is `Present` and the `AC input` is `Check (2 feed expected, 1 feed connected)`. This indicates there is a mismatch between the DIP switch setting and the number of feeds connected. Therefore, the power supply is running at reduced capacity (2550 W). If PEM 1 should be running at full-capacity, verify that there are two feeds connected to the power supplies and the DIP switch is set to position 1.

AC Power Circuit Breaker Requirements for the SRX5800 Firewall

Each AC power supply has a single AC appliance inlet located in the chassis directly above the power supply that requires a dedicated AC power feed. We recommend that you use a dedicated customer site circuit breaker rated for 15 A (250 VAC) minimum for each AC power supply, or as required by local code.

Each high-capacity second-generation (MX960-PSM-5K-AC) power supply accepts two AC feeds in two unique AC receptacles. We recommend that you use a dedicated customer site circuit breaker rated for 38 A (264 VAC) minimum for each high-capacity second generation AC power supply, or as required by local code.

Each power cord feed must have a dedicated circuit breaker.

High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supply for SRX5800 Firewall—MX960-PSM-HV

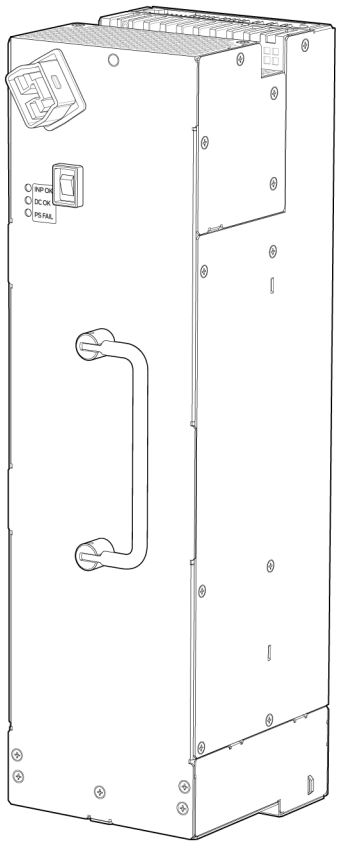
IN THIS SECTION

The SRX5800 can be powered by four high-voltage second-generation universal power supplies (MX960-PSM-HV). The MX960-PSM-HV supports high-voltage alternating current (HVAC), or high-voltage direct current (HVDC). The MX960-PSM-HV power supplies must be installed in adjacent slots in the chassis. The MX960-PSM-HV (HVAC/HVDC) power supply has one power inlet on front panel of the power supply rated at 30 A. The inlet requires a dedicated power feed and a dedicated breaker. For all power supplies the circuit breaker protection should be designed according to National Electrical Code (NEC) or any similar local standard based on maximum drawn current of the power supply specified in this document.

The MX960-PSM-HV (HVAC/HVDC) power supply configurations are zoned meaning that certain components in the SRX5800 chassis are powered by specific power supplies.

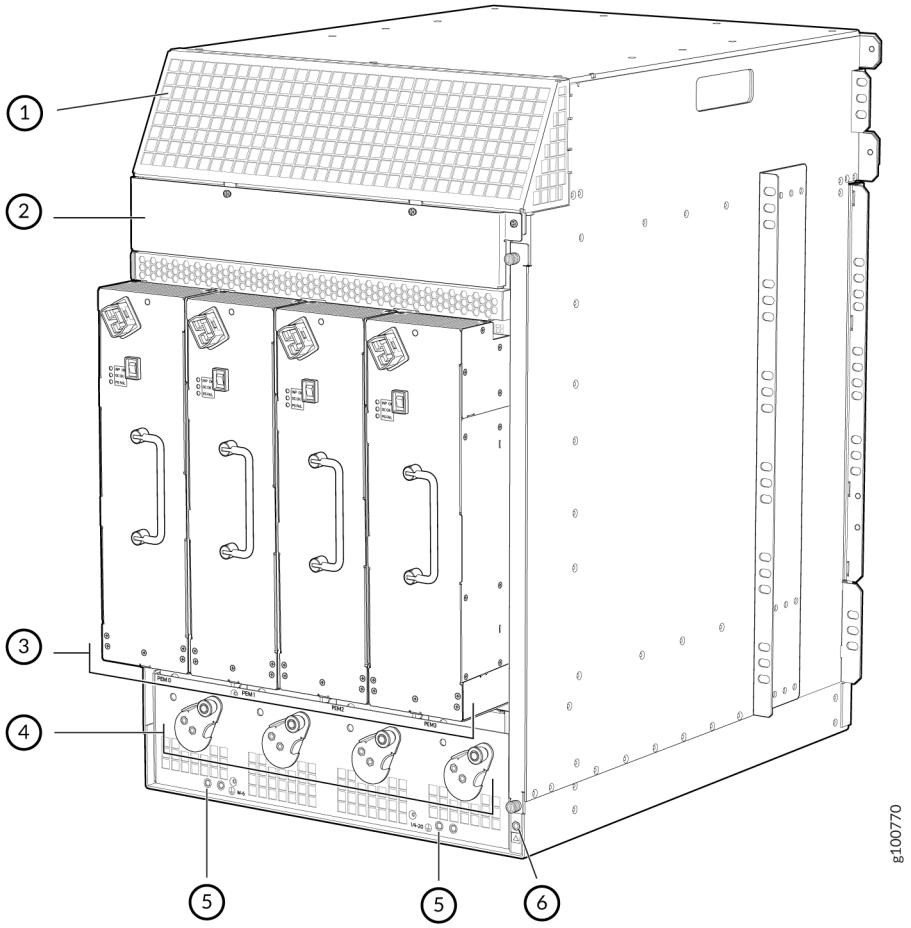
Figure 23 on page 49 and Figure 24 on page 50 illustrates MX960-PSM-HV (HVAC/HVDC) power supplies for the SRX5800.

Figure 23: MX960-PSM-HV (HVAC/HVDC) Power Supply



Each MX960-PSM-HV (HVAC/HVDC) power supply provides output power of 5100 W. Each power supply has one receptacle, located on the power supply. Do not use the receptacle located on the chassis.

Figure 24: MX960-PSM-HV (HVAC/HVDC) Power Supplies Installed



1– Air exhaust	4– Power supply ejectors
2– Power distribution unit cover	5– Grounding points
3– Power supplies	6– ESD

The minimum number of power supplies must be present in the router at all times. Refer to Table 21 on page 50.

Table 21: Minimum Number of Power Supplies Required for the SRX5800 Firewall

Configuration	Minimum Required Number of Power Supplies	Model Number

HVAC or HVDC	One per zone x two zones = 2 power supplies	MX960-PSM-HV

High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supply LEDs

Each high-voltage second-generation universal (MX960-PSM-HV) power supply faceplate contains three LEDs that indicate the status of the power supply (see Figure 25 on page 51). The power supply status is also reflected in two LEDs on the craft interface In addition, a power supply failure triggers the red alarm LED on the craft interface.

Figure 25: MX960-PSM-HV (HVAC/HVDC) Power Supply LEDs

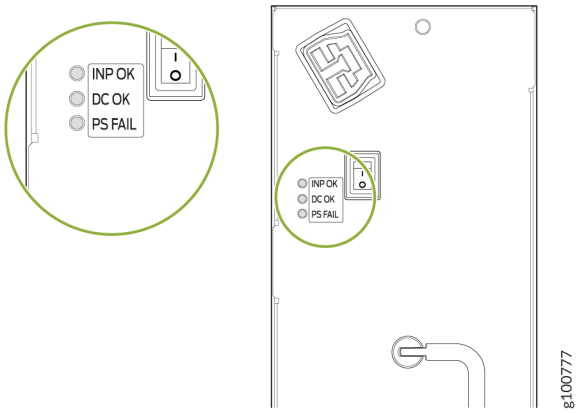


Table 22: MX960-PSM-HV (HVAC/HVDC) Power Supply LEDs

Label	Color	State	Description
INP OK	Green	Off	AC power applied to power supply is not within the normal operating range.
		On	AC power applied to power supply is within the normal operating range.
DC OK	Green	Off	DC power outputs generated by the power supply are not within the normal operating ranges.

Table 22: MX960-PSM-HV (HVAC/HVDC) Power Supply LEDs *(Continued)*

Label	Color	State	Description
		On	DC power outputs generated by the power supply are within the normal operating ranges.
PS FAIL	Red	Off	Power supply is functioning normally.
		On	Power supply is not functioning normally. Check **AC OK** and **DC OK** LEDs for more information.

High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supply Specifications for the SRX5800 Firewall

Table 23 on page 52 lists the MX960-PSM-HV (HVAC or HVDC) power supply electrical specifications.

Table 23: Power Supply Electrical Specifications

Item	Specification
HVAC/HVDC Power Supply	
Maximum output power	5100 W
AC nominal input voltage	Operating range: 200-305 VAC
DC nominal input voltage	200-410 VDC
AC input current rating	30 A maximum
DC input current rating	30 A maximum

Table 23: Power Supply Electrical Specifications *(Continued)*

Item	Specification
Maximum AC inrush current	70 A @ 264 VAC
Maximum DC inrush current	70 A @ 410 VDC

Item	High-voltage Second-Generation Universal Power Supply
Redundancy	2+2
Output power (maximum) per supply	5100 W

High-Voltage Second-Generation Universal (HVAC/HVDC) Power Cord Specifications for the SRX5800 Firewall

The MX960-PSM-HV (HVAC or HVDC) power supplies requires a high current cable assembly when set for 30-A input. One end of the cable has an Anderson APP-400 connector, the other end of the cable is bare wire. See Figure 26 on page 54 and Table 24 on page 54. These cables are separately orderable and are not shipped automatically with MX960-PSM-HV orders. An example of the right-angle cable and connector is shown in Figure 28 on page 55. For connection to AC systems, Juniper provides a cable with either a NEMA 30-A connector (Figure 26 on page 54) or an IEC 330P6W connector (Figure 27 on page 54).

Figure 26: NEMA 30-A Connector

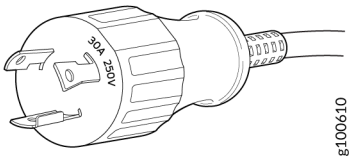
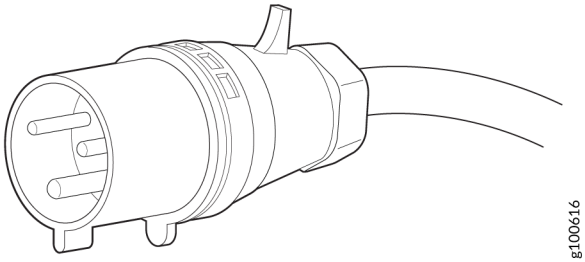


Figure 27: IEC 330P6W Connector



The MX960-PSM-HV (HVAC or HVDC) power supply has one C20 receptacles on front panel of the power supply. The cover needs to be installed to cover C20 receptacles on PDM on top of the chassis. Input receptacle is APP 2007G type from Anderson rated 30 A 400V.

The high voltage alternating current (HVAC), and high voltage direct current (HVDC) have specific cord requirements. Table 24 on page 54 provides specifications and plug standards on the power cord provided for each country or region.

CAUTION: The bend radius for the power cord cables is 7 inches. Avoid bending the cable beyond its bend radius when dressing the cables into the cable channels on the rack.

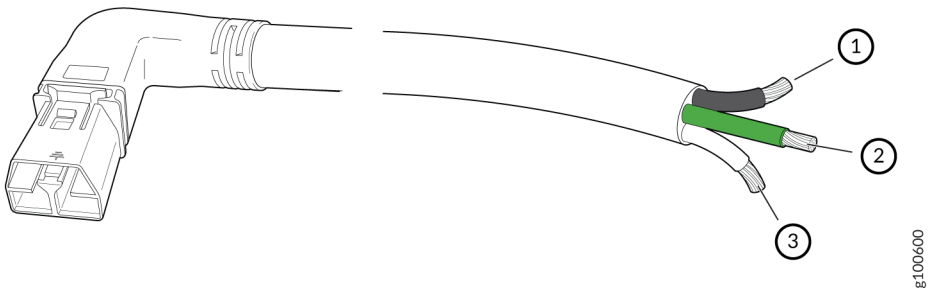
Table 24: 30-A Cabling Options

Spare Juniper Model Number	Locale	Cord Set Rating	Connector
CBL-PWR2-332P6W-RA	Continental Europe AC power cord	30-A 250 VAC	Anderson/right-angle to IEC 332P6

Table 24: 30-A Cabling Options *(Continued)*

Spare Juniper Model Number	Locale	Cord Set Rating	Connector
CBL-PWR2-BARE-RA	North America HVAC/HVDC power cord	30-A, 400 VAC	Anderson/right-angle to bare wire
CBL-PWR-SG4-RA	U.S.A	30-A, 400 VAC	SAF-D-GRID 400 right-angle (LH)
CBL-PWR-SG4	North America AC jumper power cord	30-A, 400 VAC	SAF-D-GRID 400 right-angle (LH)
CBL-PWR2-BARE	North America HVAC/HVDC power cord	30- A, 400 VAC	Anderson/straight to bare wire

Figure 28: Right-Angle, Bare Cable with Anderson Connector



1– Black wire–Positive (+)	3– White wire–Negative
2– Green wire-Ground	

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

WARNING:

注意

附属の電源コードセットはこの製品専用です。
他の電気機器には使用しないでください。

Translation from Japanese: The attached power cable is only for this product. Do not use the cable for another product.

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

WARNING: The router is a pluggable type A equipment installed in restricted access location. It has a separate protective earthing terminal (Metric [–M6] and English [–¼-20] screw ground lugs) provided on the chassis in addition to the grounding pin of the power supply cord. This separate protective earth terminal must be permanently connected to earth.

CAUTION: Power cords and cables must not block access to device components or drape where people could trip on them.

High-Voltage Second-Generation Universal (HVAC/HVDC) Power Circuit Breaker Requirements for the SRX5800 Firewall

The circuit breaker protection on all the power supplies should be designed according to National Electrical Code (NEC) of country of system installation or any similar local standard based on maximum drawn current of the power supply specified in this document.

Each high-voltage universal (MX960-PSM-HV) power supply has a single feed. The input AC or DC receptacle inlet is located on front panel of the power supply.

Each power cord feed should have dedicated circuit breakers. We recommend that size of the circuit breaker protection should be designed according to National Electrical Code (NEC) of country of system installation or any similar local standard based on maximum drawn current of the power supply specified in this document.

CAUTION: Use a 2-pole circuit breaker rated at minimum of 125% of the rated current per NEC or as local codes.

Primary Overcurrent Protection by the Building Circuit Breaker. This breaker must protect against excess current, short circuit, and earth grounding fault in accordance with NEC which is ANSI/NFPA 70.

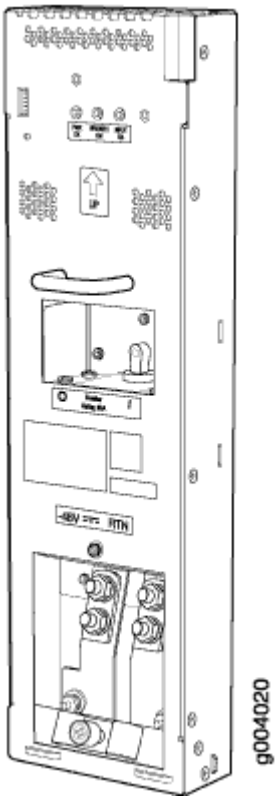
SRX5800 Firewall Standard-Capacity DC Power Supply—SRX5800-PWR-DC

In the DC power configuration, the firewall contains either two or four DC power supplies (see Figure 29 on page 58), located at the lower rear of the chassis in slots **PEM0** through **PEM3** (left to right). You can upgrade your DC power system from two to four power supplies.

Four power supplies provide full redundancy. If a DC power supply fails, its redundant power supply takes over without interruption.

Each DC power supply has a single DC input (–48 VDC and return) that requires a dedicated 80 A (–48 VDC) circuit breaker for the maximum hardware configuration.

Figure 29: Standard-Capacity DC Power Supply



SRX5800 Firewall Standard-Capacity DC Power Supply LEDs

Each standard-capacity DC power supply faceplate contains three LEDs that indicate the status of the power supply (see Table 25 on page 58). The power supply status is also reflected in two LEDs on the craft interface. In addition, a power supply failure triggers the red alarm LED on the craft interface.

Table 25: DC Power Supply LEDs

Label	Color	State	Description
PWR OK	Green	Off	Power supply is not functioning normally. Check the **INPUT OK** LED for more information.
		On	Power supply is functioning normally.

Table 25: DC Power Supply LEDs *(Continued)*

Label	Color	State	Description
BREAKER ON	Green	Off	DC power supply circuit breaker is turned off.
		On	DC power supply circuit breaker is turned on.
INPUT OK	Green	Off	DC input to the PEM is not present.
		On	DC input is present, and is connected in correct polarity.
	Amber	On	DC input is present, but connected in reverse polarity.

SRX5800 Firewall High-Capacity DC Power Supply—SRX5800-PWR-4100-DC

High-capacity DC power supplies (SRX5800-PWR-4100-DC) provide a maximum of 4100 W of power each. Two high-capacity DC power supplies are required, and you can install four high-capacity DC power supplies for redundancy. Each high-capacity DC power supply has inlets for two DC power feeds. The four power connectors (-48V and RTN for each of the two inlets) are located behind a clear plastic cover near the bottom of the power supply. Each DC power inlet you use requires a dedicated DC power feed and a dedicated 80 A circuit breaker. See Figure 30 on page 61.

NOTE: The firewall cannot be powered from standard-capacity and high-capacity DC power supplies simultaneously. The one exception is during the process of replacing standard-capacity DC power supplies with high-capacity DC power supplies, when it is permissible to have both types installed briefly.

NOTE: The high-capacity power supply will operate with only one of its two DC inlets connected to a DC power feed. However, its DC output will be limited to a maximum of 1700 W. We recommend that you connect two DC power feeds to each high-capacity DC power supply.

NOTE: The firewall must be running Junos OS Release 12.1X44-D10 or later in order to use high-capacity DC power supplies.

Each high-capacity DC power supply has an input mode switch, covered by a small metal plate. The input mode switch tells the system the number of DC power feeds it should expect. The input mode switch settings are described in Table 26 on page 60. The default setting is 1.

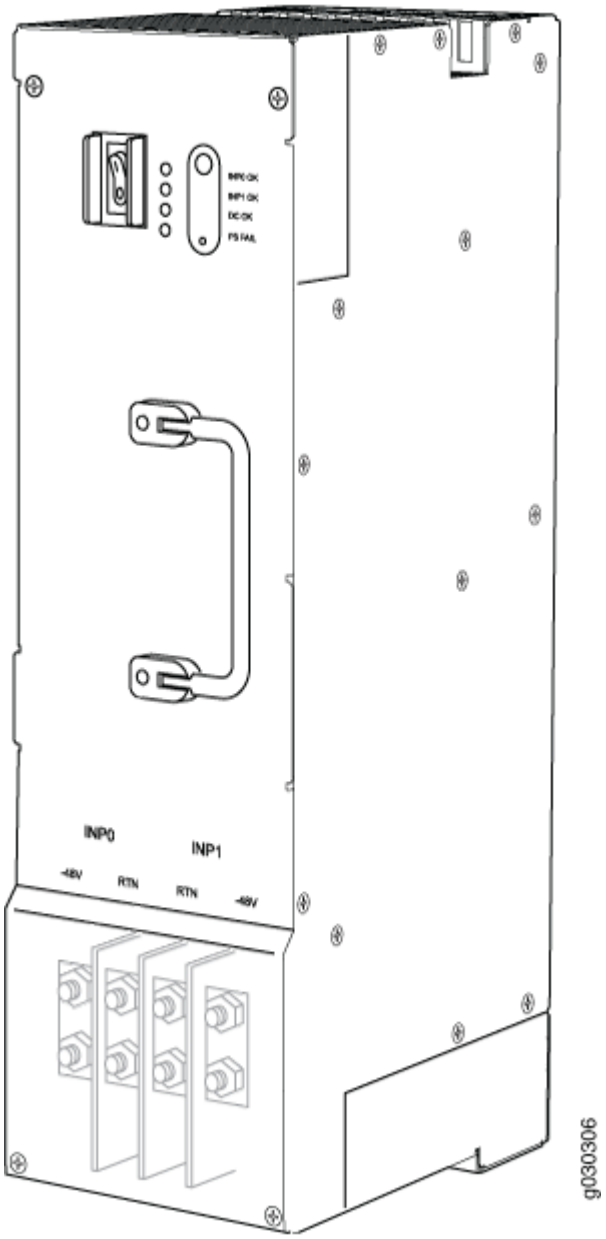
Table 26: High-Capacity DC Power Supply Input Mode Switch Settings

Mode Switch Setting	DC Inputs	Result
1	Both DC inlets powered	DC output of 4100 W **DC OK** LED lights
	Only one DC inlet powered	DC output of 1700 W **DC OK** LED unlit
0	Both DC inlets powered	DC output of 4100 W **DC OK** LED lights
	Only one DC inlet powered	DC output disabled **DC OK** LED unlit

NOTE: We recommend that you set the input mode switch to **1** and connect two DC input feeds to each high-capacity DC power supply.

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, the firewall chassis must be adequately grounded before power is connected. See "Grounding the SRX5800 Firewall" on page 252 for instructions.

Figure 30: High-Capacity DC Power Supply



SRX5800 Firewall High-Capacity DC Power Supply LEDs

Each high-capacity DC power supply faceplate contains four LEDs that indicate the status of the power supply (see Table 27 on page 62). The power supply status is also reflected in two LEDs on the craft interface. In addition, a power supply failure triggers the red alarm LED on the craft interface.

Table 27: High-Capacity DC Power Supply LEDs

Label	Color	State	Description
INP0 OK	Green	Off	DC power applied to the power supply at input INP0 is not within the normal operating range.
		On	DC power applied to the power supply at input INP0 is within the normal operating range.
INP1 OK	Green	Off	DC power applied to the power supply at input INP1 is not within the normal operating range.
		On	DC power applied to the power supply at input INP1 is within the normal operating range.
DC OK	Green	Off	DC power outputs generated by the power supply are not within the normal operating ranges.
		On	DC power outputs generated by the power supply are within the normal operating ranges.
PS FAIL	Red	Off	Power supply is functioning normally.
		On	Power supply is not functioning normally. Check the **INP0 OK**, **INP1 OK**, and **DC OK** LEDs for more information.

SRX5800 Firewall DC Power Supply Specifications

Table 28 on page 63 lists the DC power supply electrical specifications.

Table 28: DC Power Supply Electrical Specifications

Item	Standard-Capacity	High-Capacity	
		Two-Feed Mode	One-Feed Mode
Maximum output power	2800 W	4100 W	1700 W
DC input voltage	Nominal: –48 VDC Operating range: –40 to –72 VDC	Nominal: –48 VDC Operating range: –40 to –72 VDC	Nominal: –48 VDC Operating range: –40 to –72 VDC
Maximum input current rating @ 40 VDC	70 A	128 A for both feeds (66 A and 62 A per feed)	52 A
DC nominal input current rating @48 VDC	58 A maximum@–48 VDC (nominal)	104 A for both feeds (54 A and 50 A per feed)	42 A
Efficiency	99%	86%	
	NOTE: This value is at full load and nominal voltage.		
Internal Circuit Breaker	80 A	–	–

Table 29 on page 63 lists the power system electrical specifications.

Table 29: Power System Electrical Specifications

Item	Normal-Capacity	High-Capacity	
Redundancy	2+2	2+2	
Output power (maximum) per supply	2800 W	Two-feed mode	One-feed mode

Table 29: Power System Electrical Specifications *(Continued)*

Item	Normal-Capacity	High-Capacity	
		4100 W	1700 W
Output power (maximum) per system	5600 W	8200 W	3400 W

DC Power Cable Specifications for the SRX5800 Firewall

Table 30 on page 64 summarizes the specifications for the power cables, which you must supply.

Table 30: DC Power Cable Specifications

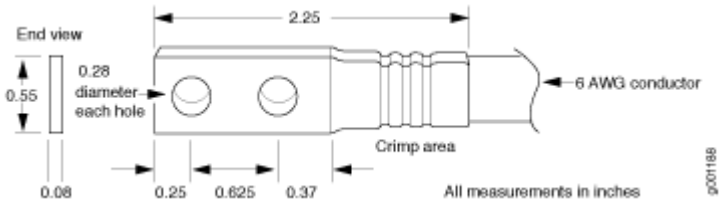
Cable Type	Quantity	Specification
Power	Four 6-AWG (13.3 mm^2) cables for each power supply	Minimum 60°C wire, or as required by the local code

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

DC Power Cable Lug Specifications for the SRX5800 Firewall

The accessory box shipped with the firewall includes the cable lugs that attach to the terminal studs of each power supply (see Figure 31 on page 65).

Figure 31: DC Power Cable Lug



CAUTION: Before firewall installation begins, a licensed electrician must attach a cable lug to the grounding and power cables that you supply. A cable with an incorrectly attached lug can damage the firewall.

WARNING: The firewall is a pluggable type A equipment installed in restricted access location. It has a separate protective earthing terminal [Metric -M6 and English - ¼-20 screw) ground lugs] provided on the chassis. This separate protective earth terminal must be permanently connected to earth.

DC Power Circuit Breaker Requirements for the SRX5800 Firewall

If you plan to operate a maximally configured DC-powered firewall with standard-capacity power supplies, we recommend that you provision at least 116 A (58 A per feed) @ –48 VDC (nominal) for the system. Use a customer site circuit breaker rated according to respective National Electrical Code and customer site internal standards to maintain proper level of protection for the current specified above.

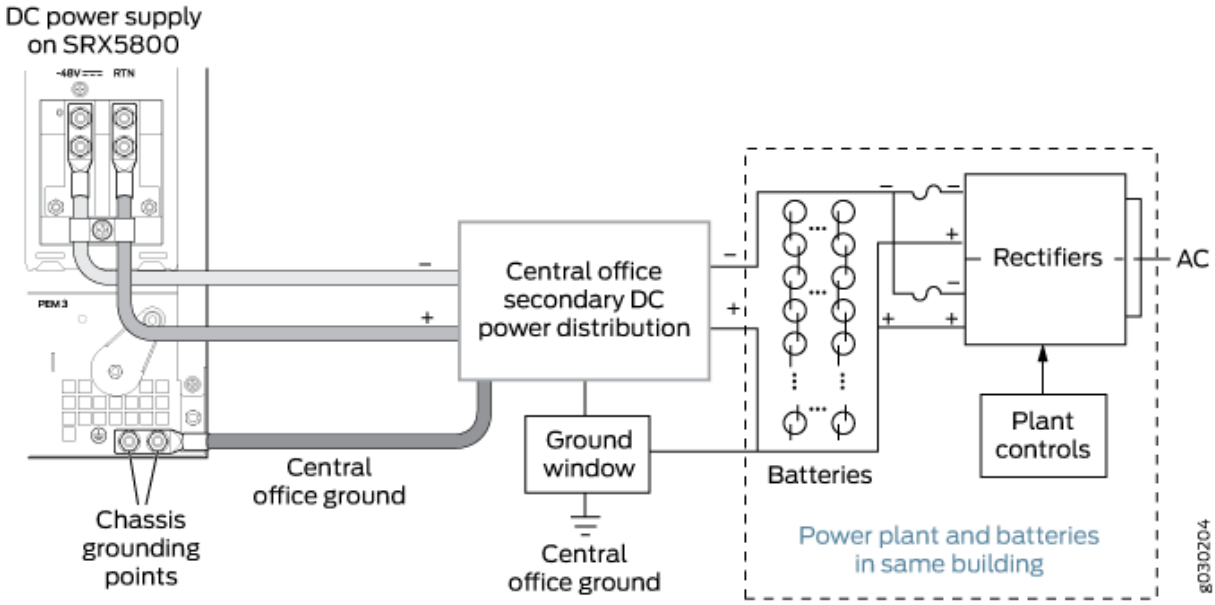
If you plan to operate a maximally configured DC-powered firewall with high-capacity power supplies, we recommend that you provision at least 208 A (104 A per supply) @ –48 VDC (nominal) for the system. This is maximum current draw at –48 VDC when two power supplies are providing the power to the system and the redundant power supplies are not supplying power or not present. Use a customer site circuit breaker rated according to respective National Electrical Code and customer site internal standards to maintain proper level of protection for the current specified above.

If you plan to operate a DC-powered firewall at less than the maximum configuration, we recommend that you provision a circuit breaker according to respective National Electrical Code and customer site internal standards to maintain proper level of protection for the current specified above or each DC power supply rated for at least 125% of the continuous current that the system draws at –48 VDC.

DC Power Source Cabling for the SRX5800 Firewall

Figure 32 on page 66 shows a typical DC source cabling arrangement.

Figure 32: Typical DC Source Cabling to the Firewall



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.

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

WARNING: For field-wiring connections, use copper conductors only.

CAUTION: Power cords and cables must not block access to device components or drape where people could trip on them.

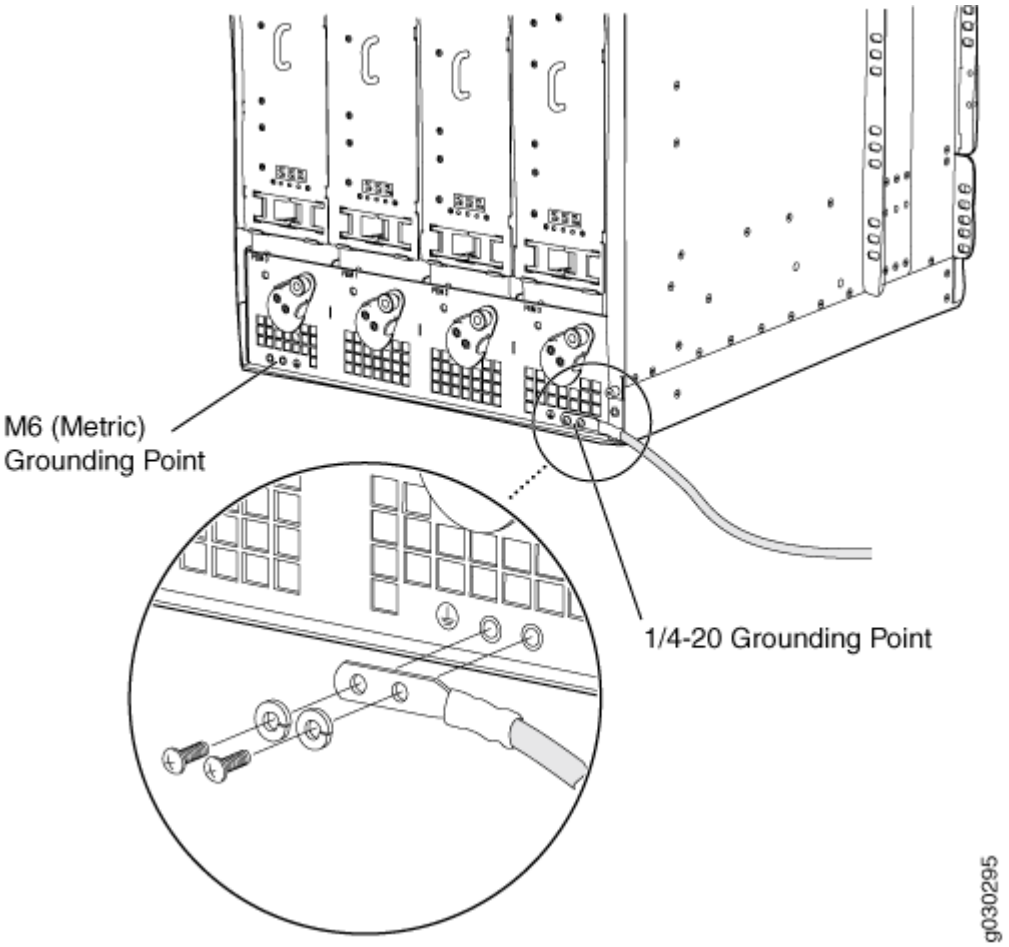
SRX5800 Firewall Chassis Grounding Point Specifications

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power. See "Grounding the SRX5800 Firewall" on page 252 for instructions.

CAUTION: Before firewall installation begins, a licensed electrician must attach cable lugs to the grounding and power cables that you supply. A cable with an incorrectly attached lug can damage the firewall.

The firewall chassis has two grounding points along the lower edge of the back panel. Each grounding point consists of two threaded holes spaced 0.625-in. (15.86-mm) apart (see Figure 33 on page 68). The left grounding point fits M6 screws (European), and the right grounding point fits UNC 1/4–20 screws (American). The accessory box shipped with the firewall includes the cable lug that attaches to the grounding cable and two UNC 1/4–20 screws used to secure the grounding cable to the right-side grounding point on the firewall.

Figure 33: SRX5800 Firewall Chassis Grounding Points



To ground the firewall, you must connect a grounding cable to earth ground and then attach it to the chassis grounding point using the two screws provided.

NOTE: Additional grounding is provided to an AC-powered firewall when you plug its power supplies into grounded AC power receptacles.

SRX5800 Firewall Grounding Cable Specifications

The grounding cable that you provide must meet the specifications in Table 31 on page 69.

Table 31: Grounding Cable Specifications

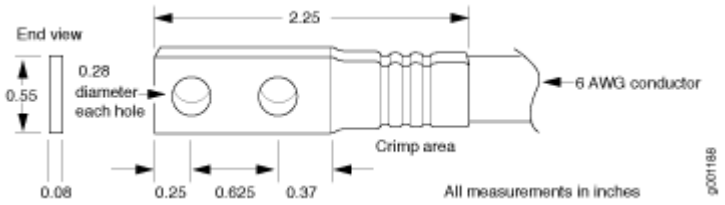
Cable Type	Quantity and Specification
Grounding	One 6-AWG (13.3 mm^2), minimum 60°C wire, or as required by the local code

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power. See "Grounding the SRX5800 Firewall" on page 252 for instructions.

SRX5800 Firewall Grounding-Cable Lug Specification

The accessory box shipped with the firewall includes the cable lug that attaches to the grounding cable (see Figure 34 on page 69) and two UNC 1/4–20 screws used to secure the grounding cable to the grounding points.

Figure 34: Grounding Cable Lug



CAUTION: Before firewall installation begins, a licensed electrician must attach a cable lug to the grounding and power cables that you supply. A cable with an incorrectly attached lug can damage the firewall.

NOTE: The same cable lug is used for the DC power cables.

SRX5800 Host Subsystem

IN THIS SECTION

SRX5800 Firewall Host Subsystem Description

The host subsystem is composed of a Routing Engine installed in a Switch Control Board (SCB). The host subsystem provides the routing and system management functions of the firewall. You must install one host subsystem on the device. The host subsystem components are as follows:

- Switch Control Board
  - SRX5K-SCB–from Junos OS Release 9.2 to 12.3X48
  - SRX5K-SCBE–from Junos OS Release 12.1X47-D15 and later
  - SRX5K-SCB3–from Junos OS Release 15.1X49-D10 and later
  - SRX5K-SCB4–from Junos OS Release 19.3R1 and later

NOTE: SRX5K-SCB4 is not supported on SRX5400 Firewalls.

- Routing Engine
  - SRX5K-RE-13-20–from Junos OS Release 9.2 to 12.3X48
  - SRX5K-RE-1800X4–from Junos OS Release 12.1X47-D15 and later
  - SRX5K-RE3-128G–from Junos OS Release 19.3R1 and later

NOTE: You can only configure the following combination of Routing Engine and SCB within a host subsystem:

- SRX5K-RE-13-20 and SRX5K-SCB
- SRX5K-RE-1800X4 and SRX5K-SCBE
- SRX5K-RE-1800X4 and SRX5K-SCB3
- SRX5K-RE-1800X4 and SRX5K-SCB4
- SRX5K-RE3-128G and SRX5K-SCB3 or SRX5K-SCB4

The host subsystem has three LEDs that display its status. The host subsystem LEDs are located in the middle of the craft interface.

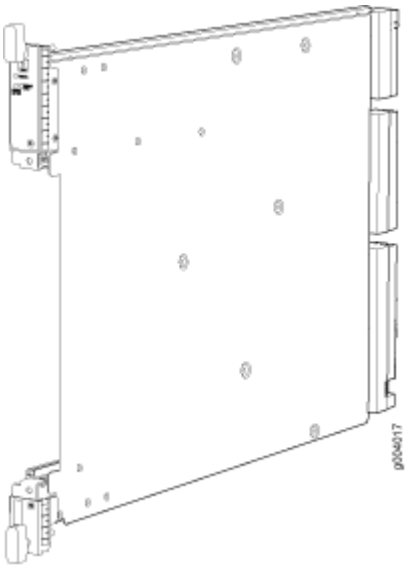
Switch Control Board SRX5K-SCB Overview

The Switch Control Board (SCB) provides the following functions:

- Powers on and powers off IOCs and SPCs
- Controls clocking, system resets, and booting
- Monitors and controls system functions, including fan speed, board power status, PDM status and control, and the system front panel
- Provides interconnections to all the IOCs within the chassis through the switch fabrics integrated into the SCB

When the SCB is part of a host subsystem, the Routing Engine installs directly into a slot on the SCB (see Figure 35 on page 72).

Figure 35: SRX5K-SCB



The SRX5800 Firewall has two SCBs installed and you can install a third SCB for switch fabric redundancy.

NOTE: The SRX5800 Firewall supports a redundant SCB, provided the SCB is a SRX5K-SCBE (SCB2) running Junos OS Release 12.1X47-D15 and later, SRX5K-SCB3 (SCB3) running Junos OS Release 15.1X49-D10 and later, or a SRX5K-SCB4 (SCB4) running Junos OS Release 19.3R1 and later.
The SRX5800 Firewall does not support a redundant SCB (third SCB) card if SRX5K-SPC-4-15-320 (SPC2) is installed with SCB1 (SRX5K-SCB). If you have installed a SPC2 on a SRX5800 Firewall with a redundant SCB1 card, make sure to remove the redundant SCB1 card.

SCBs install vertically into the front of the chassis. The SCB slots are located at the middle of the card cage and are labeled **0**, **1**, and **2/6**. If any slots are empty, you must install a blank panel.

SCBs installed in slots **0** and **1** provide nonredundant fabric connections. A SCB installed in slot **2/6**, in conjunction with SCBs in slots **0** and **1**, provides redundant fabrics. If no SCB is installed in slot **2/6**, you must install a blank panel in the slot (see Table 32 on page 73).

Table 32: SCB Slot Mapping and Functionality

Functionality	Slot **0**	Slot **1**	Slot **2/6**
Full fabric	SCB Routing Engine	SCB	–
Redundant fabric	SCB Routing Engine	SCB	SCB

For detailed information about SCBs supported by the SR5800 Firewall, see the *SRX5400, SRX5600, and SRX5800 Firewall Card Guide* at www.juniper.net/documentation/.

Switch Control Board SRX5K-SCB Specifications

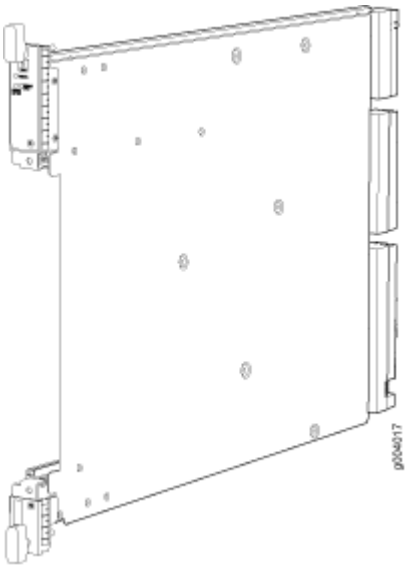
The SRX5K-SCB Switch Control Board (SCB) (Figure 36 on page 74) performs the following functions:

- Powers on and powers off I/O cards (IOCs) and Services Processing Cards (SPCs)
- Controls clocking, system resets, and booting
- Monitors and controls system functions, including fan speed, board power status, PDM status and control, and the system front panel
- Provides interconnections to all the IOCs within the chassis through the switch fabrics integrated into the SCB

SRX5400 and SRX5600 Firewalls have one SCB each installed and you can install a second SCB for redundancy. The SRX5800 Firewall has two SCBs installed and you can install a third SCB for switch fabric redundancy.

The host subsystem is composed of a Routing Engine installed directly into a slot on the faceplate of the SCB. When there is no Routing Engine is a SCB, its slot must be covered with a blank panel.

Figure 36: Switch Control Board SRX5K-SCB



Each SCB consists of the following components:

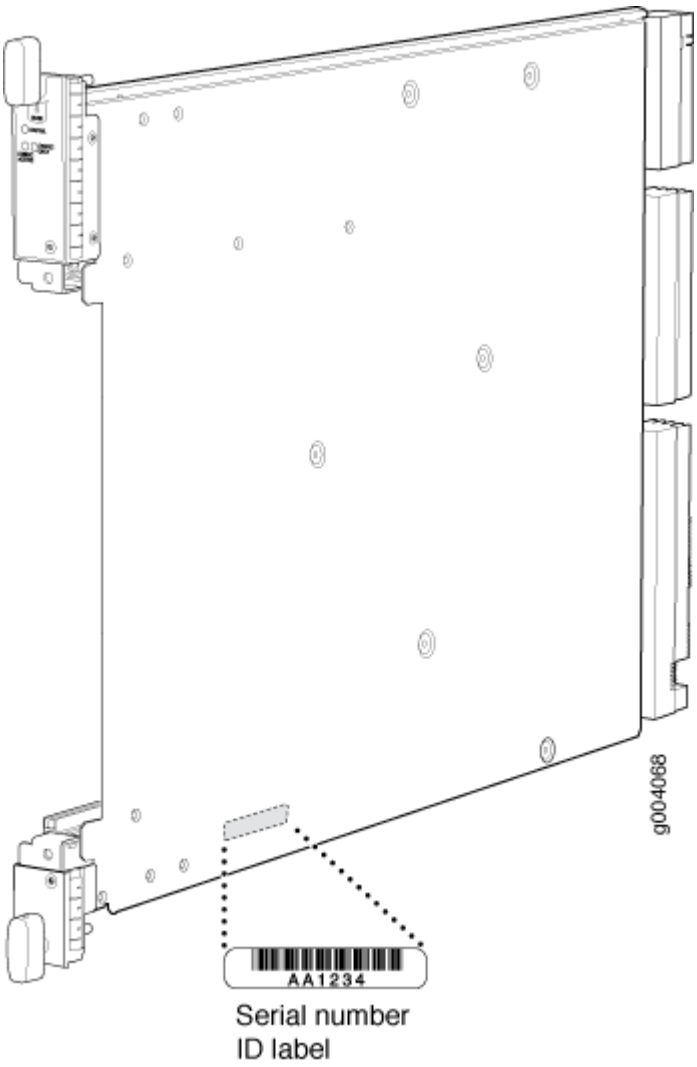
- Chassis management Ethernet switch.
- I2C bus logic, used for low-level communication with each component.
- Component redundancy circuitry.
- Gigabit Ethernet switch that is connected to the embedded CPU complex on all components.
- Switch fabric—Provides the switching functions for the IOCs.
- Control FPGA—Provides the Peripheral Component Interconnect (PCI) interface to the Routing Engine.
- 1000Base-T Ethernet controller—Provides a 1-Gbps Ethernet link between the Routing Engines.
- Ethernet switch—Provides 1-Gbps link speeds between the Routing Engine and the IOCs.
- Circuits for chassis management and control.
- Power circuits for the Routing Engine and SCB.

Description	• SCB with slot for Routing Engine • Maximum throughput: 75 Gbps per slot

Software release	• Junos OS Release 9.2 and later
Cables and connectors	Slot for Routing Engine
Controls	None
Supported Slots	• SRX5400–Only bottom slots **0** and **1/0** • SRX5600–Only bottom slots **0** and **1** • SRX5800–Only center slots **0**, **1**, and **2/6**
Power Requirement	150 W
Weight	Approximately 10 lb (4.5 kg)
LEDs	**OK/FAIL** LED, one bicolor: • Green–The SCB is operating normally. • Red–The SCB has failed and is not operating normally. • Off–The SCB is powered down. **FABRIC ONLY** LED: • Green–The SCB is operating in fabric-only mode. • Off–The SCB is operating in fabric/control board mode. **FABRIC ACTIVE** LED: • Green–The fabric is in active mode.

Serial Number Location — The serial number label is located as shown in Figure 37 on page 76.

Figure 37: SCB Serial Number Label



Switch Control Board SRX5K-SCBE Overview

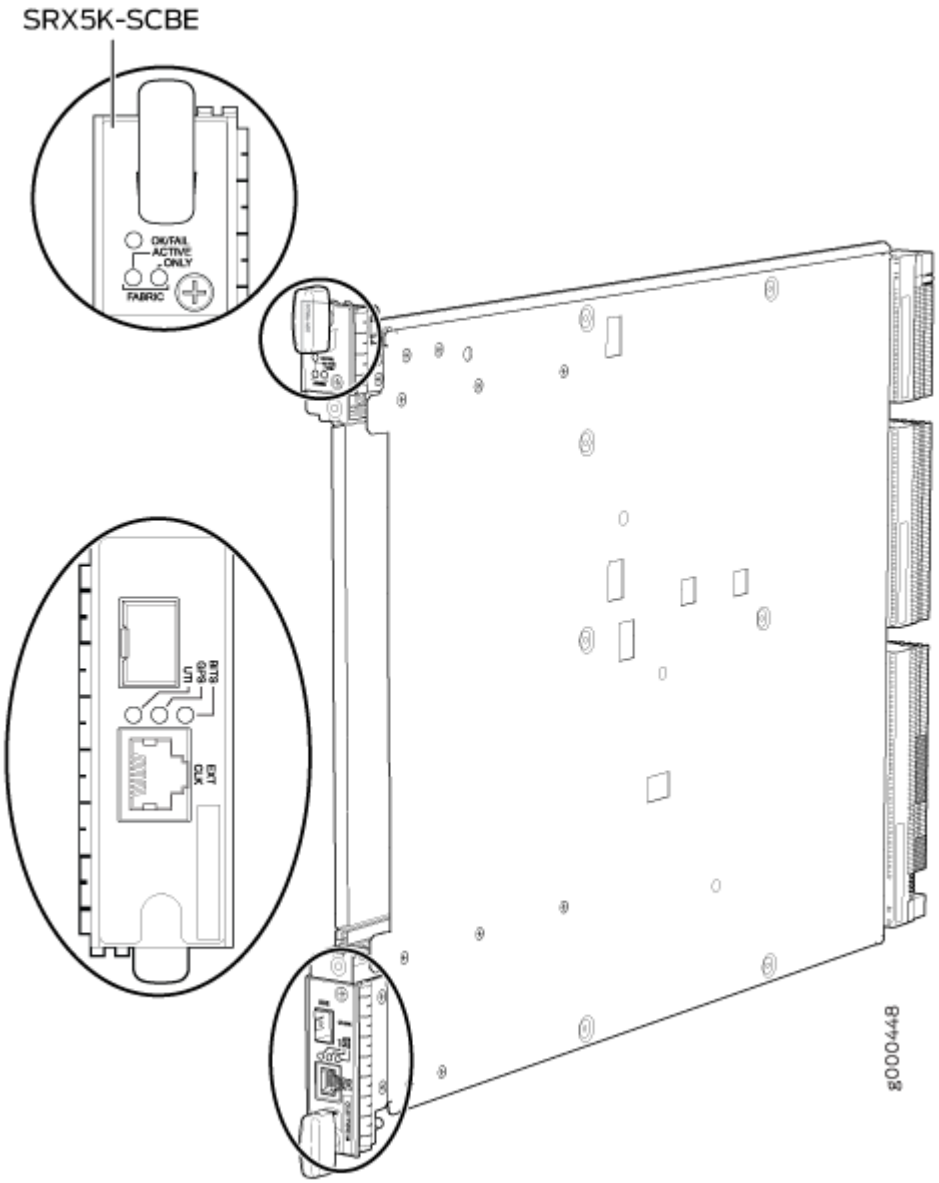
The SRX5000 line enhanced Switch Control Board (SRX5K-SCBE) caters to high-end security markets requiring support for higher capacity traffic. The SRX5K-SCBE provides greater interface density (slot and capacity scale) and improved services.

Some key attributes of the SRX5K-SCBE are:

- A bandwidth of 120 Gbps per slot with redundant fabric support and improved fabric performance by using the next-generation fabric (XF) chip.
- A centralized clocking architecture that supports clock cleanup and distribution. The Stratum 3 clock module performs clock monitoring, filtering, and holdover in a centralized chassis location.
- Full performance with fabric redundancy for higher capacity line cards such as the SRX5K-MPC.

The Routing Engine installs directly into a slot on the SRX5K-SCBE as shown in Figure 38 on page 78.

Figure 38: SRX5K-SCBE



Switch Control Board SRX5K-SCBE Specifications

IN THIS SECTION

- SRX5K-SCBE LEDs | **80**

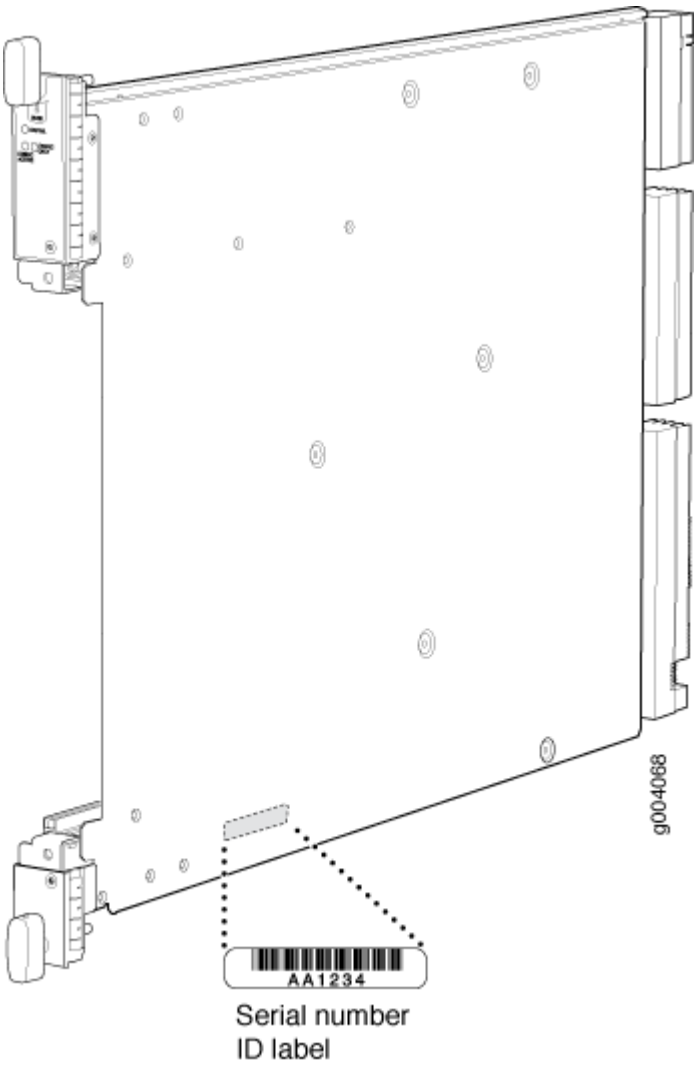
Each SRX5K-SCBE consists of the following components:

- I2C bus logic for low-level communication with each component
- Component redundancy circuitry
- Control Board/Routing Engine primary-role mechanism
- Gigabit Ethernet switch that is connected to the embedded CPU complex on all components
- Switch fabric to provide the switching functions for the MPCs
- 1000BASE-T Ethernet controller to provide a 1-Gbps Ethernet link between the Routing Engines
- Power circuits for the Routing Engine and the SRX5K-SCBE
- LEDs—Provides status of the SRX5K-SCBE and clocking interface

Description	• SRX5K-SCBE with slot for Routing Engine • Maximum throughput: 120 Gbps per slot
Software release	Junos OS Release 12.1X47-D15 and later
Cables and connectors	Slot for Routing Engine
Controls	None
Supported slots	• SRX5400–Only bottom slots **0** and **1/0** • SRX5600–Only bottom slots **0** and **1** • SRX5800–Only center slots **0**, **1**, and **2/6**
Power requirement	• 160 W at 131° F (55° C) • 130 W at 104° F (40° C) • 120 W at 77° F (25° C)
Weight	9.6 lb (4.4 kg) with Routing Engine

Serial number location	The serial number label is located as shown in Figure 39 on page 80.

Figure 39: SRX5K-SCBE Serial Number Label



SRX5K-SCBE LEDs

Table 33 on page 81 describes the SRX5K-SCBE LEDs and their states.

Table 33: SRX5K-SCBE LEDs

Label	Color	State	Description
FABRIC ACTIVE	Green	On steadily	Fabric is in active mode.
FABRIC ONLY	Green	On steadily	SRX5K-SCBE operates in fabric-only mode.
	None	Off	SRX5K-SCBE operates in fabric/control board mode.
OK/FAIL	Green	On steadily	SRX5K-SCBE is online.
	Red	On steadily	SRX5K-SCBE has failed.
	None	Off	SRX5K-SCBE is offline.

Switch Control Board SRX5K-SCB3 Overview

The SRX5K-SCB3 (SCB3) caters to high-end security markets requiring support for higher capacity traffic, greater interface density (slot and capacity scale), and improved services. The SCB3 is supported on SRX5400, SRX5600, and SRX5800 Firewalls.

The SCB3 supports the standard midplane and the enhanced midplane.

Some key attributes of the SCB3 are:

- With the existing midplane and fabric link speed of 8.36 Gbps, supports a bandwidth of 205 Gbps per slot with redundant fabric support and 308 Gbps per slot without redundancy.
- With the enhanced midplane and fabric link speed of 10.2 Gbps, supports a bandwidth of 249 Gbps per slot with redundant fabric support and 374 Gbps per slot without redundancy with the enhanced midplane
- Improved fabric performance with the next-generation fabric (XF2) chip.
- Full performance with fabric redundancy for higher-capacity line cards.

- Support for MPC line cards such as SRX5K-MPC (IOC2), IOC3 (SRX5K-MPC3-40G10G or SRX5K-MPC3-100G10G), and IOC4 (SRX5K-IOC4-10G or SRX5K-IOC4-MRAT).
- Two 10-Gigabit Ethernet SFP+ ports (These ports are disabled and reserved for future use).

The Routing Engine installs directly into a slot on the SCB3, as shown in Figure 40 on page 82.

Figure 40: SRX5K-SCB3

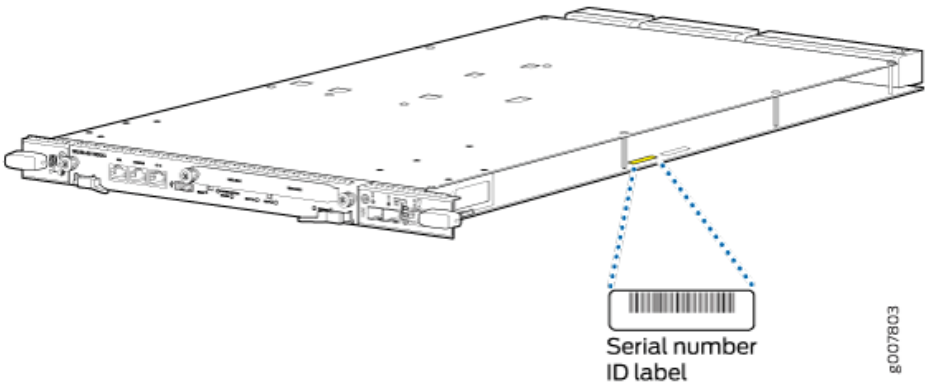
Switch Control Board SRX5K-SCB3 Specifications

IN THIS SECTION

Each SRX5K-SCB3 (SCB3) consists of the following components:

- I2C bus logic for low-level communication with each component
- Component redundancy circuitry
- Control Board/Routing Engine primary-role mechanism
- Gigabit Ethernet switch that is connected to the embedded CPU complex on all components
- Switch fabric to provide the switching functions for the MPCs
- Control field-programmable gate array (FPGA) to provide the Peripheral Component Interconnect (PCI) interface to the Routing Engine
- Circuits for chassis management and control
- Power circuits for the Routing Engine and SCB3

- LEDs to provides status of the SCB3

Description	SCB3 with slot for Routing Engine
Software release	Junos OS Release 15.1X49-D10 and later
Cables and connectors	Slot for Routing Engine
Controls	None
Supported slots	• SRX5400–Only bottom slots **0** and **1/0** • SRX5600–Only bottom slots **0** and **1** • SRX5800–Only center slots **0**, **1**, and **2/6**
Power requirement	300 W
Weight	9.6 lb (4.4 kg) with Routing Engine
Serial number location	The serial number label is located as shown in Figure 41 on page 83. **Figure 41: SRX5K-SCB3 Serial Number Label** 

SRX5K-SCB3 LEDs

Table 34 on page 84 describes the SCB3 LEDs and their states.

Table 34: SRX5K-SCB3 LEDs

Label	Color	State	Description
FABRIC ACTIVE	Green	On steadily	Fabric is in active mode.
OK/FAIL	Green	On steadily	SCB3 is online.
	Red	On steadily	SCB3 has failed.
	–	Off	SCB3 is offline.
LINK	Green	On steadily	Port is enabled and link is established.
	–	Off	Port is disabled or no link is established.

Switch Control Board SRX5K-SCB4 Overview

The SRX5K-SCB4 (SCB4) Enhanced Switch Control Board provides improved fabric performance and bandwidth capabilities for high-capacity line cards using the ZF-based switch fabric. The SCB4 is supported on SRX5600 and SRX5800 Firewalls, but not supported on SRX5400 Firewalls.

The SCB4 supports the standard and the enhanced midplane.

Some key attributes of the SCB4 are:

- With the SRX5K-SCB4 Switch Control Board, Increased Fabric Bandwidth mode is the default mode on the SRX5600 and SRX5800 Firewalls and the firewalls will use six active planes without any spare planes.
- With the Redundant Fabric mode, the SRX5600 and SRX5800 Firewalls will use four active planes and will have two spare planes.
- SRX5K-SCB4, with fabric link speed of 19 Gbps enables:

  - 480 Gbps throughput per slot with enhanced midplane and fabric redundancy
  - 720 Gbps throughput per slot with enhanced midplane and without fabric redundancy
- Two 10-Gigabit Ethernet SFP+ ports (These ports are disabled and reserved for future use).

Increased Fabric Bandwidth mode is the default fabric mode of SCB4. In this mode you must install two SCB4s in SRX5600 and three SCB4s in SRX5800 Firewalls/Chassis clusters.

You can change the fabric mode of SCB4 from Increased Fabric Bandwidth mode to Redundant Fabric mode using the CLI. If you change the fabric mode of SCB4 to Redundant Fabric mode you must install two SCB4s in SRX5600 and you can install either two or three SCB4s in SRX5800 Firewalls.

If you are upgrading from SCB3 (Redundant Fabric mode is the default fabric mode in SCB2 and SCB3) to SCB4 and installing only two SCB4s, you must have Junos OS 19.3R1 or later and change the default fabric mode of SCB4s to Redundant Fabric mode by using the CLI.

NOTE: To achieve maximum throughput on an SRX5800 Firewall, you must configure the firewall with 3x IOC4 + 7x SPC3 + 2x RE3 and only 2x SCB4s (configured in redundant fabric mode). This configuration makes your firewall fullyloaded with still two empty slots in the chassis. You must not install additional line cards or a third SCB in the empty slots. If you install a third SCB or an additional line card, the chassis will hit chassis power limit and one of the line cards will go offline due to power shortage.

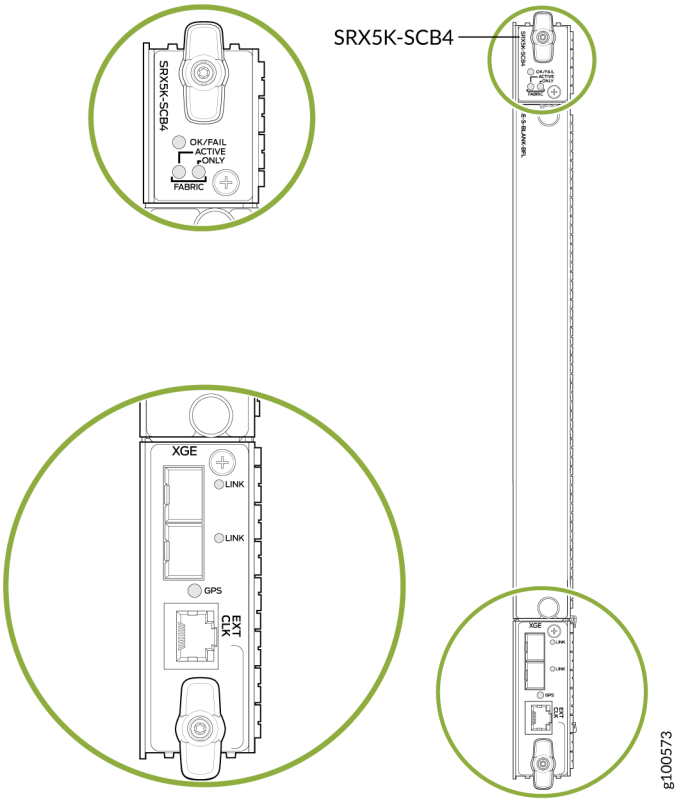
You can change the fabric mode by following one of these two methods:

1. Use the CLI command `request chassis fabric mode <increased-bandwidth|redundant-fabric>`
2. Save the change in the Configuration file

```
set chassis fabric redundancy-mode increased-bandwidth
set chassis fabric redundancy-mode redundant
```

The Routing Engine installs directly into a slot on the SCB4, as shown in Figure 42 on page 86.

Figure 42: SRX5K-SCB4



Switch Control Board SRX5K-SCB4 Specifications

IN THIS SECTION

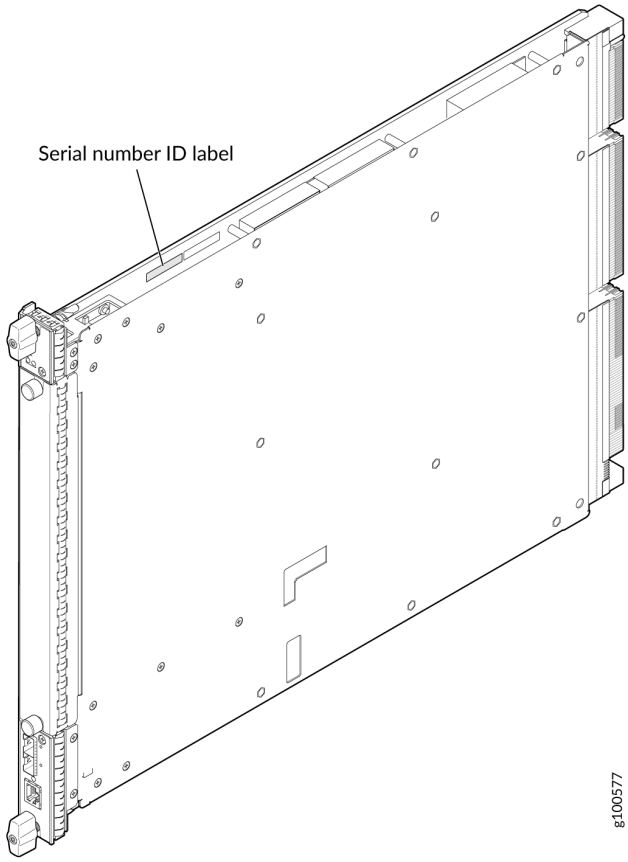
SRX5K-SCB4 (SCB4) consists of the following components:

- LEDs to provides status of the SCB4.
- Circuits for chassis management and control.
- Power circuits for the Routing Engine and SCB4.

Description	SCB4 with slot for SRX5K-RE-1800X4 and SRX5K-RE3-128G Routing Engines
Software release	Junos OS Release 19.3R1 and later
Cables and connectors	Slot for Routing Engine
Controls	None
Supported slots	• SRX5400–Not supported • SRX5600–Only bottom slots **0** and **1** • SRX5800–Only center slots **0**, **1**, and **2/6**
Power requirement	At different temperatures: • 55° C: 425 W • 40° C: 400 W • 25° C: 385 W
Cooling requirement	For efficient and reliable power and cooling, you must install SRX Series high-capacity power supplies and fan trays in the SRX Series chassis.
Weight and Dimensions	• Weight: 13.6 lb (6.2 kg) • Width: 15.7 in (39.87 cm) • Depth: 21.2 in (53.85 cm) • Height: 1.2 in (3.05 cm)

Serial number location	The serial number label is located as shown in Figure 43 on page 88.

Figure 43: SRX5K-SCB4 Serial Number Label



SRX5K-SCB4 LEDs

Table 35 on page 88 describes the SCB4 LEDs and their states.

Table 35: SRX5K-SCB4 LEDs

Label	Color	State	Description
OK/FAIL	Green	On steadily	SCB4 is online.

Table 35: SRX5K-SCB4 LEDs *(Continued)*

Label	Color	State	Description
	Red	On steadily	SCB4 has failed.
	–	Off	SCB4 is offline.
FABRIC			
ACTIVE	Green	On steadily	The switch fabric on this board is in Active mode.
ONLY	Green	On steadily	The switch is in Fabric-Only mode.
LINK (XGE port)	Green	On steadily	SFP+ port is enabled and link is established.
	–	Off	SFP+ port is disabled or no link is established.
GPS	Green	On steadily	Indicates the status of the GPS clocking interface, and the link is OK.
	Yellow	Blinking	Activity on the clocking interface.

Routing Engine SRX5K-RE-13-20 Overview

The Routing Engine is an Intel-based PC platform that runs Junos OS. Software processes that run on the Routing Engine maintain the routing tables, manage the routing protocols used on the device, control the device interfaces, control some chassis components, and provide the interface for system management and user access to the device.

You must install at least one Routing Engine in the firewall. You can install a second Routing Engine if both Routing Engines are running Junos OS Release 10.0 or later.

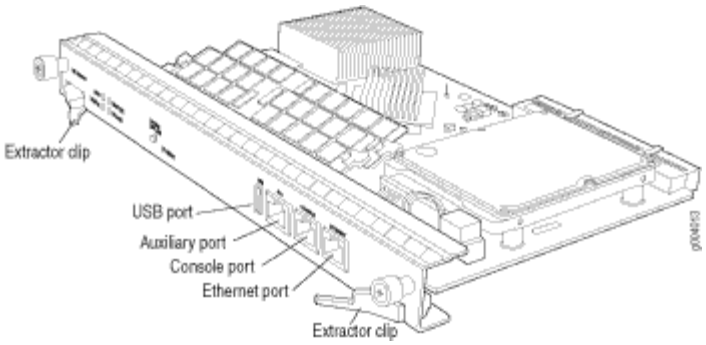
A second Routing Engine is required if you are using the dual chassis cluster control link feature available in Junos OS Release 10.0 and later. The second Routing Engine does not perform all the functions of a Routing Engine and does not improve resiliency or redundancy. The second Routing Engine and the Switch Control Board (SCB) in which it is installed do not constitute a host subsystem. The only function

of the second Routing Engine is to enable the hardware infrastructure that enables the **Chassis Cluster Control 1** port on the Services Processing Card (SPC) used for chassis cluster control links.

If you install only one Routing Engine in the firewall, you must install it in the slot in the front panel of SCB0. If you install a second Routing Engine to use the dual chassis cluster control link feature, you install it in the slot in the front panel of SCB1 (see Figure 44 on page 90).

A USB port on the Routing Engine accepts a USB memory card that allows you to load Junos OS.

Figure 44: SRX5K-RE-13-20 Routing Engine

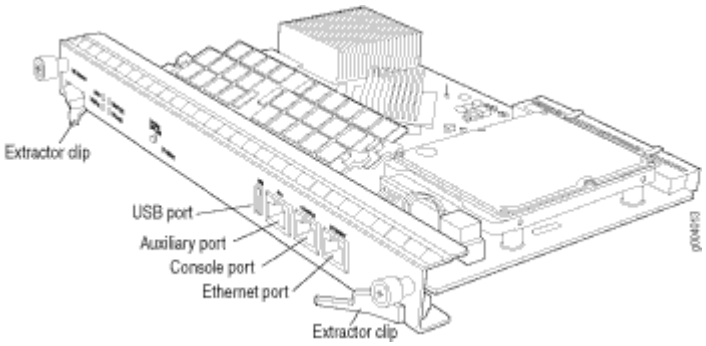


For detailed information about the Routing Engines supported by the firewall, see the *SRX5400, SRX5600, and SRX5800 Firewall Card Reference* at www.juniper.net/documentation/.

Routing Engine SRX5K-RE-13-20 Specifications

The SRX5K-RE-13-20 Routing Engine (Figure 45 on page 91) is an Intel-based PC platform that runs the Junos operating system (Junos OS). Software processes that run on the Routing Engine maintain the routing tables, manage the routing protocols used on the device, control the device interfaces, control some chassis components, and provide the interface for system management and user access to the device.

Figure 45: Routing Engine



You must install at least one Routing Engine in the firewall. You can install a second Routing Engine if both Routing Engines are running Junos OS Release 10.0 or later. A second Routing Engine is required if you are using the dual chassis cluster control link feature available in Junos OS Release 10.0 and later. The second Routing Engine does not perform all the functions of a Routing Engine and does not improve resiliency or redundancy. The second Routing Engine and the Switch Control Board (SCB) in which it is installed do not constitute a host subsystem. The only function of the second Routing Engine is to enable the hardware infrastructure that enables the chassis cluster control 1 port on the Services Processing Card (SPC) used for chassis cluster control links. If you install only one Routing Engine in the firewall, you must install it in the slot in the front panel of SCB0. If you install a second Routing Engine to use the dual chassis cluster control link feature, you install it in the slot in the front panel of SCB1.

The Routing Engine consists of the following components:

- CPU—Runs Junos OS to maintain the firewall's routing tables and routing protocols. It has a Pentium-class processor.
- DRAM—Provides storage for the routing and forwarding tables and for other Routing Engine processes.
- USB port—Provides a removable media interface through which you can install Junos OS manually. Junos supports USB version 1.0.
- Internal flash disk—Provides primary storage for software images, configuration files, and microcode. The disk is a fixed compact flash and is inaccessible from outside the firewall.
- Hard disk—Provides secondary storage for log files, memory dumps, and rebooting the system if the internal compact flash disk fails.
- HDD LED—Indicates disk activity for the hard disk drive.
- Management ports—Each Routing Engine has one 10/100-Mbps Ethernet port for connecting to a management network, and two asynchronous serial ports—one for connecting to a console and one for connecting to a modem or other auxiliary device. The interface ports are labeled **AUX**, **CONSOLE**, and **ETHERNET**.

- EEPROM—Stores the serial number of the Routing Engine.
- Extractor clips—Used for inserting and extracting the Routing Engine.
- Captive screws—Secures the Routing Engine in place.

The Routing Engine boots from the storage media in this order: the USB device (if present), then the internal flash disk, then the hard disk, then the LAN.

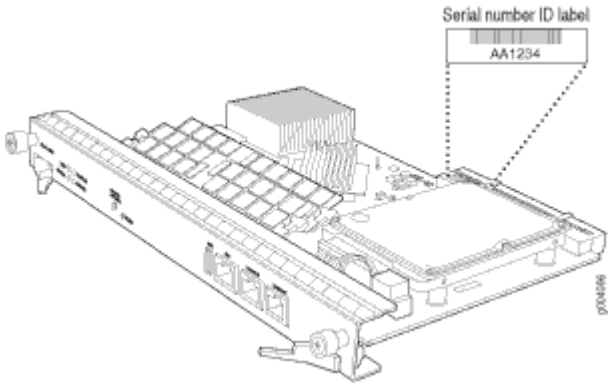
NOTE: For specific information about Routing Engine components (for example, the amount of DRAM), issue the `show chassis routing-engine` command.

Description	Routing Engine for SRX5400, SRX5600, and SRX5800 Firewalls
Software release	• Junos OS Release 9.2 and later • Junos OS Release 10.0 and later required to install a second Routing Engine
Cables and connectors	**AUX**—Connects the Routing Engine to a laptop, a modem, or another auxiliary device through a cable with an RJ-45 connector. **CONSOLE**—Connects the Routing Engine to a system console through a cable with an RJ-45 connector. **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.
Controls	• **RESET** button—Reboots the Routing Engine when pressed • **ONLINE/OFFLINE** Button—Not supported in the current release

Supported Slots	Front panel slot in an SCB installed in: • SRX5400: Bottom slot 0 • SRX5600: Bottom slots 0 or 1 • SRX5800: Center slots 0 or 1 **NOTE**: The firewall host subsystem Routing Engine must be installed in the SCB in slot **0**. A Routing Engine installed in an SCB in slot **1** only enables dual control links in chassis cluster configurations.
Power Requirement	90 W
Weight	Approximately 2.4 lb (1.1 kg)
LEDs	**HDD** LED: • Blinking green–The Routing Engine hard disk is functioning normally. **MASTER** LED: • Blue–The Routing Engine is Primary. **NOTE**: The SRX5400, SRX5600, and SRX5800 Firewalls do not support a secondary or backup Routing Engine, so the **MASTER** LED should always be lit. **OK/FAIL** LED, one bicolor: • Off–The Routing Engine is operating normally. • Red–The Routing Engine has failed and is not operating normally. **ONLINE** LED: • Blinking green–The Routing Engine is coming online. • Steady green–The Routing Engine is functioning normally.

Serial Number Location	The serial number label is located on the right side of the top of the Routing Engine as shown in Figure 46 on page 94

Figure 46: SRX5K-RE-13-20 Serial Number Label

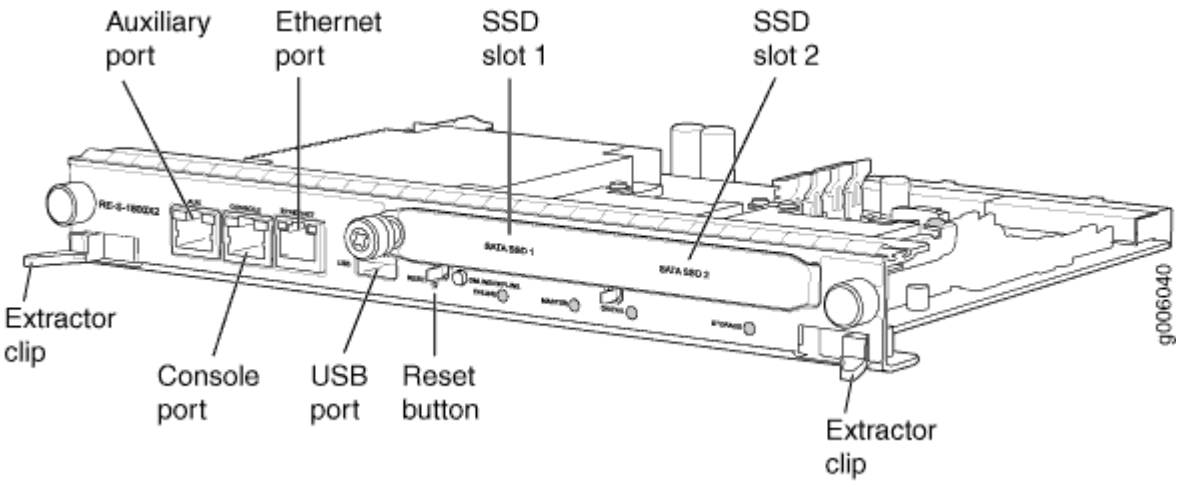


Routing Engine SRX5K-RE-1800X4 Overview

IN THIS SECTION

The enhanced Routing Engine is an Intel-based PC platform that runs Junos OS. Software processes that run on the Routing Engine maintain the routing tables, manage the routing protocols used on the device, control the device interfaces, control some chassis components, and provide the interface for system management and user access to the device.The Routing Engine must be installed directly into the SRX5K-SCBE. A USB port on the Routing Engine accepts a USB memory device that allows you to load Junos OS. Figure 47 on page 95 shows the Routing Engine.

Figure 47: SRX5K-RE-1800X4 Routing Engine



Three ports located on the Routing Engine connect to one or more external devices on which system administrators can issue Junos OS CLI commands to manage the firewall.

The ports function as follows:

- **AUX**–Connects the Routing Engine to a laptop, modem, or other auxiliary device through a serial cable with an RJ-45 connector.
- **CONSOLE**–Connects the Routing Engine to a system console through a serial cable with an RJ-45 connector.
- **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 10/100/1000 Mbps connections. Two small LEDs on the bottom of the port indicate the connection in use: the LED flashes yellow or green for a 10/100/1000 Mbps connection, and the LED is light green when traffic is passing through the port.

The solid-state drive (SSD) slots located on the Routing Engine provide secondary storage for log files, for generating core files, and for rebooting the system if the CompactFlash card fails. Currently, SRX5K-RE-1800X4 only supports one 128-GB SSD.

SRX5K-RE-1800X4 Routing Engine Boot Sequence

The firewall is shipped with three copies of the Junos OS preinstalled on the Routing Engine in the following locations:

- On the CompactFlash card in the Routing Engine
- On the SSD in the Routing Engine

- On a USB flash drive that can be inserted into the slot on the Routing Engine faceplate

The Routing Engine boots from the storage media in this order: the USB device (if present), the CompactFlash card, the solid-state drive (SSD), and then the LAN. Normally, the firewall boots from the copy of the software on the CompactFlash card.

Routing Engine SRX5K-RE-1800X4 Specifications

IN THIS SECTION

Each Routing Engine consists of the following components:

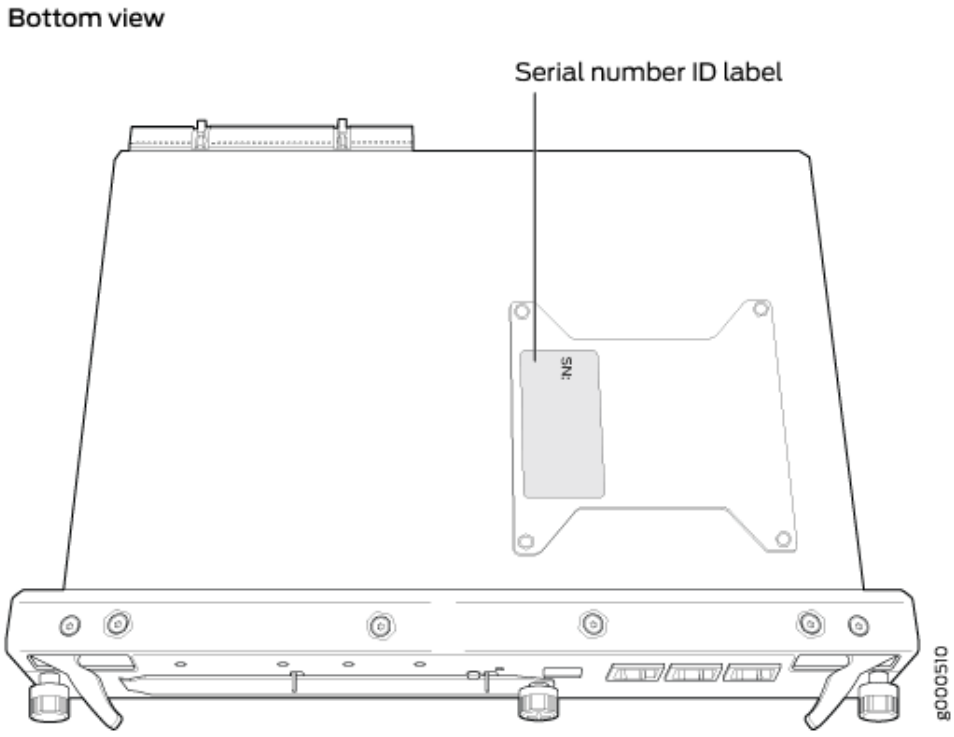
- CPU—Runs Junos OS to maintain the routing tables and routing protocols.
- DRAM—Provides storage for the routing and forwarding tables and for other Routing Engine processes.
- USB port—Provides a removable media interface through which you can install the Junos OS manually. Junos OS supports USB version 1.0 and 2.0.
- CompactFlash card—Provides primary storage for software images, configuration files, and microcode. The CompactFlash card is fixed and is inaccessible from outside the device.
- Solid-state drive (SSD)—Provides secondary storage for log files, for generating core files, and for rebooting the system if the CompactFlash card fails.
- Interface ports—The **AUX**, **CONSOLE**, and **ETHERNET** ports provide access to management devices. Each Routing Engine has one 10/100/1000-Mbps Ethernet port for connecting to a management network, and two asynchronous serial ports—one for connecting to a console and one for connecting to a modem or other auxiliary device.
- EEPROM—Stores the serial number of the Routing Engine.
- Reset button—Reboots the Routing Engine when pressed.
- Online/Offline button—Takes the Routing Engine online or offline when pressed.
- Extractor clips—Inserts and extracts the Routing Engine.

- Captive screws—Secures the Routing Engine in place.

Description	Routing Engine for SRX5400, SRX5600, and SRX5800 Firewalls
Software release	Junos OS Release 12.1X47-D15 and later
Cables and connectors	Slot for Routing Engine • **AUX**–Connects the Routing Engine to a laptop, a modem, or another auxiliary device through a cable with an RJ-45 connector. • **CONSOLE**–Connects the Routing Engine to a system console through a cable with an RJ-45 connector. • **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.
Controls	RESET button–Reboots the Routing Engine when pressed.
Supported slots	Front panel slot in an SCB installed in: • SRX5400: Bottom slot 0 • SRX5600: Bottom slots 0 or 1 • SRX5800: Center slots 0 or 1 **NOTE**: The firewall host subsystem Routing Engine must be installed in the SCB in slot 0. A Routing Engine installed in an SCB in slot 1 only enables dual control links in chassis cluster configurations.
Power requirement	90 W
Weight	2.4 lb (1.1 kg)

Serial number location	The serial number label is located as shown in Figure 48 on page 98.

Figure 48: SRX5K-RE-1800X4 Serial Number Label



SRX5K-RE-1800X4 LEDs

Each Routing Engine has four LEDs that indicate its status. The LEDs, labeled **MASTER**, **STORAGE**, **ONLINE**, and **OK/FAIL**, are located directly on the faceplate of the Routing Engine. Table 36 on page 98 describes the Routing Engine LEDs and their states.

Table 36: SRX5K-RE-1800X4 LEDs

Label	Color	State	Description
MASTER	Blue	On steadily	Routing Engine is the primary.
STORAGE	Green	Blinking	Indicates activity on the SSD or CompactFlash card.

Table 36: SRX5K-RE-1800X4 LEDs *(Continued)*

Label	Color	State	Description
ONLINE	Green	Blinking	Routing Engine is transitioning online.
	None	On steadily	Routing Engine is functioning normally.
OK/FAIL	Red	On steadily	Routing Engine has failed.

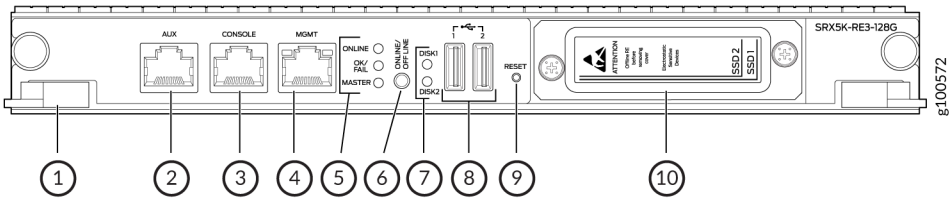
Routing Engine SRX5K-RE3-128G Specifications

IN THIS SECTION

The Routing Engine maintains the routing tables, manages the routing protocols used on the device, controls the device interfaces, controls some chassis components, and provides the interfaces for system management and user access to the device.

Figure 49 on page 99 shows the SRX5K-RE3-128G Routing Engine.

Figure 49: SRX5K-RE3-128G Routing Engine Front View



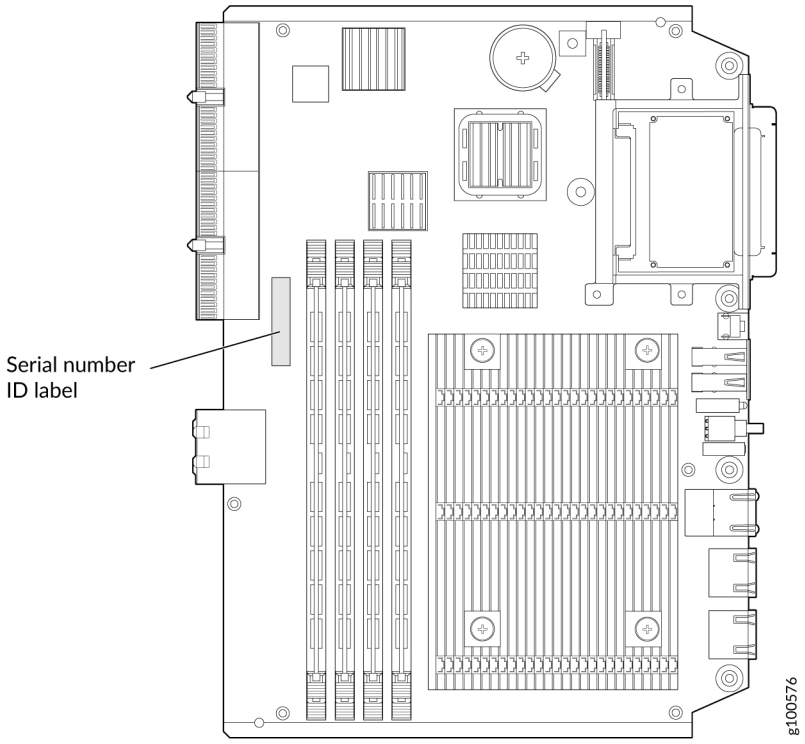
1– Extractor clips	6– **ONLINE/OFFLINE** button
2– Auxiliary port (**AUX**)	7– SSD LEDs—**DISK1** and **DISK2**
3– Console port (**CONSOLE**)	8– USB ports—**USB1** and **USB2**
4– Management port (**MGMT**)	9– **RESET** button
5– Routing Engine status LEDs—**ONLINE**, **OK/FAIL**, and **MASTER**	10– SSD card slot cover

Description	Routing Engine for SRX5400, SRX5600, and SRX5800 Firewalls, based on Intel's Haswell-EP CPU with 6 cores, and 128GB of DDR4 memory. It provides increased control plane performance and scalability along with virtualization features in the SRX Series 5000 line of chassis.
Software release	Junos OS Release 19.3R1 and later
Cables and connectors	Slot for Routing Engine • **AUX**–Connects the Routing Engine to a laptop, a modem, or another auxiliary device through a cable with an RJ-45 connector. • **CONSOLE**–Connects the Routing Engine to a system console through a cable with an RJ-45 connector. • **MGMT**–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.
Controls	**RESET** button–Reboots the Routing Engine when pressed.

Supported slots	Front panel slot in an SCB installed in: • SRX5400: Bottom slot 0 • SRX5600: Bottom slots 0 or 1 • SRX5800: Center slots 0 or 1 **NOTE**: The firewall host subsystem Routing Engine must be installed in the SCB in slot 0. A Routing Engine installed in an SCB in slot 1 only enables dual control links in chassis cluster configurations. **NOTE**: In the SRX5600 or SRX5800 Firewalls chassis cluster configurations, dual control links functionality is not supported if you mix SRX5K-RE-1800X4 and SRX5K-RE3-128G Routing Engines. To support dual control links you have to install two SRX5K-RE3-128Gs.
Power requirement	110 W
Weight	2.69 lb (1.22 kg)

Serial number location	The serial number label is located as shown in Figure 50 on page 102.

Figure 50: SRX5K-RE3-128G Serial Number Label



SRX5K-RE3-128G Routing Engine Components

Each Routing Engine consists of the following components:

- CPU—Runs Junos OS to maintain the routing tables and routing protocols.
- EEPROM—Stores the serial number of the Routing Engine.
- DRAM—Provides storage for the routing and forwarding tables and for other Routing Engine processes.
- One 10-Gigabit Ethernet interface between the Routing Engine and Switch Control Board.
- Extractor clips—Control the locking system that secures the Routing Engine.
- Interface ports—The **AUX**, **CONSOLE**, and **MGMT** ports provide access to management devices. Each Routing Engine has one 10/100/1000-Mbps Ethernet port for connecting to a management

network, and two asynchronous serial ports—one for connecting to a console and one for connecting to a modem or other auxiliary device.

> **NOTE**: The control interface names differ based on the routing engine:
>
> - For RE2, the control interfaces are displayed as `em0` and `em1`.
> - For RE3, the control interfaces are displayed as `ixlv0` and `igb0`.
>
> For more information, see show chassis cluster interfaces.

- Status LEDs—Table 37 on page 103 describes the functions of the **ONLINE**, **OK/FAIL**, **MASTER**, **DISK1**, and **DISK2** LEDs.
- **ONLINE/OFFLINE** button—Takes the Routing Engine online or offline when pressed.

  > **NOTE**: The **ONLINE/OFFLINE** button must be pressed for a minimum of 4 seconds.

- **USB1** and **USB2** ports—Provide a removable media interface through which you can install Junos OS manually. Junos OS supports USB versions 3.0, 2.0, and 1.1.
- **RESET** button—Reboots the Routing Engine when pressed.
- **SSD1** (primary) and **SSD2** (secondary) Solid-state drives (SSD)—Two 200-GB each slim solid-state drives that provide storage for software images, configuration files, microcode, log files, and memory dumps. The Routing Engine reboots from **SSD2** when boot from primary **SSD1** fails.
- Captive screws—Secures the Routing Engine.

SRX5K-RE3-128G Routing Engine LEDs

Each Routing Engine has four LEDs that indicate its status. The LEDs, labeled **ONLINE**, **OK/FAIL**, **MASTER**, **DISK1**, and **DISK2**, are located directly on the faceplate of the Routing Engine. Table 37 on page 103 describes the Routing Engine LEDs and their states.

Table 37: SRX5K-RE3-128G Routing Engine LEDs

Label	Color	State	Description
ONLINE	Green	Blinking slowly	Routing Engine is in the process of booting BIOS and the host OS.

Table 37: SRX5K-RE3-128G Routing Engine LEDs *(Continued)*

Label	Color	State	Description
		Blinking rapidly	Routing Engine is in the process of booting Junos OS.
	-	Off	Routing Engine is not online or not functioning normally.
OK/FAIL	Green	On steadily	Routing Engine is powering up.
	Yellow	On steadily	Routing Engine is not powering up, which indicates failure.
MASTER	Blue	On steadily	This Routing Engine is the primary Routing Engine.
DISK1	Green	Blinking	Indicates presence of disk activity.
	-	Off	There is no disk activity.
DISK2	Green	Blinking	Indicates presence of disk activity.
	-	Off	There is no disk activity.

SRX5K-RE3-128G Routing Engine Boot Sequence

Booting in a SRX5K-RE3-128G Routing Engine follows this sequence—the USB device, SSD1, SSD2, and LAN. SSD1 is the primary boot device. The boot sequence is tried twice for SSD1 and SSD2.

SRX5800 Line Cards and Modules

IN THIS SECTION

SRX5400, SRX5600, and SRX5800 Firewall Card Overview

The cards described in this guide let you upgrade and customize your SRX5400, SRX5600, or SRX5800 Firewall to suit the needs of your network. The following types of cards are available for the SRX5400, SRX5600, and SRX5800 Firewalls:

- I/O cards (IOCs) provide additional physical network connections to the firewall. Their primary function is to deliver data packets arriving on the physical ports to the Services Processing Cards (SPCs) and to forward data packets out the physical ports after services processing.
- Flex IOCs have two slots for port modules that add additional physical network connections to the firewall. Like IOCs, their primary function is to deliver data packets arriving on the physical ports to the SPCs and to forward data packets out the physical ports after services processing.
- Modular Port Concentrators (MPCs) have slots on the front panel that accept smaller cards called Modular Interface Cards (MICs). Each MIC has one or more physical interfaces on it. An MPC with MICs installed functions in the same way as a regular I/O card (IOC), but allows greater flexibility in adding different types of Ethernet ports to your firewall. MPCs and MICs are similar in form and function to Flex IOCs and port modules. However, the two use different form-factors, so you cannot install port modules in an MPC, nor can you install MICs in a Flex IOC.
- Services Processing Cards (SPCs) provide the processing power to run integrated services such as firewall, IPsec and IDP. All traffic traversing the firewall is passed to an SPC to have services processing applied to it.
- Switch Control Boards (SCBs) power on and power off IOCs and SPCs; control clocking and system resets; and control booting, monitor, and system functions. Each SCB has a slot in the front panel for a Routing Engine.

Although the following modules are not cards in the sense of having a form-factor that fits the card cage of the SRX5400, SRX5600, and SRX5800 Firewall, this guide also addresses the following modules that fit into certain SRX5400, SRX5600, and SRX5800 Firewall cards:

- Routing Engines fit into slots in SCBs and maintain the routing tables, manage the routing protocols used on the device, control the device interfaces and some chassis components, and provide the interface for system management and user access to the device.
- Port modules fit into slots in Flex IOCs and add additional physical network interface ports to the firewall.
- Modular Interface Cards (MICs) fit into slots in MPCs and add additional physical network interface ports to the firewall. MPCs and MICs are similar in form and function to Flex IOCs and port modules. However, the two use different form-factors, so you cannot install port modules in an MPC, nor can you install MICs in a Flex IOC.

Cards Supported on SRX5400, SRX5600, and SRX5800 Firewalls

Table 38 on page 107 describes the cards and other modules supported on the SRX5400, SRX5600, and SRX5800 Firewalls.

Table 38: Supported Cards for SRX5400, SRX5600, and SRX5800 Firewalls

Card Name and Model Number	Earliest Supported Junos OS Release		Last Supported Junos OS Release
	SRX5400	SRX5600 and SRX5800	SRX5400, SRX5600, and SRX5800
SPCs			
"Services Processing Card SRX5K-SPC-2-10-40 Specifications" on page 114	Not supported	9.2	12.3X48
"Services Processing Card SRX5K-SPC-4-15-320 Specifications" on page 120	12.1X46-D10	12.1X44-D10	
"Services Processing Card SRX5K-SPC3 Specifications" on page 126	18.2R1-S1	18.2R1-S1	
Interface Cards			
"I/O Card SRX5K-40GE-SFP Specifications" on page 167	Not supported	9.2	12.3X48
"I/O Card SRX5K-4XGE-XFP Specifications" on page 170	Not supported	9.2	12.3X48
"Flex I/O Card (SRX5K-FPC-IOC) Specifications" on page 173	Not supported	10.2	12.3X48

Table 38: Supported Cards for SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Card Name and Model Number	Earliest Supported Junos OS Release		Last Supported Junos OS Release
	SRX5400	SRX5600 and SRX5800	SRX5400, SRX5600, and SRX5800
"Modular Port Concentrator (SRX5K-MPC) Specifications" on page 130	12.1X46-D10	12.1X46-D10	
"SRX5K-MPC3-40G10G Specifications" on page 148	15.1X49-D10	15.1X49-D10	
"SRX5K-MPC3-100G10G Specifications" on page 152	15.1X49-D10	15.1X49-D10	
"SRX5K-IOC4-10G Specifications" on page 156	19.3R1	19.3R1	
"SRX5K-IOC4-MRAT Specifications" on page 160	19.3R1	19.3R1	
SCBs			
"Switch Control Board SRX5K-SCB Specifications" on page 73	12.1X46-D10	9.2	12.3X48
"Switch Control Board SRX5K-SCBE Specifications" on page 78	12.1X47-D15	12.1X47-D15	
"Switch Control Board SRX5K-SCB3 Specifications" on page 82	15.1X49-D10	15.1X49-D10	

Table 38: Supported Cards for SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Card Name and Model Number	Earliest Supported Junos OS Release		Last Supported Junos OS Release
	SRX5400	SRX5600 and SRX5800	SRX5400, SRX5600, and SRX5800
"Switch Control Board SRX5K-SCB4 Specifications" on page 86	Not supported	19.3R1	
Other modules			
"Flex I/O Card Port Module SRX-IOC-16GE-SFP Specifications" on page 175	Not supported	10.2	
"Flex I/O Card Port Module SRX-IOC-16GE-TX Specifications" on page 177	Not supported	10.2	
"Flex I/O Card Port Module SRX-IOC-4XGE-XFP Specifications" on page 180	Not supported	10.2	
"MIC with 1x100GE CFP Interface (SRX-MIC-1X100G-CFP)" on page 144	12.1X46-D10	12.1X46-D10	
"MIC with 2x40GE QSFP+ Interfaces (SRX-MIC-2X40G-QSFP)" on page 146	12.1X46-D10	12.1X46-D10	
"MIC with 10x10GE SFP+ Interfaces (SRX-MIC-10XG-SFPP)" on page 140	12.1X46-D10	12.1X46-D10	

Table 38: Supported Cards for SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Card Name and Model Number	Earliest Supported Junos OS Release		Last Supported Junos OS Release
	SRX5400	SRX5600 and SRX5800	SRX5400, SRX5600, and SRX5800
"MIC with 20x1GE SFP Interfaces (SRX-MIC-20GE-SFP)" on page 133	12.1X47-D10	12.1X47-D10	
"Routing Engine SRX5K-RE-13-20 Specifications" on page 90	12.1X46-D10	9.2	12.3X48
"Routing Engine SRX5K-RE-1800X4 Specifications" on page 96	12.1X47-D15	12.1X47-D15	
"Routing Engine SRX5K-RE3-128G Specifications" on page 99	19.3R1	19.3R1	

Figure 51 on page 111 is an interoperability matrix that describes the compatibility between various interface cards for the SRX5400, SRX5600, and SRX5800 Firewalls.

Figure 51: Interoperability Matrix for SRX5400, SRX5600, and SRX5800 Firewalls

Model Numbers	SRX5400 SRX5K-SCB SRX5K-RE-13-20	SRX5600/SRX5800 SRX5K-SCB SRX5K-RE-13-20	SRX5K-SCBE SRX5K-RE-1800X4	SRX5K-SCB3 SRX5K-RE-1800X4	SRX5K-SPC-2-10-40	SRX5K-SPC-4-15-320	SRX5K-SPC3	SRX5K-4XGE-XFP SRX5K-40GE-SFP SRX5K-FPC-IOC	SRX5K-MPC (SRX-MIC-20GE-SFP), (SRX-MIC-10XG-SFPP) (SRX-MIC-1X100G-CFP), (SRX-MIC-2X40G-QSFP)	SRX5K-MPC3-40G10G SRX5K-MPC3-100G10G	SRX5K-IOC4-10G SRX5K-IOC4-MRAT	SRX5600/SRX5800 SRX5K-SCB4 SRX5K-RE3-128G	SRX5600/SRX5800 SRX5K-SCB4 SRX5K-RE-1800X4	SRX5K-SCB3 SRX5K-RE3-128G
SRX5400 SRX5K-SCB SRX5K-RE-13-20	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗
SRX5600/SRX5800 SRX5K-SCB SRX5K-RE-13-20	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗
SRX5K-SCBE SRX5K-RE-1800X4	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗
SRX5K-SCB3 SRX5K-RE-1800X4	✗	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗
SRX5K-SPC-2-10-40	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗
SRX5K-SPC-4-15-320	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SRX5K-SPC3	✗	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓
SRX5K-4XGE-XFP SRX5K-40GE-SFP SRX5K-FPC-IOC	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗
SRX5K-MPC (SRX-MIC-20GE-SFP) (SRX-MIC-10XG-SFPP) (SRX-MIC-1X100G-CFP) (SRX-MIC-2X40G-QSFP)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SRX5K-MPC3-40G10G SRX5K-MPC3-100G10G	✗	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓
SRX5K-IOC4-10G SRX5K-IOC4-MRAT	✗	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓
SRX5600/SRX5800 SRX5K-SCB4 SRX5K-RE3-128G	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗
SRX5600/SRX5800 SRX5K-SCB4 SRX5K-RE-1800X4	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗
SRX5K-SCB3 SRX5K-RE3-128G	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✗	✗	✓

g004198

SRX5800 Firewall Card Cage and Slots

The card cage is the set of 14 vertical slots in the front of the chassis where you install cards. The slots are numbered from left to right. Table 39 on page 112 describes the types of cards that you can install into each slot.

Table 39: SRX5800 Firewall Card Cage Slots

Card Cage Slot	Eligible Cards				
	SPC	SPC3	IOC, Flex IOC, or MPC	SCB	IOC3 & IOC4
0 (leftmost)	X	X	X		
1	X	X	X		X
2	X	X	X		X
3	X	X	X		X
4	X	X	X		X
5	X	X	X		X
0				X	
1				X	
2/6	X	X	X	X	X
7	X	X	X		X
8	X	X	X		X
9	X	X	X		X

Table 39: SRX5800 Firewall Card Cage Slots *(Continued)*

Card Cage Slot	Eligible Cards				
	SPC	SPC3	IOC, Flex IOC, or MPC	SCB	IOC3 & IOC4
10	X	X	X		X
11 (rightmost)	X		X		

NOTE: For operational and cooling efficiency in SRX5800 Firewalls, we recommend that slot 0 and 11 be filled last.

SRX5800 Firewall SPC Description

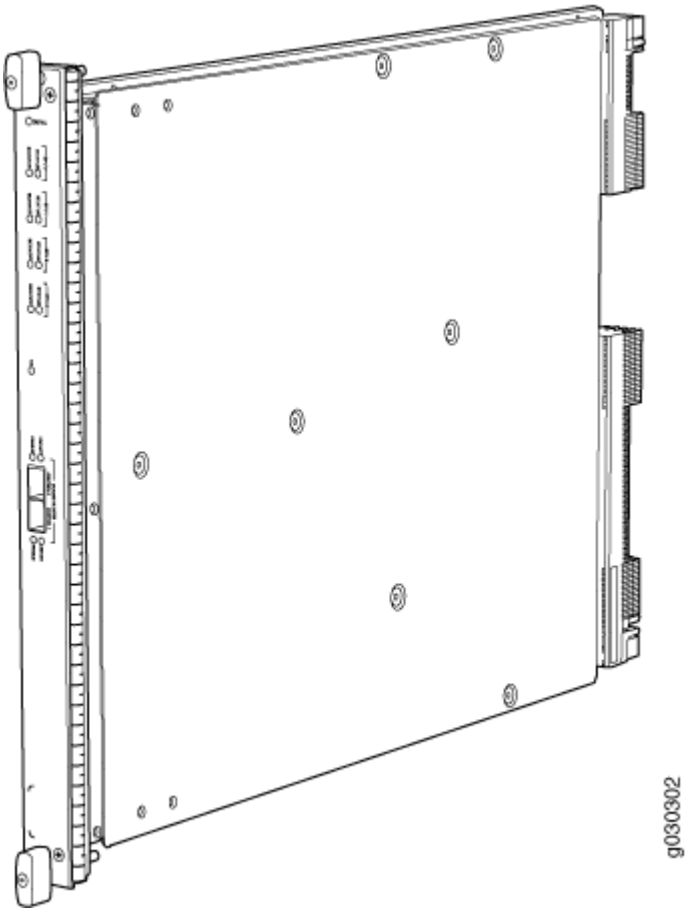
The Services Processing Card (SPC) has Services Processing Units (SPUs), which provide the processing power to run integrated services such as firewall, IPsec, and IDP (see Figure 52 on page 114). All traffic traversing the firewall is passed to an SPU to have services processing applied to it. Traffic is intelligently distributed by interface cards to SPUs for services processing.

The firewall must have one SPC installed.

You can install an SPC in any of the slots that are not reserved for Switch Control Board (SCB). If a slot is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the device.

Figure 52 on page 114 shows a typical SPC supported on the firewall.

Figure 52: Typical SPC



For detailed information about SPCs supported by the firewall, see the *SRX5400, SRX5600, and SRX5800 Firewall Card Reference* at www.juniper.net/documentation/.

Services Processing Card SRX5K-SPC-2-10-40 Specifications

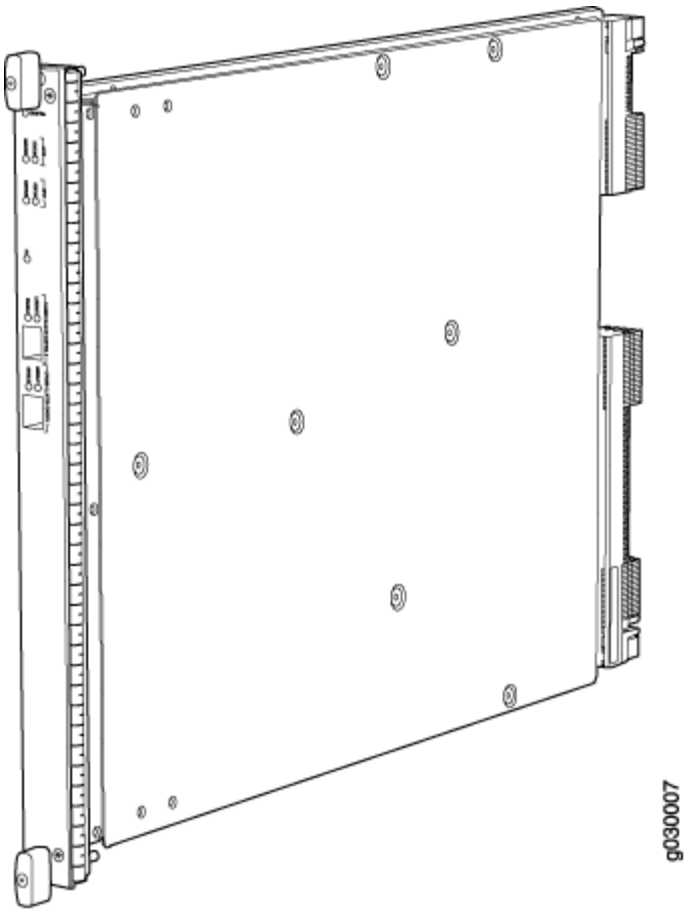
The SRX5K-SPC-2-10-40 Services Processing Card (SPC) contains two Services Processing Units (SPUs), which provide the processing power to run integrated services such as firewall, IPsec, and IDP (see Figure 53 on page 115). All traffic traversing the firewall is passed to an SPU to have services processing applied to it. Traffic is intelligently distributed by I/O cards (IOCs) to SPUs for services processing.

The firewall must have at least one SPC installed. You can install additional SPCs to increase services processing capacity.

You can install SPCs in any of the slots that are not reserved for Switch Control Boards (SCBs). If a slot is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the device.

Figure 53 on page 115 shows a typical SPC supported on the firewall.

Figure 53: Services Processing Card SRX5K-SPC-2-10-40



Each SPC consists of the following components:

- SPC cover, which functions as a ground plane and a stiffener.
- Two small form-factor pluggable (SFP) chassis cluster control ports for connecting multiple devices into a redundant chassis cluster. See *Chassis Cluster User Guide for SRX Series Devices* for more information about connecting and configuring redundant chassis clusters.

> **CAUTION**: The Juniper Networks Technical Assistance Center (JTAC) provides complete support for Juniper-supplied optical modules and cables. However, JTAC does not provide support for third-party optical modules and cables that are not qualified or supplied by Juniper Networks. If you face a problem running a Juniper device that uses third-party optical modules or cables, JTAC may help you diagnose

host-related issues if the observed issue is not, in the opinion of JTAC, related to the use of the third-party optical modules or cables. Your JTAC engineer will likely request that you check the third-party optical module or cable and, if required, replace it with an equivalent Juniper-qualified component.

Use of third-party optical modules with high-power consumption (for example, coherent ZR or ZR+) can potentially cause thermal damage to or reduce the lifespan of the host equipment. Any damage to the host equipment due to the use of third-party optical modules or cables is the users' responsibility. Juniper Networks will accept no liability for any damage caused due to such use.

- Fabric interfaces.
- Two Gigabit Ethernet interfaces that allow control information, route information, and statistics to be sent between the Routing Engine and the CPU on the SPCs.
- Two interfaces from the SCBs that enable the boards to be powered on and controlled.
- Physical SPC connectors.
- Midplane connectors and power circuitry.
- Processor subsystem, which includes a 1.2-GHz CPU, system controller, and 1 GB of SDRAM.
- LEDs on the faceplate that indicate the SPC and SPU status.

Description	SPC with two SPUs
Software release	• Junos OS Release 9.2 and later
Cables and connectors	**CHASSIS CLUSTER CONTROL 0** and **CHASSIS CLUSTER CONTROL 1**–SFP ports for control links in chassis cluster configurations. Supported SFP transceivers: 1000BASE-LH (model numbers SRX-SFP-1GE-LH, SRX-SFP-1GE-LH-ET) 1000BASE-LX (model numbers SRX-SFP-1GE-LX, SRX-SFP-1GE-LX-ET) 1000BASE-SX (model numbers SRX-SFP-1GE-SX, SRX-SFP-1GE-SX-ET)
Controls	None

Supported Slots	• SRX5600–Any slot, except the bottom slots **0** or **1** which are reserved for SCB/RE. • SRX5800–Any slot, except the centre or middle slots **0** or **1** which are reserved for SCB/RE.
Power Requirement	Maximum 265 W
Weight	Approximately 13 lb (5.9 kg)

LEDs

OK/FAIL LED, one bicolor:

- Steady green–The SPC is operating normally.
- Red–The SPC has failed and is not operating normally.
- Off–The SPC is powered down.

STATUS LED, one tricolor for each of the two SPUs **SPU 0** and **SPU 1**:

- Green–The SPU is operating normally.
- Amber–The SPU is initializing.
- Red–The SPU has encountered an error or a failure.
- Off–The SPU is offline. If all four SPUs are offline, it is safe to remove the SPC from the chassis.

SERVICE LED, one bicolor for each of the two SPUs, **SPU 0** and **SPU 1**:

- Green–Service is running on the SPU under acceptable load.
- Amber–Service on the SPU is overloaded.
- Off–Service is not running on the SPU.

HA LED, one tricolor:

NOTE: The **HA** LED is lit only if the SPC has a control link, otherwise it is off.
Sometimes even after the control link is removed from the SPC, the **HA** LED would lit. Power cycle both the nodes to turn off the LED,

- Green (bold)–Clustering is operating normally. All cluster members and monitored links are available, and no error conditions are detected.
- Green (blinking)–Data transfer between the nodes.
- Red–A critical alarm is present on clustering. A cluster member is missing or unreachable, or the other node is no longer part of a cluster because it has been disabled by the dual membership and detection recovery process in reaction to a control link or fabric link failure.
- Amber–All cluster members are present, but an error condition has compromised the performance and resiliency of the cluster. The reduced bandwidth could cause packets to be dropped or could result in reduced resiliency because a single point of failure might exist. The error condition might be caused by:

- The loss of chassis cluster links which causes an interface monitoring failure.
- An error in an SPU or NPU.
- Failure of the spu-monitoring or cold-sync-monitoring processes.
- A chassis cluster IP monitoring failure.

LINK/ACT LED, one for each of the two ports **CHASSIS CLUSTER CONTROL 0** and **CHASSIS CLUSTER CONTROL 1**:

- Green (flickering)–Chassis cluster control port link is active.
- Off–No link.

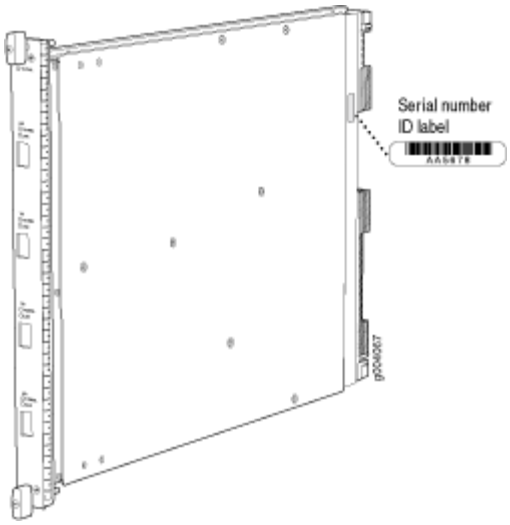
ENABLE LED, one for each of the two ports **CHASSIS CLUSTER CONTROL 0** and **CHASSIS CLUSTER CONTROL 1**:

- Green–The chassis cluster control port is enabled.
- Off–The chassis cluster control port is disabled.

Serial Number Location

The serial number label is located as shown in Figure 54 on page 119.

Figure 54: Serial Number Label (IOC Shown, Other Cards Similar)



Services Processing Card SRX5K-SPC-4-15-320 Specifications

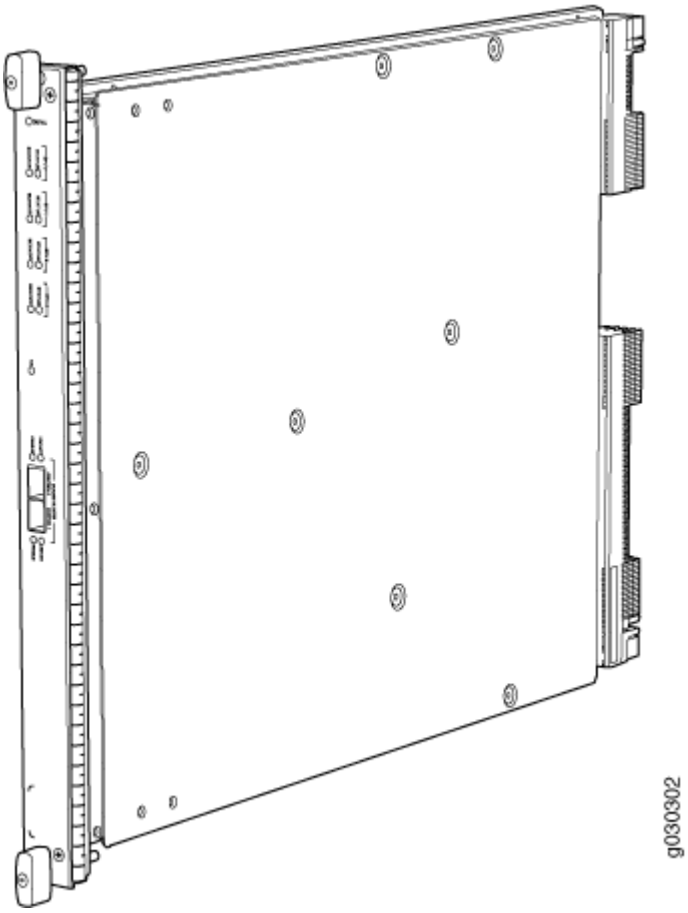
The SRX5K-SPC-4-15-320 Services Processing Card (SPC) contains four Services Processing Units (SPUs), which provide the processing power to run integrated services such as firewall, IPsec, and IDP (see Figure 55 on page 121). All traffic traversing the firewall is passed to an SPU to have services processing applied to it. Traffic is intelligently distributed by I/O cards (IOCs) to SPUs for services processing.

The firewall must have at least one SPC installed. You can install additional SPCs to increase services processing capacity.

You can install SPCs in any of the slots that are not reserved for Switch Control Boards (SCBs). If a slot is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the device.

If your firewall contains a mix of SRX5K-SPC-4-15-320 SPCs and earlier SRX5K-SPC-2-10-40 SPCs, an SRX5K-SPC-4-15-320 SPC must occupy the lowest-numbered slot of any SPC in the chassis. This configuration ensures that the center point (CP) function is performed by the faster and higher-performance SPC type.

Figure 55: Services Processing Card SRX5K-SPC-4-15-320



Each SPC consists of the following components:

- SPC cover, which functions as a ground plane and a stiffener.
- Two small form-factor pluggable (SFP) chassis cluster control ports for connecting multiple devices into a redundant chassis cluster. See *Chassis Cluster User Guide for SRX Series Devices* for more information about connecting and configuring redundant chassis clusters.

> **CAUTION**: The Juniper Networks Technical Assistance Center (JTAC) provides complete support for Juniper-supplied optical modules and cables. However, JTAC does not provide support for third-party optical modules and cables that are not qualified or supplied by Juniper Networks. If you face a problem running a Juniper device that uses third-party optical modules or cables, JTAC may help you diagnose host-related issues if the observed issue is not, in the opinion of JTAC, related to the use of the third-party optical modules or cables. Your JTAC engineer will likely request

that you check the third-party optical module or cable and, if required, replace it with an equivalent Juniper-qualified component.

Use of third-party optical modules with high-power consumption (for example, coherent ZR or ZR+) can potentially cause thermal damage to or reduce the lifespan of the host equipment. Any damage to the host equipment due to the use of third-party optical modules or cables is the users' responsibility. Juniper Networks will accept no liability for any damage caused due to such use.

- Fabric interfaces.
- Two Gigabit Ethernet interfaces that allow control information, route information, and statistics to be sent between the Routing Engine and the CPU on the SPCs.
- Two interfaces from the SCBs that enable the boards to be powered on and controlled.
- Physical SPC connectors.
- Midplane connectors and power circuitry.
- Processor subsystem, which includes a 1.2-GHz CPU, system controller, and 1 GB of SDRAM.
- LEDs on the faceplate that indicate the SPC and SPU status.

Description	SPC with four SPUs
Software release	• Junos OS Release 12.1X44-D10 and later
Cables and connectors	**CHASSIS CLUSTER CONTROL 0** and **CHASSIS CLUSTER CONTROL 1**–SFP ports for control links in chassis cluster configurations. Supported SFP transceivers: 1000BASE-LH (model numbers SRX-SFP-1GE-LH, SRX-SFP-1GE-LH-ET) 1000BASE-LX (model numbers SRX-SFP-1GE-LX, SRX-SFP-1GE-LX-ET) 1000BASE-SX (model numbers SRX-SFP-1GE-SX, SRX-SFP-1GE-SX-ET)
Controls	None

Supported Slots	• SRX5400–Any slot, except the bottom slot **0** which is reserved for SCB/RE. • SRX5600–Any slot, except the bottom slots **0** or **1** which are reserved for SCB/RE. • SRX5800–Any slot, except the centre or middle slots **0** or **1** which are reserved for SCB/RE.
Power Requirement	475 W typical, 585 W maximum **NOTE**: • In the SRX5600 and SRX5800 Firewalls, you must have high-capacity power supplies (either AC or DC) and high-capacity fan trays installed in the firewall in order to install and use SRX5K-SPC-4-15-320 SPCs. If you do not have high-capacity power supplies and fan trays installed, the firewall will log an alarm condition when it recognizes the SRX5K-SPC-4-15-320 SPCs. • On SRX5600 Firewalls with AC power supplies, we recommend that you use high-line (220v) input power to ensure the device has adequate power to support SRX5K-SPC-4-15-320 SPCs.
Weight	Approximately 18 lb (8.3 kg)

LEDs

OK/FAIL LED, one bicolor:

- Steady green–The SPC is operating normally.
- Red–The SPC has failed and is not operating normally.
- Off–The SPC is powered down.

STATUS LED, one tricolor for each of the four SPUs **SPU 0** through **SPU 3**:

- Green–The SPU is operating normally.
- Amber–The SPU is initializing.
- Red–The SPU has encountered an error or a failure.
- Off–The SPU is offline. If all four SPUs are offline, it is safe to remove the SPC from the chassis.

SERVICE LED, one bicolor for each of the four SPUs **SPU 0** through **SPU 3**:

- Green–Service is running on the SPU under acceptable load.
- Amber–Service on the SPU is overloaded.
- Off–Service is not running on the SPU.

HA LED, one tricolor:

- Green–Clustering is operating normally. All cluster members and monitored links are available, and no error conditions are detected.
- Red–A critical alarm is present on clustering. A cluster member is missing or unreachable, or the other node is no longer part of a cluster because it has been disabled by the dual membership and detection recovery process in reaction to a control-link or fabric-link failure.
- Amber–All cluster members are present, but an error condition has compromised the performance and resiliency of the cluster. The reduced bandwidth could cause packets to be dropped or could result in reduced resiliency because a single point of failure might exist. The error condition might be caused by:
  - The loss of chassis cluster links which causes an interface monitoring failure.
  - An error in an SPU or NPU.
  - Failure of the spu-monitoring or cold-sync-monitoring processes.

- A chassis cluster IP monitoring failure.

- Off–The node is not configured for clustering or it has been disabled by the dual membership and detection recovery process in reaction to a control link or fabric link failure.

LINK/ACT LED, one for each of the two ports **CHASSIS CLUSTER CONTROL 0** and **CHASSIS CLUSTER CONTROL 1**:

- Green–Chassis cluster control port link is active.

- Off–No link.

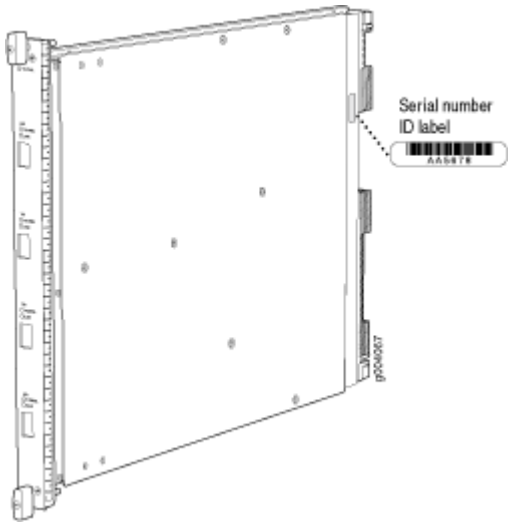
ENABLE LED, one for each of the two ports **CHASSIS CLUSTER CONTROL 0** and **CHASSIS CLUSTER CONTROL 1**:

- Green–The chassis cluster control port is enabled.

- Off–The chassis cluster control port is disabled.

Serial Number Location	The serial number label is located as shown in Figure 56 on page 125.

Figure 56: Serial Number Label (IOC Shown, Other Cards Similar)



Services Processing Card SRX5K-SPC3 Specifications

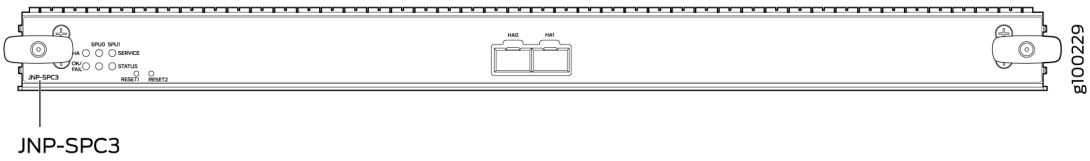
The SRX5K-SPC3 Services Processing Card (SPC) contains two Services Processing Units (SPUs) with 128GB of memory per SPU, that provide the processing power to run integrated services such as firewall, IPsec, and IDP (see Figure 57 on page 126). All traffic traversing the firewall is passed to an SPU to have services processing applied to it. Traffic is intelligently distributed by I/O cards (IOCs) to SPUs for services processing.

The firewall must have at least one SPC installed. You can install additional SPCs to increase services processing capacity.

SPCs cannot be installed in slots that are reserved for Switch Control Boards (SCBs) or in slot **11** on the SRX5800. If a slot is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the device.

NOTE: Your firewall cannot have a mix of SRX5K-SPC-2-10-40 SPCs and SRX5K-SPC3 SPCs. Starting with Junos OS release 18.2R2 and then 18.4R1 but not 18.3R1, you can have a mix of SRX5K-SPC-4-15-320 SPCs and SRX5K-SPC3 SPCs.

Figure 57: Services Processing Card SRX5K-SPC3



Each SPC consists of the following components:

- SPC cover, which functions as a ground plane and a stiffener.
- Two 10–Gigabit Ethernet small form-factor pluggable plus (SFP+) chassis cluster control ports for connecting multiple devices into a redundant chassis cluster. See the *Chassis Cluster User Guide for SRX Series Devices* for more information about connecting and configuring redundant chassis clusters.

CAUTION: The Juniper Networks Technical Assistance Center (JTAC) provides complete support for Juniper-supplied optical modules and cables. However, JTAC does not provide support for third-party optical modules and cables that are not qualified or supplied by Juniper Networks. If you face a problem running a Juniper

device that uses third-party optical modules or cables, JTAC may help you diagnose host-related issues if the observed issue is not, in the opinion of JTAC, related to the use of the third-party optical modules or cables. Your JTAC engineer will likely request that you check the third-party optical module or cable and, if required, replace it with an equivalent Juniper-qualified component.

Use of third-party optical modules with high-power consumption (for example, coherent ZR or ZR+) can potentially cause thermal damage to or reduce the lifespan of the host equipment. Any damage to the host equipment due to the use of third-party optical modules or cables is the users' responsibility. Juniper Networks will accept no liability for any damage caused due to such use.

- Fabric interfaces
- One Gigabit Ethernet switch that provides control connectivity to the Routing Engine.
- Two interfaces from the SCBs that enable the boards to be powered on and controlled.
- Physical SPC connectors
- Midplane connectors and power circuitry.
- Processor subsystem, which includes a 2.3-GHz CPU, system controller, and two 128 GB solid state-drives (SSDs).
- LEDs on the faceplate that indicate the SPC and SPU status.

Description	SPC with two SPUs of 256 GB memory.
Software release	• Junos OS Release 18.2R1-S1
Cables and connectors	**HA0** and **HA1** SFP+ ports for control links in chassis cluster configurations. Supported transceivers: • 10GBASE–LR: transceiver model number SRX-SFP-10GE-LR • 10GBASE–SR: transceiver model number SRX-SFP-10GE-SR
Controls	None

Supported Slots	• SRX5400–Any slot, except the bottom slot **0** which is reserved for SCB/RE. • SRX5600–Any slot, except the bottom slots **0** or **1** which are reserved for SCB/RE. • SRX5800–Any slot, except slot **11**, and the centre or middle slots **0** or **1** which are reserved for SCB/RE.
Power Requirement	650 W maximum **NOTE**: • In the SRX5600 and SRX5800 Firewalls, you must have high-capacity power supplies (either AC or DC) and high-capacity fan trays installed in the firewall in order to install and use SRX5K-SPC3 SPCs. If you do not have high-capacity power supplies and fan trays installed, the firewall will log an alarm condition when it recognizes the SRX5K-SPC3 SPCs. • On SRX5600 Firewalls with AC power supplies, we recommend that you use high-line (220v) input power to ensure the device has adequate power to support SRX5K-SPC3 SPCs.
Weight	Approximately 18 lb (8.3 kg)

LEDs

OK/FAIL LED, one bicolor:

- Steady green–The SPC is operating normally.
- Red–The SPC has failed and is not operating normally.
- Off–The SPC is powered down.

STATUS LED, one tricolor for each SPU **SPU 0** and **SPU 1**:

- Off–The SPU is offline.
- Blinking Amber–The SPU is initializing.
- Green–The SPU initialization is done and it is operating normally.
- Red–The SPU has encountered an error or a failure.

SERVICE LED, one tricolor for each SPU **SPU 0** and **SPU 1**:

- Off–The SPU is offline.
- Blinking Red–The SPU initialization is done.
- Blinking Amber–Service is initializing on the SPU.
- Green–Service is running on the SPU under acceptable load.
- Solid Red–Service encountered an error or a failure.

HA LED, one tricolor:

- Green–Clustering is operating normally. All cluster members and monitored links are available, and no error conditions are detected.
- Red–A critical alarm is present on clustering. A cluster member is missing or unreachable, or the other node is no longer part of a cluster because it has been disabled by the dual membership and detection recovery process in reaction to a control-link or fabric-link failure.
- Amber–All cluster members are present, but an error condition has compromised the performance and resiliency of the cluster. The reduced bandwidth could cause packets to be dropped or could result in reduced resiliency because a single point of failure might exist. The error condition might be caused by:
    - The loss of chassis cluster links which causes an interface monitoring failure.

  - An error in an SPU or NPU.
  - Failure of the spu-monitoring or cold-sync-monitoring processes.
  - A chassis cluster IP monitoring failure.
- Off–The node is not configured for clustering or it has been disabled by the dual membership and detection recovery process in reaction to a control link or fabric link failure.

LINK/ACT LED, one for each of the two ports **CHASSIS CLUSTER CONTROL 0** and **CHASSIS CLUSTER CONTROL 1**:

- Green–Chassis cluster control port link is active.
- Off–No link.

Modular Port Concentrator (SRX5K-MPC) Specifications

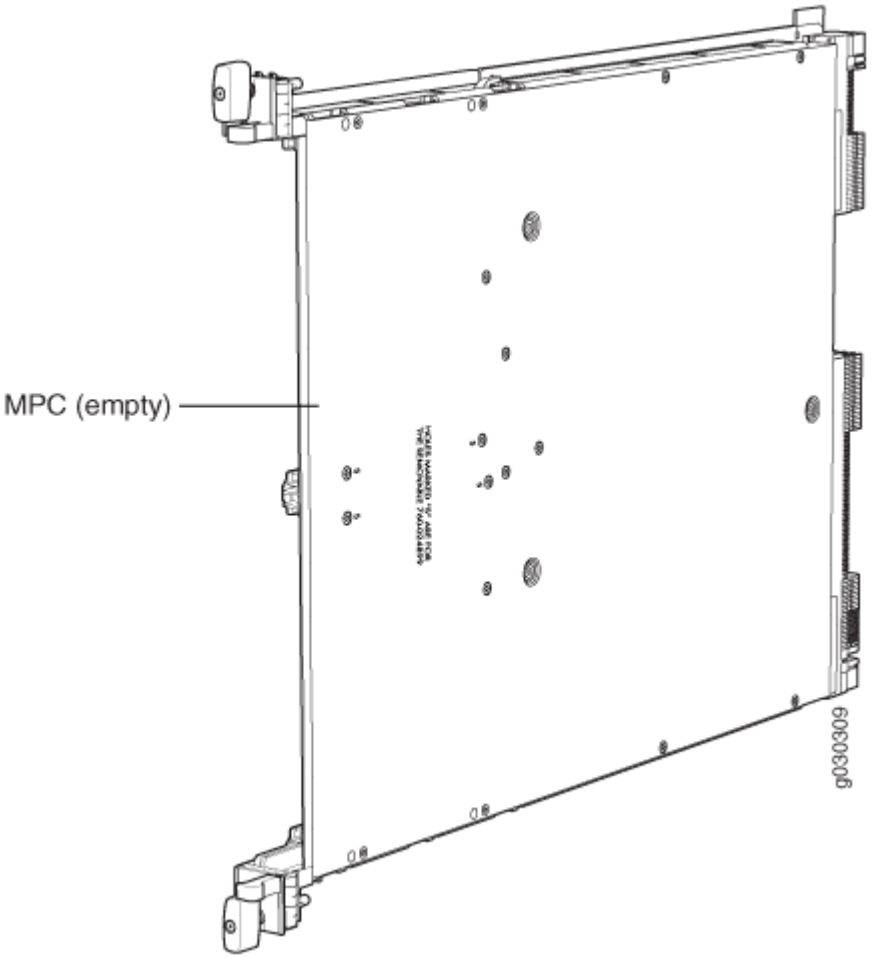
The SRX5K-MPC (see Figure 58 on page 131) is an interface card with two slots that accept MICs. These MICs add Ethernet ports to your firewall. An MPC with MICs installed functions in the same way as a regular IOC but allows you to add different types of Ethernet ports to your firewall. MPCs and MICs are similar in form and function to Flex IOCs and port modules. However, the two use different form-factors, so you cannot install port modules in an MPC, nor can you install MICs in a Flex IOC.

You must install at least one interface card in the firewall. The interface card can be of any of the available IOC, Flex IOC, or MPC types. You can add just one MIC; or you can add two MICs of the same or different types.

You can install MPCs in any of the slots that are not reserved for Switch Control Boards (SCBs).

If a slot in the SRX5400, SRX5600, or SRX5800 Firewall card cage is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the firewall. If a slot in an MPC is not occupied by a MIC, you must install a blank panel in the empty MIC slot to shield it and to allow cooling air to circulate properly through the MPC.

Figure 58: SRX5K-MPC



NOTE: When installing an SRX5K-MPC in an SRX5600 or SRX5800 Firewall:

- If the `session-distribution-mode` has not been explicitly configured using the CLI command:

  `user@host` **set security forwarding-process application-services session-distribution-mode**

  The SRX5K-MPC defaults to hash-based mode automatically even if existing SRX5K-MPC or non-MPCs are installed. You cannot set the `session-distribution-mode` to `normal`.

- If the `session-distribution-mode` has been explicitly configured to `normal`, and the MIC is installed in the device, then the SRX5K-MPC will remain offline, and the firewall generates a major alarm and logs the event for troubleshooting. You must explicitly configure the `session-distribution-mode` using the CLI command:

user@host **set security forwarding-process application-services session-distribution-mode hash-based**

When installing an SRX5K-MPC in an SRX5400 Firewall, the `session-distribution-mode` will only function when `hash-based` mode is configured or set as the default. The normal mode is not supported.

A 9% drop is observed for PPS (throughput) when moving from session mode to hash mode (for SRX5K-MPC or non-MPCs), whereas no drop in performance is observed on CPS (connection per second) and session capacity numbers.

For more information about the CLI command, see the Junos OS documentation at www.juniper.net/documentation/.

Description	• MPC with slots for two MICs • Maximum throughput: 75 Gbps per slot from Junos OS Release 12.1X46-D10 and later 120 Gbps per slot from Junos OS Release 12.1x47-D15 and later
Software release	Junos OS Release 12.1x46-D10
Cables and connectors	Slots for two MICs
Controls	One ejector knob each for MIC slots **0** and **1**. Pull the ejector knob to unseat and partially eject the adjacent MIC.
Supported slots	• SRX5400–Any slot except bottom slot **0** • SRX5600–Any slot except bottom slots **0** or **1** • SRX5800–Any slot except center slots **0** or **1**

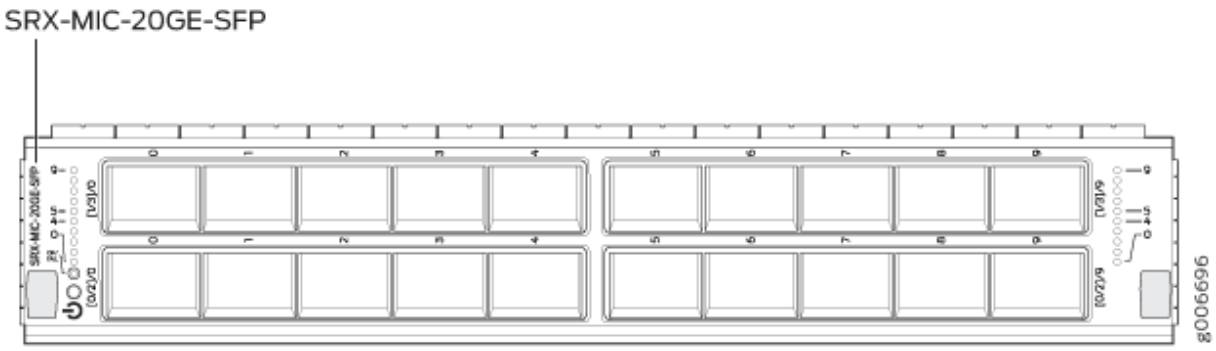
Power requirement	Maximum of 570 W for the MPC with two MICs, including applicable transceivers. **NOTE**: • To install and use SRX5K-MPCs in the SRX5600 and SRX5800 Firewalls, you must have high-capacity power supplies (either AC or DC) and high-capacity fan trays installed in the firewalls. All models of SRX5400 Firewalls already include high-capacity supplies. If you do not have high-capacity power supplies and fan trays installed, the firewall will log an alarm condition when it recognizes the SRX5K-MPCs. • On SRX5400 and SRX5600 Firewalls with AC power supplies, we recommend that you use high-line (220 V) input power to ensure that the devices have adequate power to support SRX5K-MPCs.
Weight	Approximately 10 lb (4.5 kg) without MICs
LEDs	**OK/FAIL** LED, one bicolor: • Green–The MPC is operating normally. • Blinking green–The MPC is transitioning to online or offline. • Red–The MPC has failed and is not operating normally. • Off–The MPC is powered down.
Serial number location	The serial number label is yellow and is located on the opposite side of the card.

MIC with 20x1GE SFP Interfaces (SRX-MIC-20GE-SFP)

You use Modular Interface Cards (MICs) and Modular Port Concentrators (MPCs) to add different combinations of Ethernet interfaces to your firewall to suit the specific needs of your network.

The SRX-MIC-20GE-SFP MIC (see Figure 59 on page 134) can be installed in the SRX-5K MPC to add twenty 1-Gigabit Ethernet small form-factor pluggable (SFP) Ethernet ports.

Figure 59: SRX-MIC-20GE-SFP

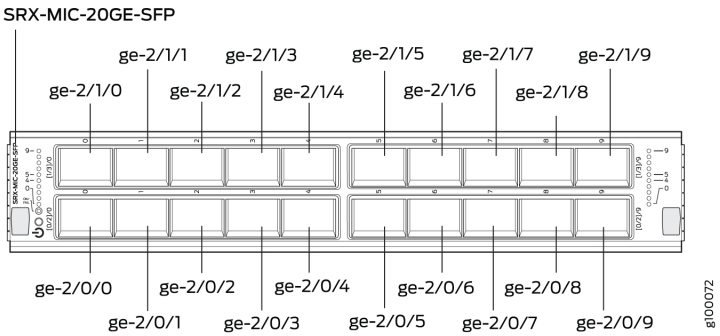


Description	• MIC with twenty 1-Gigabit Ethernet SFP Ethernet ports • Fits into either of the two slots of SRX-5K-MPC • Supports up to 20 Gbps of full-duplex traffic • Maximum configurable MTU: 9192 bytes • Maximum throughput: 20 Gbps
Software release	Junos OS Release 12.1X47-D10
Cables and connectors	Sockets for 20 SFP Gigabit Ethernet transceivers. Supported SFP transceivers: 1000BASE-LX (model numbers SRX-SFP-1GE-LX, SRX-SFP-1GE-LX-ET) 1000BASE-SX (model numbers SRX-SFP-1GE-SX, SRX-SFP-1GE-SX-ET) 1000BASE-T (model numbers SRX-SFP-1GE-T, SRX-SFP-1GE-T-ET)
Weight	Approximately 1.2 lb (0.54 kg)

LEDs	**OK/FAIL** LED, one bicolor: • Green–MIC is operating normally. • Red–MIC has failed. • Off–MIC is powered down. **LINK** LED, single color, one per SFP port: • Green–Link is active. • Off–Link is inactive.

Port and Interface Numbering	Each MPC accepts up to two MICs. SRX-MIC-20GE-SFP is a 20-port Gigabit Ethernet MIC with SFP.
	
	Each port on a MIC corresponds to a unique interface name in the CLI.
	
	In the syntax of an interface name, a hyphen (-) separates the media type from the *MPC* number (represented as an FPC in the CLI). The MPC slot number corresponds to the first number in the interface. The second number in the interface corresponds to the logical PIC number. The last number in the interface matches the port number on the MIC. Slashes (/) separate the MPC number from the logical PIC number and port number:
	
	type-*fpc*/*pic*/*port*
	
	• *type*—Media type, which identifies the network device. For example:
	  • ge—Gigabit Ethernet interface
	  • so—SONET/SDH interface
	  • xe—10-Gigabit Ethernet interface
	  For a complete list of media types, see Interface Naming Overview.
	• *fpc*—Slot in which the MPC is installed in an SRX5400, SRX5600, or SRX5800 Firewall.
	• *pic*—Two Logical PICs on the *MIC*, numbered 0 or 1 when installed in the first slot, and 2 or 3 when installed in the second slot.
	• *port*—Port number.
	
	Figure 60 on page 137 shows the SRX-MIC-20GE-SFP MIC installed in slot **0** of an MPC in slot 2 of an SRX5400, SRX5600, or SRX5800 Firewall.

Figure 60: SRX-MIC-20GE-SFP Interface Port Mapping



The SRX-MIC-20GE-SFP MIC contains two logical PICs, numbered `PIC 0` through `PIC 1` in the CLI. Each logical PIC contains 10 ports numbered **0** through **9**.

The sample output of the `show chassis fpc pic-status` command output displays two 20-port Gigabit Ethernet MICs with SFP — inserted into the slots of an MPC in slot `2`.

The logical PICs of the two MICs— `10x 1GE(LAN) SFP` — are shown as `PIC 0`, `PIC 1`, `PIC 2`, and `PIC 3`.

```
user@host> show chassis hardware
node1:
--------------------------------------------------------------------
------
Slot 1   Online       SRX5k SPC II
  PIC 0  Online       SPU Cp
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 2   Online       SRX5k IOC II
  PIC 0  Online       10x 1GE(LAN) SFP
  PIC 1  Online       10x 1GE(LAN) SFP
  PIC 2  Online       10x 1GE(LAN) SFP
  PIC 3  Online       10x 1GE(LAN) SFP

{primary:node1}
```

The `show interfaces terse` command output displays the Gigabit Ethernet interfaces that correspond to all the ports located on the two MICs.

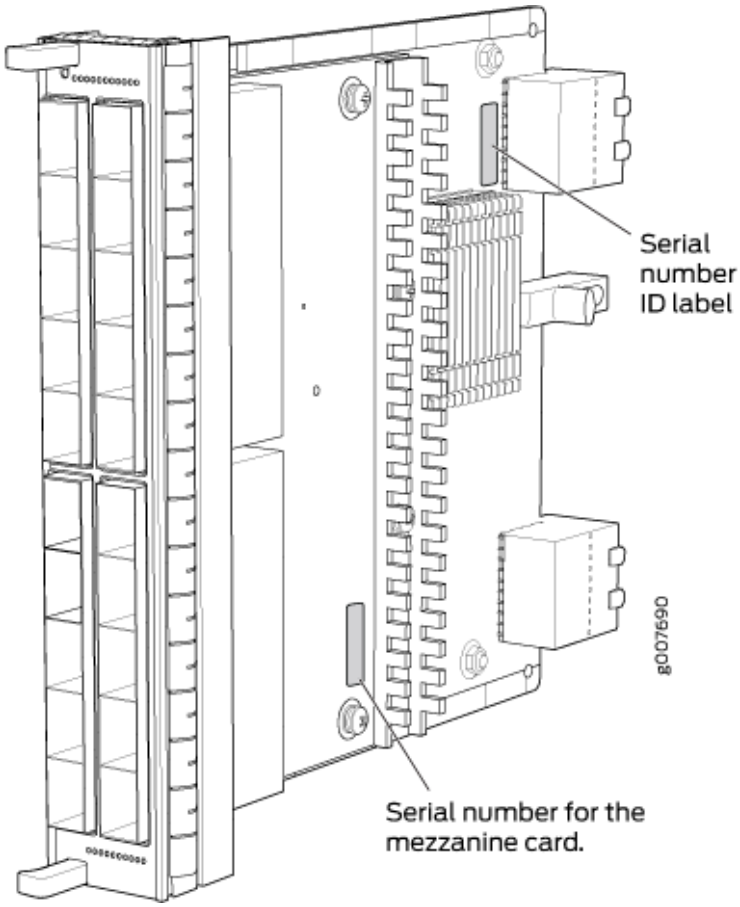
```
user@host> show interfaces terse

Interface               Admin Link Proto    Local
Remote
gr-0/0/0                up    up
ip-0/0/0                up    up
lt-0/0/0                up    up
ge-2/0/0                up    up
ge-2/0/1                up    down
ge-2/0/2                up    down
ge-2/0/3                up    down
ge-2/0/4                up    down
ge-2/0/5                up    up
ge-2/0/6                up    down
ge-2/0/7                up    down
ge-2/0/8                up    up
ge-2/0/9                up    up
ge-2/1/0                up    down
ge-2/1/1                up    up
ge-2/1/2                up    down
ge-2/1/3                up    down
ge-2/1/4                up    up
ge-2/1/5                up    down
ge-2/1/6                up    down
ge-2/1/7                up    down
ge-2/1/8                up    up
ge-2/1/9                up    up
ge-2/2/0                up    down
ge-2/2/1                up    down
ge-2/2/2                up    down
ge-2/2/3                up    down
ge-2/2/4                up    down
ge-2/2/5                up    down
ge-2/2/6                up    down
ge-2/2/7                up    down
ge-2/2/8                up    down
ge-2/2/9                up    down
ge-2/3/0                up    down
ge-2/3/1                up    down
ge-2/3/2                up    down
ge-2/3/3                up    down
ge-2/3/4                up    down
ge-2/3/5                up    down
ge-2/3/6                up    down
ge-2/3/7                up    down
```

```
ge-2/3/8                up    down
ge-2/3/9                up    down
```

Serial number location

The serial number label is yellow and is located as shown in Figure 61 on page 139.

Figure 61: SRX-MIC-20GE-SFP Serial Number Label

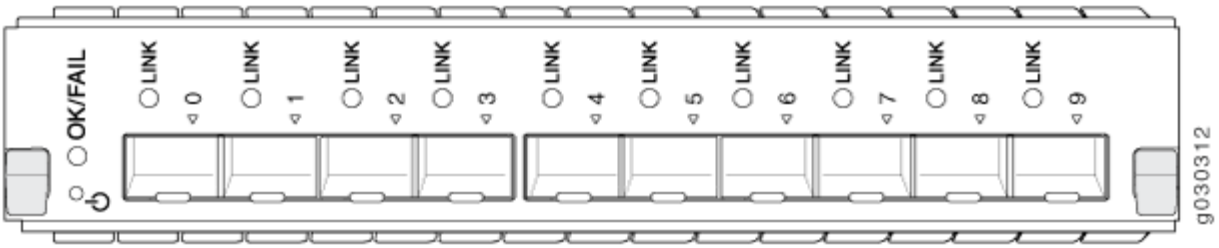


NOTE: The serial number for the mezzanine card is shown only for reference and is never used for any purpose.

MIC with 10x10GE SFP+ Interfaces (SRX-MIC-10XG-SFPP)

You use MICs and MPCs to add different combinations of Ethernet interfaces to your firewall to suit the specific needs of your network. The SRX-MIC-10XG-SFPP (see Figure 62 on page 140) can be installed in an MPC to add ten 10-Gigabit Ethernet SFP+ ports.

Figure 62: SRX-MIC-10XG SFPP



Description	• MIC with ten SFP+ 10-Gigabit Ethernet ports • Fits into MPC • Supports up to 100 Gbps of full-duplex traffic • Maximum configurable MTU: 9192 bytes • Maximum throughput: 100 Gbps
Software release	Junos OS Release 12.1X46-D10
Cables and connectors	Sockets for ten 10-Gbps SFP+ transceivers See Hardware Compatibility Tool for the transceivers supported.
Supported slots	Either slot in SRX5K-MPC
Weight	Approximately 1.6 lb (0.7 kg)

LEDs	**OK/FAIL** LED, one bicolor: • Green–The MIC is operating normally. • Red–The MIC has failed and is not operating normally. • Off–The MIC is powered down. **LINK** LED, single color: • Green–The link is active. • Off–No link.

Port and Interface Numbering

Each port on a MIC corresponds to a unique interface name in the CLI.

In the syntax of an interface name, a hyphen (-) separates the media type from the *MPC* number (represented as an FPC in the CLI). The MPC slot number corresponds to the first number in the interface. The second number in the interface corresponds to the logical PIC number. The last number in the interface matches the port number on the MIC. Slashes (/) separate the MPC number from the logical PIC number and port number:

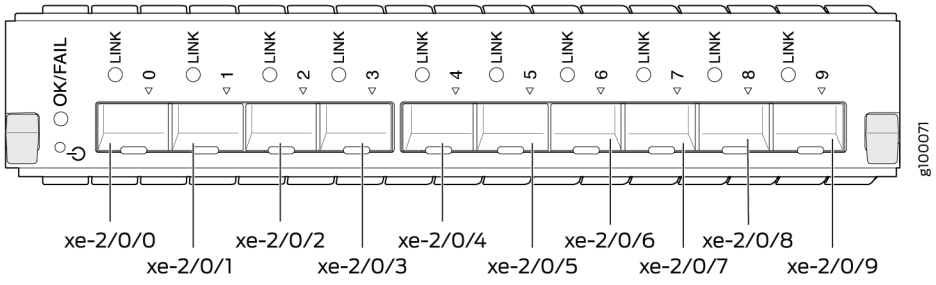
type-fpc/pic/port

- *type*—Media type, which identifies the network device. For example:
  - ge—Gigabit Ethernet interface
  - so—SONET/SDH interface
  - xe—10-Gigabit Ethernet interface

  For a complete list of media types, see Interface Naming Overview.
- *fpc*—Slot in which the MPC is installed in an SRX5400, SRX5600, or SRX5800 Firewall.
- *pic*—Logical PIC on the *MIC*, numbered 0 when installed in the first slot or 2 when installed in the second slot.
- *port*—Port number.

Figure 63 on page 142 shows the port and interface numbering of an SRX-MIC-10XG-SFPP MIC when it is installed in slot **0** of an MPC in slot 2 of an SRX5400, SRX5600, or SRX5800 Firewall.

Figure 63: SRX-MIC-10XG-SFPP Port and Interface Numbering



The SRX-MIC-10XG-SFPP MIC contains one logical PIC, numbered PIC 0 in the CLI when inserted in the first slot of the MPC or PIC 2 when inserted in the second slot of the MPC. Each logical PIC contains 10 ports numbered **0** through **9**.

The sample output of the `show chassis fpc pic-status` command displays two 10-port 10-Gigabit Ethernet MICs with SFP+ — inserted into the slots of an MPC in slot `2`.

The logical PICs of the two MICs— `10x 10GE SFP+` — are shown as `PIC 0` and `PIC 2`.

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

Slot 1   Online       SRX5k SPC II
  PIC 0  Online       SPU Cp
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 2   Online       SRX5k IOC II
  PIC 0  Online       10x 10GE SFP+
  PIC 2  Online       10x 10GE SFP+
```

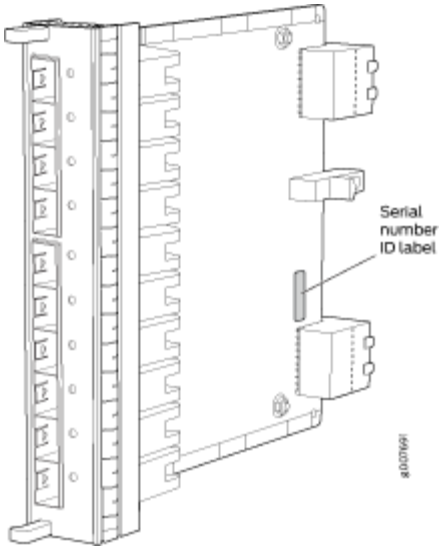
The `show interfaces terse` command output displays the 10–Gigabit Ethernet interfaces that correspond to the 10 ports located on each MIC.

```
user@host> show interfaces terse

Interface               Admin Link Proto    Local                 Remote
gr-0/0/0                up    up
ip-0/0/0                up    up
lt-0/0/0                up    up
xe-2/0/0                up    up
xe-2/0/1                up    up
xe-2/0/2                up    up
xe-2/0/2.0              up    up   inet     131.131.131.2/24
                                   inet6    1300::2/64
                                            fe80::224:dcff:fe20:b94c/64
                                   multiservice
xe-2/0/3                up    up
xe-2/0/4                up    up
xe-2/0/5                up    up
xe-2/0/6                up    up
xe-2/0/6.0              up    up   inet     141.141.141.1/24
                                   inet6    1400::1/64
                                            fe80::224:dcff:fe20:b950/64
                                   multiservice
xe-2/0/7                up    down
xe-2/0/8                up    down
xe-2/0/9                up    down
xe-2/2/0                up    down
xe-2/2/1                up    down
xe-2/2/2                up    down
```

```
xe-2/2/3                up    down
xe-2/2/4                up    down
xe-2/2/5                up    down
xe-2/2/6                up    down
xe-2/2/7                up    down
xe-2/2/8                up    down
xe-2/2/9                up    down
```

Serial number location	The serial number label is yellow and located as shown in Figure 64 on page 144.

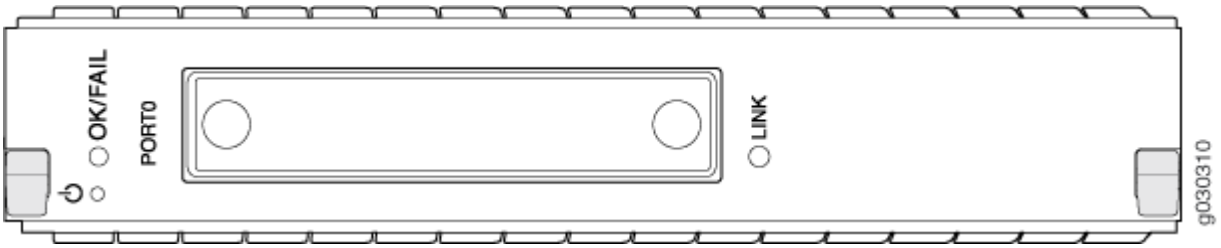
Figure 64: SRX-MIC-10XG-SFPP Serial Number Label



MIC with 1x100GE CFP Interface (SRX-MIC-1X100G-CFP)

You use MICs and MPCs to add different combinations of Ethernet interfaces to your firewall to suit the specific needs of your network. The SRX-MIC-1X100G-CFP (see Figure 65 on page 145) can be installed in an MPC to add one 100-Gigabit Ethernet CFP port.

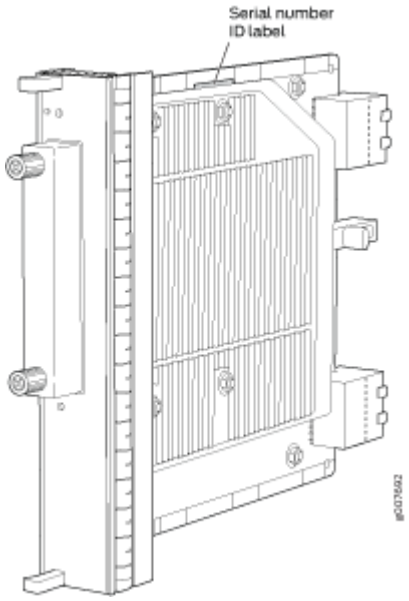
Figure 65: SRX-MIC-1X100G-CFP



Description	• MIC with one CFP 100-Gigabit Ethernet port • Fits into MPC • Supports up to 100 Gbps of full-duplex traffic • Maximum configurable MTU: 9192 bytes • Maximum throughput: 100 Gbps
Software release	Junos OS Release 12.1X46-D10
Cables and connectors	One socket for a 100-Gigabit CFP transceiver. Supported CFP transceivers: • 100GBASE-LR4 (model number: SRX-CFP-100G-LR4) • 100GBASE-SR10 (model number: SRX-CFP-100G-SR10)
Supported slots	Either slot in SRX5K-MPC
Weight	Approximately 1.6 lb (0.7 kg)

LEDs	**OK/FAIL** LED, one bicolor: • Green–The MIC is operating normally. • Red–The MIC has failed and is not operating normally. • Off–The MIC is powered down. **LINK** LED, single color: • Green–The link is active. • Off–No link.
Serial number location	The serial number label is yellow and located as shown in Figure 66 on page 146.

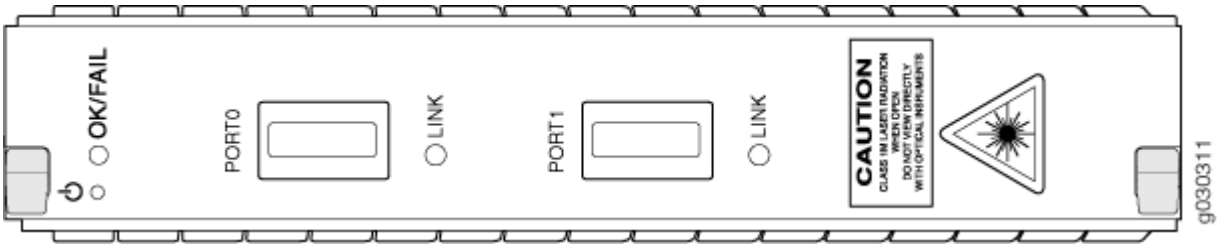
Figure 66: SRX-MIC-1X100G-CFP Serial Number Label



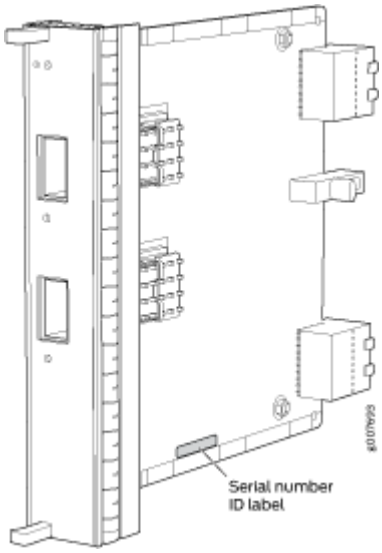
MIC with 2x40GE QSFP+ Interfaces (SRX-MIC-2X40G-QSFP)

You use MICs and MPCs to add different combinations of Ethernet interfaces to your firewall to suit the specific needs of your network. The SRX-MIC-2X40G-QSFP (see Figure 67 on page 147) can be installed in an MPC to add two 40-Gigabit quad small form-factor pluggable (QSFP+) Ethernet ports.

Figure 67: SRX-MIC-2X40G QSFP



Description	• MIC with two QSFP+ Ethernet ports • Fits into MPC • Supports up to 80 Gbps of full-duplex traffic • Maximum configurable MTU: 9192 bytes • Maximum throughput: 80 Gbps
Software release	Junos OS Release 12.1X46-D10
Cables and connectors	Sockets for two QSFP+ 40-Gigabit Ethernet fiber-optic transceivers. Supported QSFP+ transceiver: 40GBASE-SR4 (model number SRX-QSFP-40G-SR4) 40GBASE-LR4 (model number SRX-QSFP-40G-LR4)
Supported slots	Either slot in SRX5K-MPC
Weight	Approximately 1.6 lb (0.7 kg)

LEDs	**OK/FAIL** LED, one bicolor: • Green–The MIC is operating normally. • Red–The MIC has failed and is not operating normally. • Off–The MIC is powered down. **LINK** LED, single color, one per QSFP+ port: • Green–The link is active. • Off–No link.
Serial number location	The serial number label is yellow and typically located as shown in Figure 68 on page 148. **Figure 68: SRX-MIC-2X40G-QSFP Serial Number Label** 

SRX5K-MPC3-40G10G Specifications

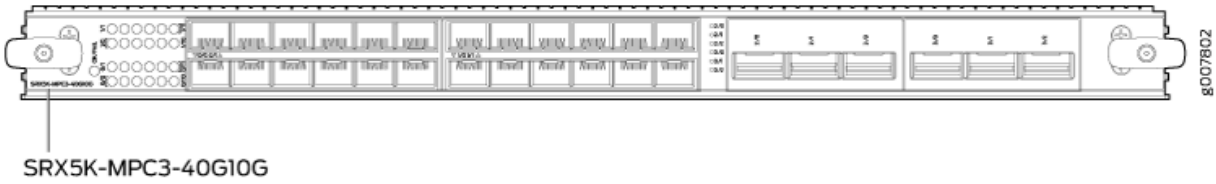
The SRX5K-MPC3-40G10G (IOC3) is an interface card that provides 10 Gigabit Ethernet and 40 Gigabit Ethernet interfaces, with a Packet Forwarding Engine that provides a 240 Gbps line rate. This interface card is supported on SRX5400, SRX5600, and SRX5800 Firewalls. See Figure 69 on page 149.

NOTE: These cards do not support plug-in Modular Interface Cards (MICs).

All ports on the interface card have dual-color LEDs for reporting link status.

The interface card also supports hot-pluggable optical modules.

Figure 69: SRX5K-MPC3-40G10G



If a slot in the SRX5400, SRX5600, or SRX5800 Firewall card cage is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the firewall.

Description	• Fixed-configuration MPC with six 40-Gigabit Ethernet ports and twenty-four 10-Gigabit Ethernet ports • Maximum throughput: 240 Gbps • Maximum configurable MTU: 9192 bytes
Software release	Junos OS Release 15.1X49-D10 and later
Supported Slots	• SRX5400 – Any slot, except the bottom slot **0** which is reserved for SCB/RE. • SRX5600 – Any slot, except the bottom slots **0** or **1** which are reserved for SCB/RE. • SRX5800 – Any slot, except the middle slots **0**, **1**, and **2/6** which are reserved for SCB/RE and slots **0** (left most) and **11** (right most). **NOTE**: You can use the 2/6 slot to install an interface card if an SCB is not already installed in it.

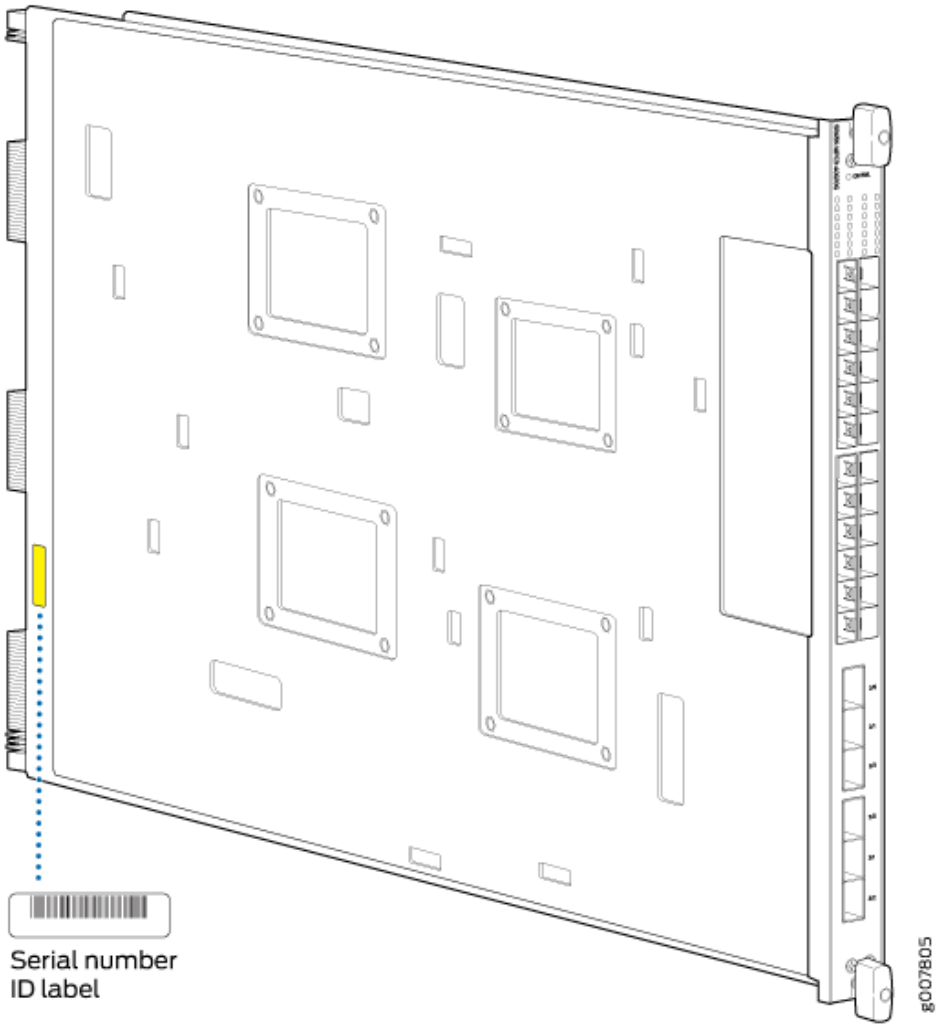
Cables and connectors	Sockets for 40-Gbps and 10-Gbps SFP+ transceivers See Hardware Compatibility Tool for the transceivers supported.
Power requirements	Typical: 9.68 A @ 48 V (460 W) At different temperatures: • 55° C: 607 W • 40° C: 541 W • 25° C: 511 W
Weight	21 lb (9.52 kg)

Hardware features	• Line-rate throughput of up to 240 Gbps
	• Supports up to 32,000 queues per-slot
	• LAN-PHY mode at 10.3125 Gbps on a per-port basis
	• The ports are labeled as:
	  • 10-Gigabit Ethernet ports: 0/0 through 0/11 and 1/0 through 1/11
	  • 40-Gigabit Ethernet ports: 2/0 through 2/2 and 3/0 through 3/2

Software features	• Optical diagnostics and related alarms • Two packet-forwarding engines, PFE0 and PFE1. PFE0 hosts PIC0 and PIC2. PFE1 hosts PIC1 and PIC3. • Configurable LAN-PHY mode options per 10-Gigabit Ethernet port • Intelligent oversubscription services **NOTE**: At any one time you can have only one of the following PIC combinations powered on: • PIC0 & PIC1 • PIC0 & PIC3 • PIC2 & PIC1 • PIC2 & PIC3 If you configure any of the following invalid PIC combinations, the chassis will set PIC0 & PIC1 combination online. • PIC0 & PIC2 • PIC1 & PIC3
LEDs	OK/FAIL LED, one bicolor: • Solid green—MPC is functioning normally. • Blinking green—MPC is transitioning online or offline. • Red—MPC has failed. 10-Gigabit Ethernet LINK LED, one green per port: • Green—Link is up. • Off—Link is down or disabled. 40-Gigabit Ethernet LINK LED, one bicolor per port: • Green—Link is up. • Amber—Link is disabled. • Off—Link is down.

Serial Number Location	The serial number label is located as shown in Figure 70 on page 152.

Figure 70: SRX5K-MPC3-40G10G Serial Number Label



SRX5K-MPC3-100G10G Specifications

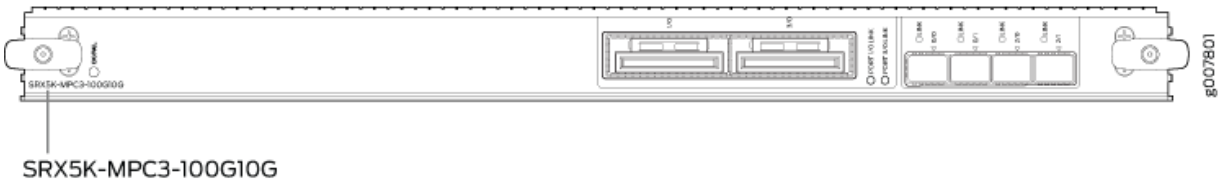
The SRX5K-MPC3-100G10G (IOC3) is an interface card that provides 100 Gigabit Ethernet and 10 Gigabit Ethernet interfaces, with a Packet Forwarding Engine that provides a 240 Gbps line rate. This interface card is supported on SRX5400, SRX5600, and SRX5800 Firewalls. See Figure 71 on page 153.

NOTE: These cards do not support plug-in Modular Interface Cards (MICs).

All ports on the interface card have dual-color LEDs for reporting link status.

The interface card also supports hot-pluggable optical modules.

Figure 71: SRX5K-MPC3-100G10G



If a slot in the SRX5400, SRX5600, or SRX5800 Firewall card cage is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the firewall.

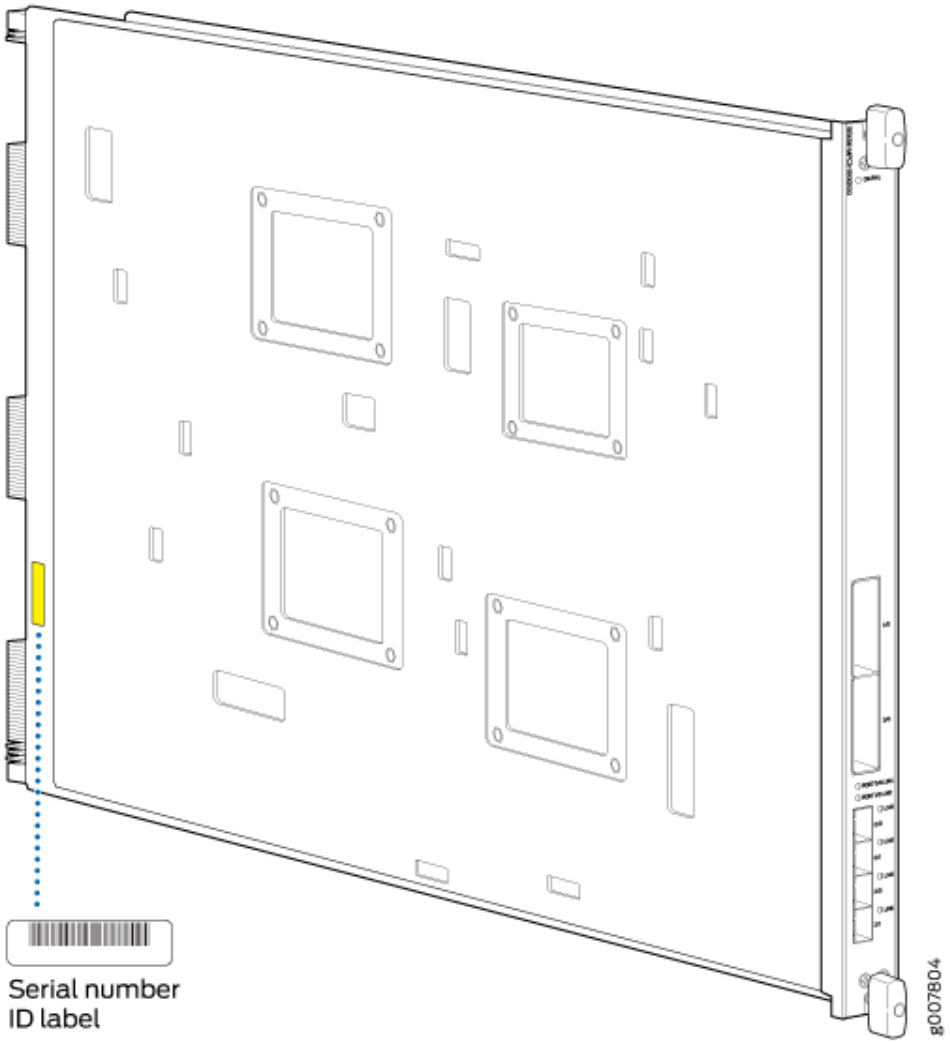
Description	• Fixed-configuration MPC with two 100-Gigabit Ethernet ports and four 10-Gigabit Ethernet ports • Maximum throughput: 240 Gbps • Maximum configurable MTU: 9192 bytes
Software release	Junos OS Release 15.1X49-D10 and later
Supported Slots	• SRX5400 – Any slot, except the bottom slot **0** which is reserved for SCB/RE. • SRX5600 – Any slot, except the bottom slots **0** or **1** which are reserved for SCB/RE. • SRX5800 – Any slot, except the middle slots **0**, **1**, and **2/6** which are reserved for SCB/RE and slots **0** (left most) and **11** (right most). **NOTE**: You can use the 2/6 slot to install an interface card if an SCB is not already installed in it.
Cables and connectors	Sockets for 100-Gbps and 10-Gbps SFP+ transceivers See Hardware Compatibility Tool for the transceivers supported.

Power requirements	• Typical: 10.52 A @ 48 V (505 W) At different temperatures: • 55° C: 607 W • 40° C: 541 W • 25° C: 511 W
Weight	21 lb (9.52 kg)
Hardware features	• Line-rate throughput of up to 240 Gbps • Supports up to 32,000 queues per-slot • LAN-PHY mode at 10.3125 Gbps on a per-port basis The ports are labeled as: • 10-Gigabit Ethernet ports: 0/0, 0/1, 2/0, and 2/1 • 100-Gigabit Ethernet ports: 1/0 and 3/0
Software features	• Configurable LAN-PHY mode options per 10-Gigabit Ethernet port • Optical diagnostics and related alarms • Intelligent oversubscription services

LEDs	OK/FAIL LED, one bicolor: • Solid green—MPC is functioning normally. • Blinking green—MPC is transitioning online or offline. • Red—MPC has failed. 10-Gigabit Ethernet LINK LED, one bicolor per port: • Green—Link is up. • Amber—Link is disabled. • Off—Link is down or disabled. 100-Gigabit Ethernet LINK LED, one bicolor per port: • Green—Link is up. • Amber—Link is disabled. • Off—Link is down.

Serial Number Location	The serial number label is located as shown in Figure 72 on page 156.

Figure 72: SRX5K-MPC3-100G10G Serial Number Label

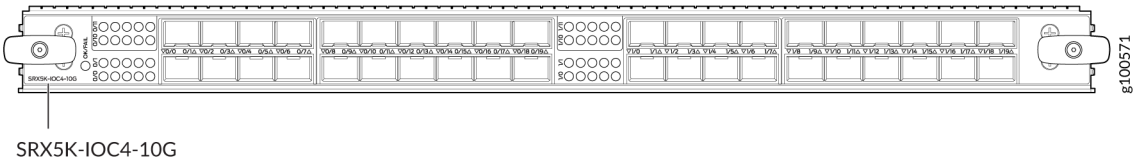


SRX5K-IOC4-10G Specifications

SRX5K-IOC4-10G is a fixed-configuration interface card with a Packet Forwarding Engine that provides 400-Gbps line rate. This interface card provides scalability in bandwidth and services to the SRX5400, SRX5600 and SRX5800 Firewalls. See Figure 73 on page 157.

NOTE: SRX5K-IOC4-10G cards do not support plug-in Modular Interface Cards (MICs).

Figure 73: SRX5K-IOC4-10G



If a slot in the SRX5400, SRX5600, or SRX5800 Firewall card cage is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the firewall.

Description	• Fixed-configuration IOC with forty 10-Gbps port speeds • Maximum throughput: 400-Gbps • Maximum configurable MTU: 9192 bytes
Software release	Junos OS Release 19.3R1 and later
Supported slots	• SRX5400—Any slot, except the bottom slots **0** and **1/0**, which are reserved for SCB/RE. **NOTE**: Slot **1/0** is a dual purpose slot. You can install SRX5K-IOC4-10G in slot **1/0** if an SCB is not already installed in it. • SRX5600—Any slot, except the bottom slots **0** and **1**, which are reserved for SCB/RE. • SRX5800—Any slot, except the middle slots **0**, **1**, and **2/6**, which are reserved for SCB/RE, and slots **0** (most left) and **11** (most right). **NOTE**: Slot **2/6** is a dual purpose slot. You can install SRX5K-IOC4-10G in slot **2/6** if an SCB is not already installed in it.

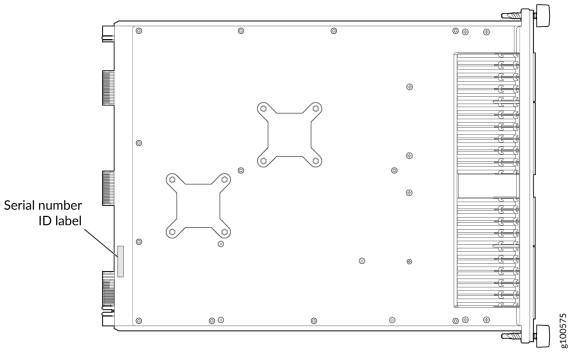
Cables and connectors	See Hardware Compatibility Tool for the transceivers supported.
Power requirements	• Typical: 405 W At different temperatures: • 131° F (55° C): 500 W • 104° F (40° C): 465 W • 75° F (25° C): 430 W
Weight	17 lb (7.7 kg)

Hardware features	• Junos Trio chipsets for increased scaling for bandwidth, subscribers, and services
	• Forty 10-Gigabit Ethernet ports. The ports support SFP+ transceivers.
	• Requires high-capacity power supplies and high-capacity fan trays.
	• The ports are labeled as (seeFigure 73 on page 157):
	  • **0/0** through **0/9**
	  • **0/10** through **0/19**
	  • **1/0** through **1/9**
	  • **1/10** through **1/19**

Software features	• Application security • Application Layer Gateway (ALG) • Attack detection and prevention • Class of service (CoS) • Equal-cost multipath (ECMP) load balancing • GPRS Tunneling Protocol (GTP) • High availability (chassis cluster) • Intrusion detection and prevention (IDP) • IPsec VPN • Layer 2 transparent mode • Logical systems • Network Address Translation (NAT) • Routing protocols (BFD, BGP, IGMP, IS-IS, MLD, Multicast, OSPF, PIM, RIP, and SCTP) • SSL proxy • Tenant systems • Content Security
LEDs	**OK/FAIL** LED, one bicolor: • Steady green—IOC is functioning normally. • Yellow—IOC has failed. **LINK** LED, one green per port: • Steady green—Link is up. • Off—Link is down or disabled.

Serial Number Location	The serial number label is located as shown in Figure 74 on page 160.

Figure 74: SRX5K-IOC4-10G Serial Number Label

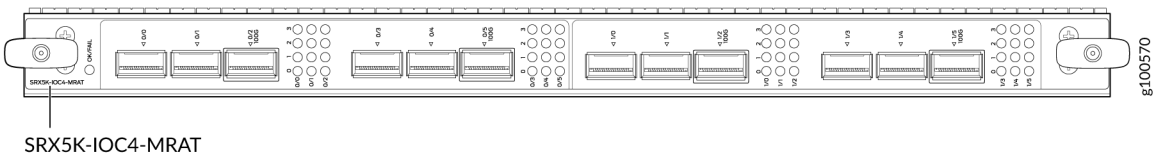


SRX5K-IOC4-MRAT Specifications

SRX5K-IOC4-MRAT is a fixed-configuration interface card with a Packet Forwarding Engine that provides up to 480-Gbps (240-Gbps per PIC slot) line rate. This interface card provides scalability in bandwidth and services to the SRX5400, SRX5600, and SRX5800 Firewalls. See Figure 75 on page 160.

NOTE: SRX5K-IOC4-MRAT cards do not support plug-in Modular Interface Cards (MICs).

Figure 75: SRX5K-IOC4-MRAT



If a slot in the SRX5400, SRX5600, or SRX5800 Firewall card cage is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the firewall.

Description	• Fixed-configuration IOC with 10-Gbps, 40-Gbps, and 100-Gbps port speeds • Maximum throughput: up to 480 Gbps (240 Gbps per PIC slot) • Maximum configurable MTU: 9192 bytes
Software release	Junos OS Release 19.3R1 and later
Supported Slots	• SRX5400—Any slot, except the bottom slots **0** and **1/0**, which are reserved for SCB/RE. **NOTE**: Slot **1/0** is a dual purpose slot. You can install SRX5K-IOC4-MRAT in slot **1/0** if an SCB is not already installed in it. • SRX5600—Any slot, except the bottom slots **0** and **1**, which are reserved for SCB/RE. • SRX5800—Any slot, except the middle slots **0**, **1**, and **2/6**, which are reserved for SCB/RE, and slots **0** (most left) and **11** (most right). **NOTE**: Slot **2/6** is a dual purpose slot. You can install SRX5K-IOC4-MRAT in slot **2/6** if an SCB is not already installed in it.
Cables and connectors	See Hardware Compatibility Tool for the transceivers supported.
Power requirements	At different temperatures: • 131° F (55° C): 545 W • 104° F (40° C): 465 W • 75° F (25° C): 430 W

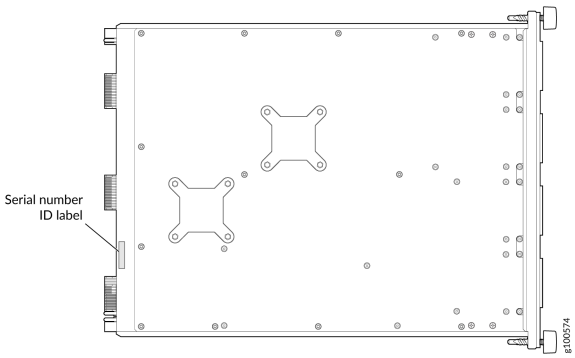
Weight	15.7 lb (7.12 kg)

Hardware features	• Junos Trio chipsets for increased scaling for bandwidth, subscribers, and services
	• Twelve Gigabit Ethernet ports that can be configured as 40-Gigabit Ethernet port or as 4X10-Gigabit Ethernet port using a breakout cable. The ports support quad small-form factor pluggable plus (QSFP+) transceivers.
	• Four out of the twelve ports can be configured as 100-Gigabit Ethernet ports. Port numbers **0/2**, **0/5**, **1/2** and **1/5** are the four 100-Gigabit Ethernet ports.
	• You can configure different combination of port speeds as long as the aggregate capacity per group of six ports labeled **0/0** through **0/5** does not exceed 240 Gbps. Similarly, aggregate capacity per group of the other six ports labeled **1/0** through **1/5** should not exceed 240 Gbps.
	• Requires high-capacity power supplies and high-capacity fan trays.
	• The ports are labeled as (see Figure 75 on page 160):
	  • 10-Gigabit Ethernet or 40-Gigabit Ethernet ports:
	  0/0, **0/1**, **0/2 100G**, **0/3**, **0/4**, **0/5 100G**, **1/0**, **1/1**, **1/2 100G**, **1/3**, **1/4**, and **1/5 100G**
	  • 100-Gigabit Ethernet ports:
	  0/2 100G, **0/5 100G**, **1/2 100G** and **1/5 100G**
	NOTE: Only ports marked **100G** support 100-Gigabit Ethernet speed using QSFP28 transceivers.

Software features	• Application security • Application Layer Gateway (ALG) • Attack detection and prevention • Class of service (CoS) • Equal-cost multipath (ECMP) load balancing • GPRS Tunneling Protocol (GTP) • High availability (chassis cluster) • Intrusion detection and prevention (IDP) • IPsec VPN • Layer 2 transparent mode • Logical systems • Network Address Translation (NAT) • Routing protocols (BFD, BGP, IGMP, IS-IS, MLD, Multicast, OSPF, PIM, RIP, and SCTP) • SSL proxy • Tenant systems • Content Security
LEDs	**OK/FAIL** LED, one bicolor: • Steady green—IOC is functioning normally. • Yellow—IOC has failed. **LINK** LED, one green per port (4 per QSFP+ cage): • Steady green—Link is up. • Off—Link is down or disabled.

Serial Number Location	The serial number label is located as shown in Figure 76 on page 164.

Figure 76: SRX5K-IOC4-MRAT Serial Number Label



SRX5800 Firewall Interface Card Description

Interface cards are cards that support physical interfaces that you use to connect the firewall to your data network. Three different types of interface cards are available:

- I/O Cards (IOCs) have fixed interface ports on the front panel of the card.
- Flex I/O Cards (Flex IOCs) have slots on the front panel that accept smaller cards called port modules. Each port module has two or more physical interfaces on it. A Flex IOC with installed port modules functions in the same way as a regular IOC, but allows greater flexibility in adding different types of Ethernet ports to your firewall.
- Modular Port Concentrators (MPCs) have slots on the front panel that accept smaller cards called Modular Interface Cards (MICs). Each MIC has one or more physical interface on it. An MPC with MICs installed functions in the same way as a regular I/O card (IOC), but allows greater flexibility in adding different types of Ethernet ports to your firewall. MPCs and MICs are similar in form and function to Flex IOCs and port modules. However, the two use different form-factors, so you cannot install port modules in an MPC, nor can you install MICs in a Flex IOC.

For all interface card types, the card assembly combines packet forwarding and Ethernet interfaces on a single board. The interface cards interface with the power supplies and Switch Control Boards (SCBs).

You can install interface cards in any of the slots that are not reserved for SCBs. If a slot is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the firewall.

Figure 77 on page 165 shows typical IOCs supported on the firewall.

Figure 77: Typical IOCs

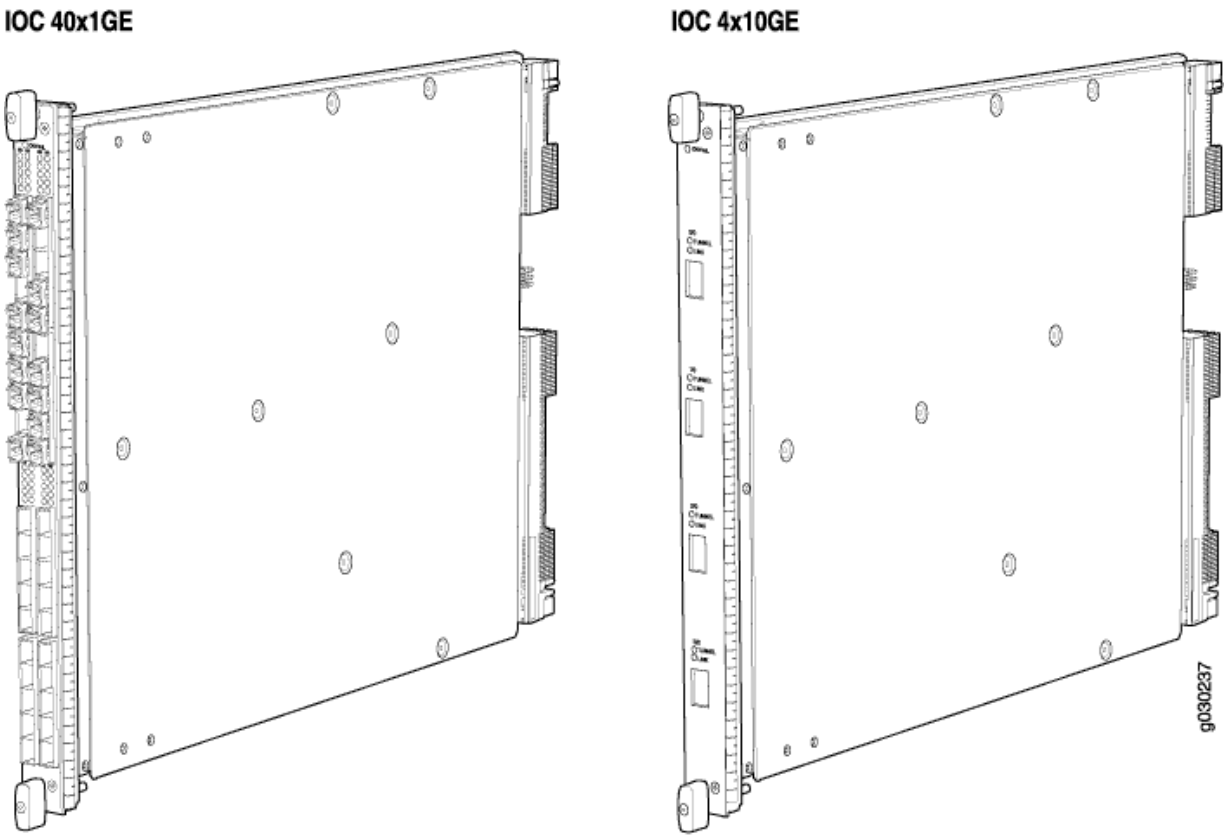


Figure 78 on page 166 shows a Flex IOC with two typical port modules installed.

Figure 78: Flex IOC with Port Modules

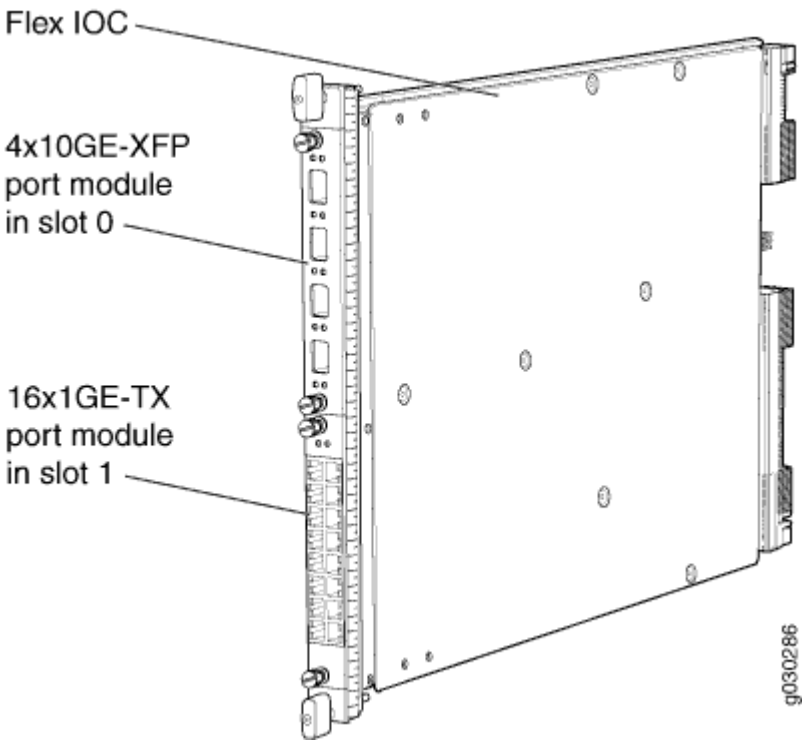
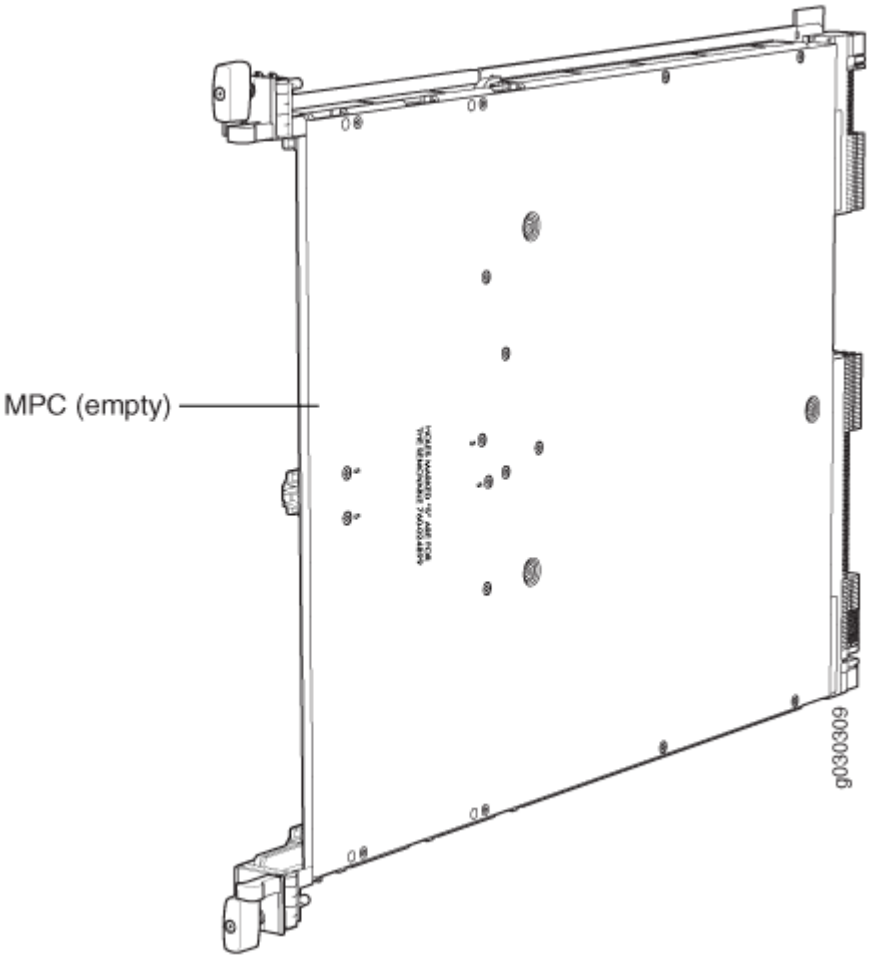


Figure 79 on page 167 shows an MPC.

Figure 79: SRX5K-MPC



For detailed information about the interface cards, port modules, and MICs supported by the firewall, see the *SRX5400, SRX5600, and SRX5800 Firewall Card Reference* at www.juniper.net/documentation/.

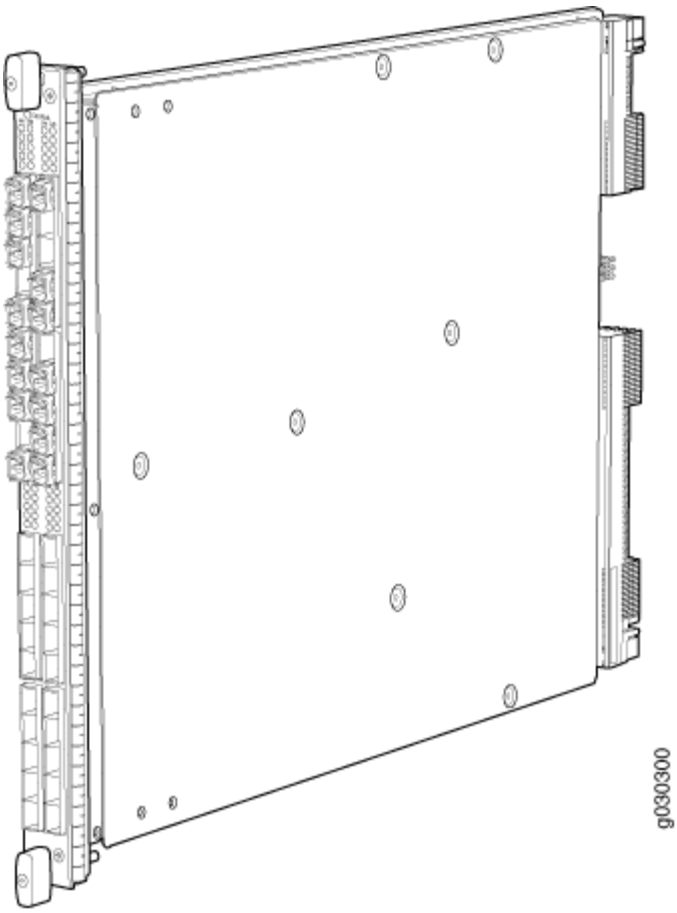
I/O Card SRX5K-40GE-SFP Specifications

The SRX5K-40GE-SFP I/O card (IOC) is optimized for Ethernet density and supports 40 Gigabit Ethernet ports (see Figure 80 on page 168). The IOC assembly combines packet forwarding and Ethernet interfaces on a single board, with four 10-Gbps Packet Forwarding Engines. Each Packet Forwarding Engine consists of one I-chip for Layer 3 processing and one Layer 2 network processor. The IOCs interface with the power supplies and Switch Control Boards (SCBs).

You must install at least one IOC in the firewall. The IOC can be of any of the available IOC or Flex IOC types.

You can install IOCs in any of the slots that are not reserved for Switch Control Boards (SCBs). If a slot is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the firewall.

Figure 80: IOC SRX5K-40GE-SFP

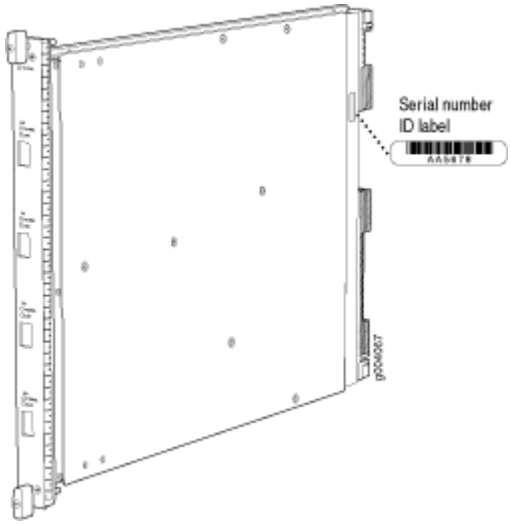


Description	• I/O card with 40 Gigabit Ethernet SFP ports • Maximum configurable MTU: 9192 bytes • Maximum throughput: 40 Gbps
Software release	• Junos OS Release 9.2 and later

Cables and connectors	40 Gigabit Ethernet SFP ports Supported SFP transceivers: 1000BASE-LH (model numbers SRX-SFP-1GE-LH, SRX-SFP-1GE-LH-ET) 1000BASE-LX (model numbers SRX-SFP-1GE-LX, SRX-SFP-1GE-LX-ET) 1000BASE-SX (model numbers SRX-SFP-1GE-SX, SRX-SFP-1GE-SX-ET) 1000BASE-T (model numbers SRX-SFP-1GE-T, SRX-SFP-1GE-T-ET)
Controls	None
Supported Slots	• SRX5600–Any slot except bottom slots **0** or **1** • SRX5800–Any slot except center slots **0**, **1**, or **2/6**
Power Requirement	312 W typical, 365 W maximum
Weight	Approximately 13 lb (5.9 kg)
LEDs	**OK/FAIL** LED, one bicolor: • Steady green–The IOC is operating normally. • Red–The IOC has failed and is not operating normally. • Off–The IOC is powered down.

Serial Number Location	The serial number label is located as shown in Figure 81 on page 170.

Figure 81: Serial Number Label (IOC Shown, Other Cards Similar)



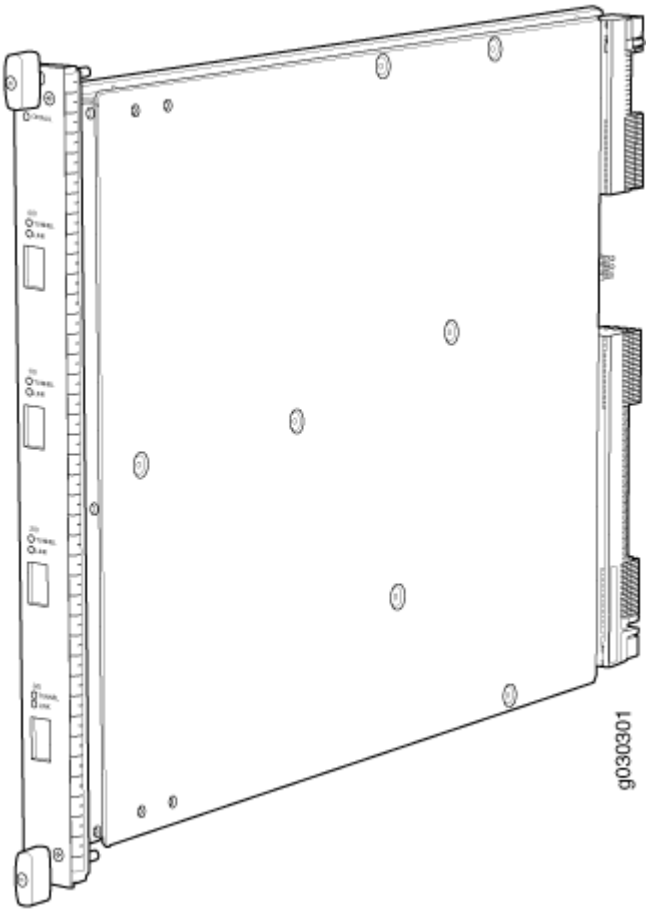
I/O Card SRX5K-4XGE-XFP Specifications

The SRX5K-4XGE-XFP I/O card (IOC) supports four 10-Gigabit Ethernet ports (see Figure 82 on page 171). The IOC assembly combines packet forwarding and Ethernet interfaces on a single board, with four 10-Gbps Packet Forwarding Engines. Each Packet Forwarding Engine consists of one I-chip for Layer 3 processing and one Layer 2 network processor. The IOCs interface with the power supplies and Switch Control Boards (SCBs).

You must install at least one IOC in the firewall. The IOC can be of any of the available IOC or Flex IOC types.

You can install IOCs in any of the slots that are not reserved for Switch Control Boards (SCBs). If a slot is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the firewall.

Figure 82: IOC SRX5K-4XGE-XFP

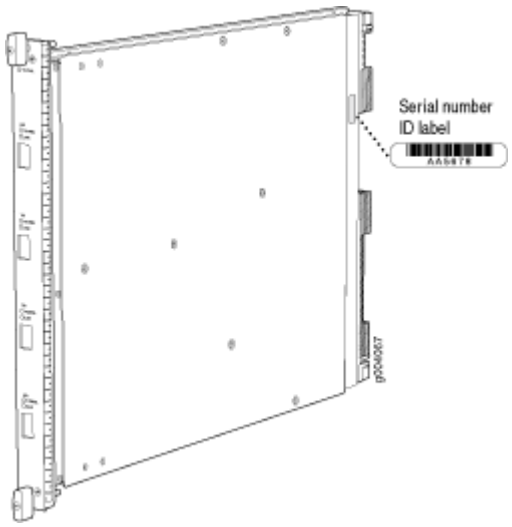


Description	• I/O card with four 10-Gigabit Ethernet XFP ports • Maximum configurable MTU: 9192 bytes • Maximum throughput: 40 Gbps
Software release	• Junos OS Release 9.2 and later

Cables and connectors	Four 10-Gbps XFP ports Supported XFP transceivers: 10GBASE-ER (model numbers SRX-XFP-10GE-ER and SRX-XFP-10GE-ER-ET) 10GBASE-LR (model numbers SRX-XFP-10GE-LR and SRX-XFP-10GE-LR-ET 10GBASE-SR (model numbers SRX-XFP-10GE-SR and SRX-XFP-10GE-SR-ET)
Controls	None
Supported Slots	• SRX5600–Any slot except bottom slots **0** or **1** • SRX5800–Any slot except center slots **0**, **1**, or **2**
Power Requirement	312 W typical, 365 W maximum
Weight	Approximately 13 lb (5.9 kg)
LEDs	**OK/FAIL** LED, one bicolor: • Steady green–The IOC is operating normally. • Red–The IOC has failed and is not operating normally. • Off–The IOC is powered down.

Serial Number Location	The serial number label is located as shown in Figure 83 on page 173.

Figure 83: SRX5K-4XGE-XFP Serial Number Label



Flex I/O Card (SRX5K-FPC-IOC) Specifications

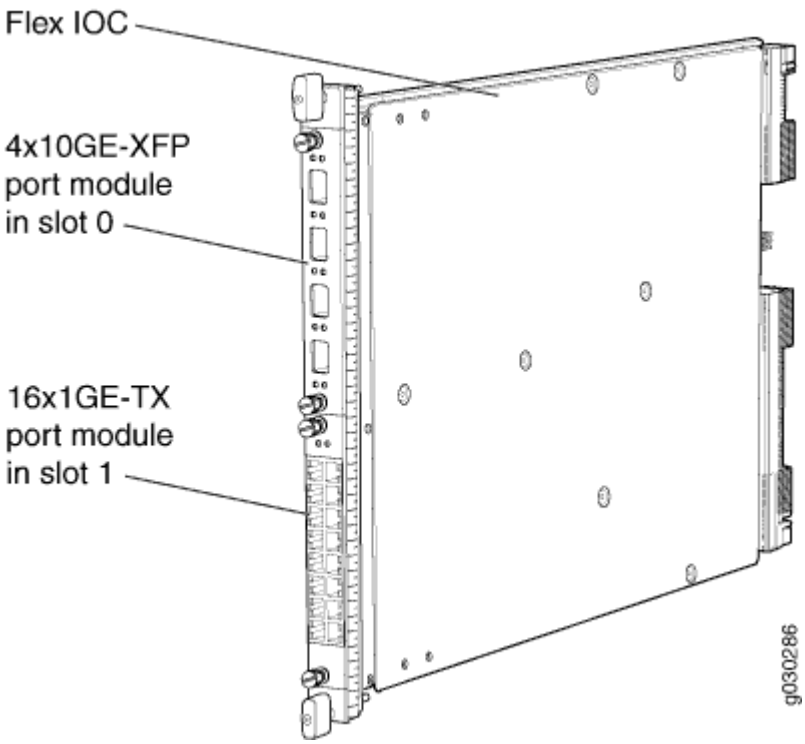
The SRX5K-FPC-IOC Flex I/O card (Flex IOC) (Figure 84 on page 174) is an IOC with two slots that accept port modules that add Ethernet ports to your firewall. A Flex IOC with installed port modules functions in the same way as a regular IOC, but allows greater flexibility in adding different types of Ethernet ports to your firewall.

Each Flex IOC has a processor subsystem, which includes a 1.2-GHz CPU, a system controller, 1 GB SDRAM, and two Packet Forwarding Engines with a maximum throughput of 10 Gbps each.

You must install at least one IOC in the firewall. The IOC can be of any of the available IOC or Flex IOC types.

You can install Flex IOCs in any of the slots that are not reserved for Switch Control Boards (SCBs). If a slot is not occupied by a card, you must install a blank panel to shield the empty slot and to allow cooling air to circulate properly through the firewall.

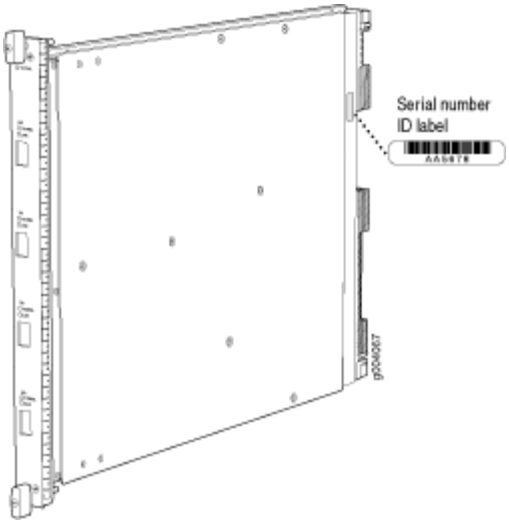
Figure 84: Flex IOC with Typical Port Modules



Description	• Flex IOC with slots for two port modules • Maximum throughput: 10 Gbps (per PFE)
Software release	• Junos OS Release 9.5R1 and later
Cables and connectors	Slots for two port modules
Controls	None
Supported Slots	• SRX5600–Any slot except bottom slots **0** or **1** • SRX5800–Any slot except center slots **0**, **1**, or **2/6**
Power Requirement	312 W typical, 365 W maximum (includes port modules)

Weight	Approximately 10 lb (4.5 kg)
LEDs	**OK/FAIL** LED, one bicolor: • Steady green–The Flex IOC is operating normally. • Red–The Flex IOC has failed and is not operating normally. • Off–The Flex IOC is powered down.
Serial Number Location	The serial number label is located as shown in Figure 85 on page 175.

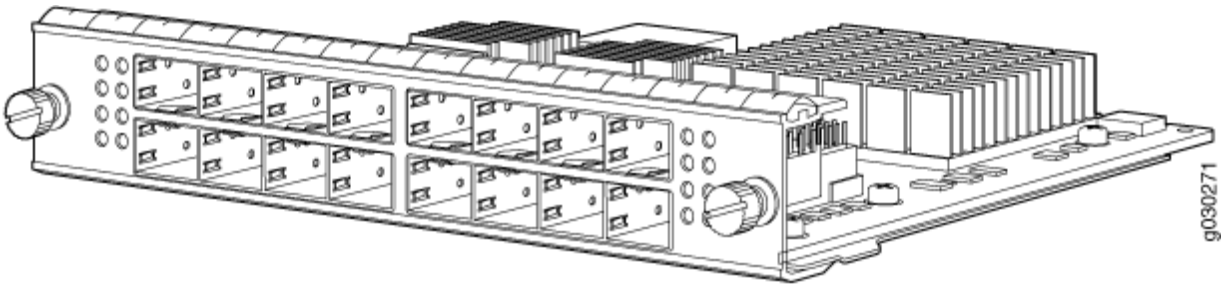
Figure 85: Serial Number Label (IOC Shown, Other Cards Similar)



Flex I/O Card Port Module SRX-IOC-16GE-SFP Specifications

You use port modules and Flex I/O Cards (Flex IOCs) to add different combinations of small form-factor pluggable transceiver (SFP), 10-gigabit SFP transceiver (XFP), and copper ports to your firewall to suit the specific needs of your network. The SRX-IOC-16GE-SFP port module (Figure 86 on page 176) installs into a Flex IOC to add sixteen 10/100/1000 Ethernet SFP ports.

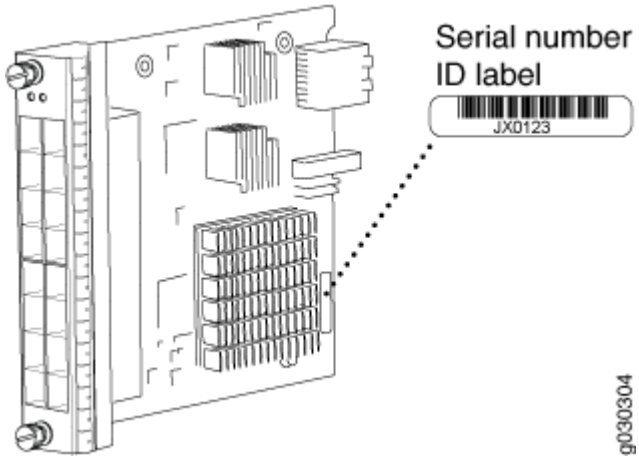
Figure 86: Flex IOC Port Module SRX-IOC-16GE-SFP



Description	• Port module with 16 Gigabit Ethernet SFP ports • Maximum throughput: 10 Gbps • Oversubscription ratio: 1.6:1 • Maximum configurable MTU: 9192 bytes
Software release	• Junos OS Release 9.5R1 and later
Cables and connectors	16 Gigabit Ethernet SFP ports Supported SFP transceivers: 1000BASE-LH (model numbers SRX-SFP-1GE-LH, SRX-SFP-1GE-LH-ET) 1000BASE-LX (model numbers SRX-SFP-1GE-LX, SRX-SFP-1GE-LX-ET) 1000BASE-SX (model numbers SRX-SFP-1GE-SX, SRX-SFP-1GE-SX-ET) 1000BASE-T (model numbers SRX-SFP-1GE-T, SRX-SFP-1GE-T-ET)
Controls	**ONLINE** Button–The **ONLINE** button on the port module front panel toggles the port module online and offline
Supported Slots	Either slot in SRX5K-FPC-IOC Flex IOC
Weight	Approximately 1.6 lb (0.7 kg)

LEDs	**OK/FAIL** LED, one bicolor: • Steady green–The port module is operating normally. • Red–The port module has failed and is not operating normally. • Off–The port module is powered down. **LINK** LED, single color, one per port: • Steady green–The link is active. • Off–No link. **TX/RX** LED, single color, one per port: • Blinking Green–The port is receiving or transmitting data. • Off–No activity.
Serial Number Location	The serial number label is located as shown in Figure 87 on page 177.

Figure 87: Port Module SRX-IOC-16GE-SFP Serial Number Label

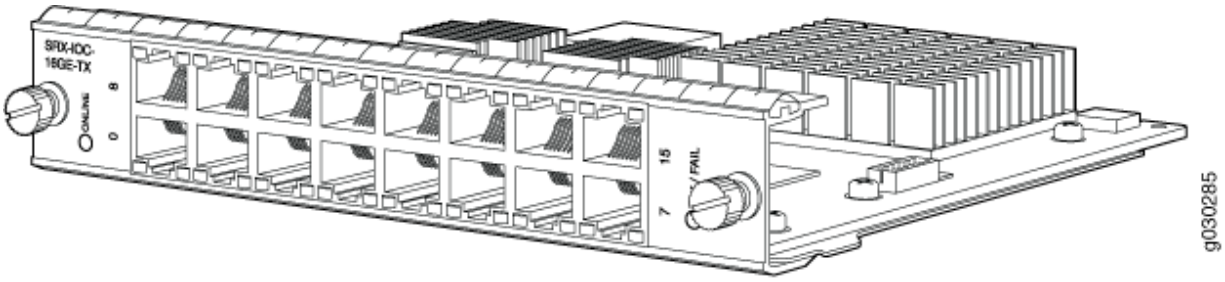


Flex I/O Card Port Module SRX-IOC-16GE-TX Specifications

You use port modules and Flex I/O Cards (Flex IOCs) to add different combinations of small form-factor pluggable transceiver (SFP), 10-gigabit SFP transceiver (XFP), and copper ports to your firewall to suit

the specific needs of your network. The SRX-IOC-16GE-TX port module (Figure 88 on page 178) installs into a Flex IOC to add sixteen 10/100/1000 Ethernet RJ-45 copper ports.

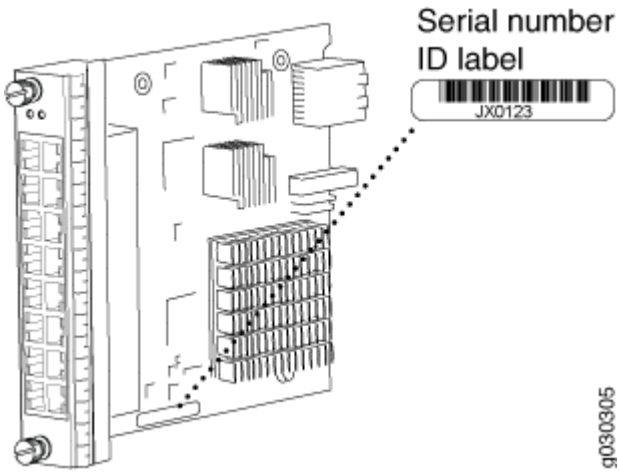
Figure 88: Flex IOC Port Module SRX-IOC-16GE-TX



Description	• Port module with sixteen 10/100/1000 Ethernet RJ45 ports • Maximum throughput: 10 Gbps • Oversubscription ratio: 1.6:1 • Maximum configurable MTU: 9192 bytes
Software release	• Junos OS Release 9.5R1 and later
Cables and connectors	Sixteen RJ-45 1-Gbps ports
Controls	**ONLINE** Button–The **ONLINE** button on the port module front panel toggles the port module online and offline.
Supported Slots	Either slot in SRX5K-FPC-IOC Flex IOC
Weight	Approximately 1.6 lb (0.7 kg)

LEDs	**OK/FAIL** LED, one bicolor: • Steady green–The port module is operating normally. • Red–The port module has failed and is not operating normally. • Off–The port module is powered down. **LINK** LED, single color, one per port: • Steady green–The link is active. • Off–No link. **TX/RX** LED, single color, one per port: • Blinking green–The port is receiving or transmitting data. • Off–No activity.
Serial Number Location	The serial number label is located as shown in Figure 89 on page 179.

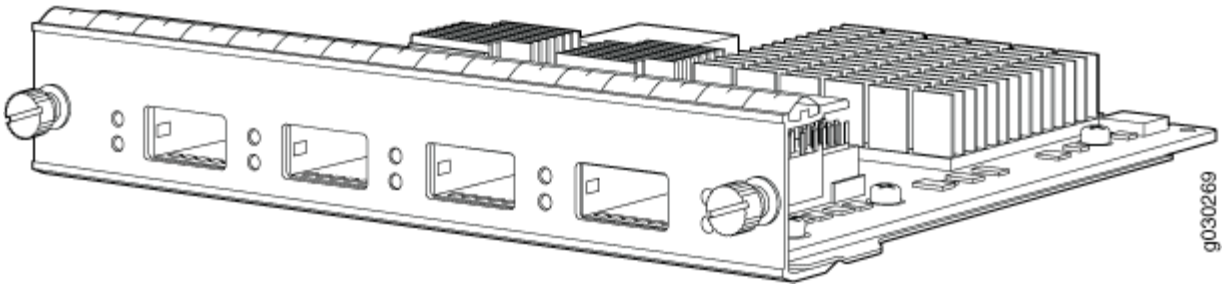
Figure 89: Port Module SRX-IOC-16GE-TX Serial Number Label



Flex I/O Card Port Module SRX-IOC-4XGE-XFP Specifications

You use port modules and Flex I/O Cards (Flex IOCs) to add different combinations of small form-factor pluggable transceiver (SFP), 10-gigabit SFP transceiver (XFP), and copper ports to your firewall to suit the specific needs of your network. The SRX-IOC-4XGE-XFP port module (Figure 90 on page 180) installs into a Flex IOC to add four 10-Gigabit Ethernet XFP ports.

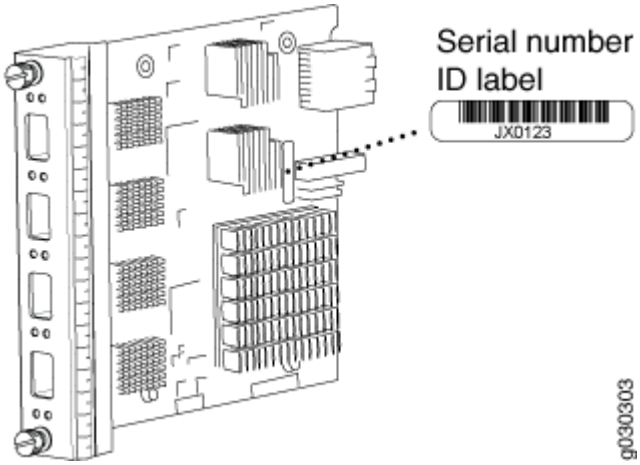
Figure 90: Flex IOC Port Module SRX-IOC-4XGE-XFP



Description	• Port module with four 10-Gigabit Ethernet XFP ports • Maximum throughput: 10 Gbps • Oversubscription ratio: 4:1 • Maximum configurable MTU: 9192 bytes
Software release	• Junos OS Release 9.5R1 and later
Cables and connectors	4 XFP Ethernet ports Supported XFP transceivers: 10GBASE-ER (model numbers SRX-XFP-10GE-ER and SRX-XFP-10GE-ER-ET) 10GBASE-LR (model numbers SRX-XFP-10GE-LR and SRX-XFP-10GE-LR-ET 10GBASE-SR (model numbers SRX-XFP-10GE-SR and SRX-XFP-10GE-SR-ET)
Controls	**ONLINE** Button–The **ONLINE** button on the port module front panel toggles the port module online and offline

Supported Slots	Either slot in SRX5K-FPC-IOC Flex IOC
Weight	Approximately 1.6 lb (0.7 kg)
LEDs	**OK/FAIL** LED, one bicolor: • Steady green–The port module is operating normally. • Red–The port module has failed and is not operating normally. • Off–The port module is powered down. **LINK** LED, single color, one per port: • Steady green–The link is active. • Off–No link.
Serial Number Location	The serial number label is located as shown in Figure 91 on page 181.

Figure 91: Port Module SRX-IOC-4XGE-XFP Serial Number Label



2

CHAPTER

Site Planning, Preparation, and Specifications

Site Preparation Checklist for the SRX5800 Firewall

The checklist in Table 40 on page 183 summarizes the tasks you need to perform when preparing a site for firewall installation.

Table 40: Site Preparation Checklist

Item or Task	For More Information ...	Performed By	Date
Verify that environmental factors such as temperature and humidity do not exceed firewall tolerances.	"SRX5800 Firewall Environmental Specifications " on page 184		
Plan rack or cabinet location, including required space clearances.	"Clearance Requirements for SRX5800 Firewall Airflow and Hardware Maintenance" on page 187		
Select the type of rack or cabinet.	"SRX5800 Firewall Cabinet Size and Clearance Requirements" on page 190, "SRX5800 Firewall Rack Size and Strength Requirements" on page 189		
If a rack is used, secure rack to floor and building structure.	"Connection to Building Structure for the SRX5800 Firewall Rack" on page 190		
Acquire cables and connectors.			
Locate sites for connection of system grounding.	DC Power Electrical Safety Guidelines and Warnings		
Measure distance between external power sources and firewall installation site.			

Table 40: Site Preparation Checklist *(Continued)*

Item or Task	For More Information ...	Performed By	Date
Calculate the optical power budget and optical power margin.	"Calculating Power Budget for Fiber-Optic Cable for the SRX5800 Firewall" on page 209,"Calculating Power Margin for Fiber-Optic Cable for the SRX5800 Firewall" on page 209		

SRX5800 Site Guidelines and Requirements

IN THIS SECTION

SRX5800 Firewall Environmental Specifications

Table 41 on page 184 specifies the environmental specifications required for normal firewall operation. In addition, the site should be as dust-free as possible.

Table 41: Firewall Environmental Specifications

Description	Value
Altitude	No performance degradation to 10,000 ft (3048 m)
Relative humidity	Normal operation ensured in relative humidity range of 5% to 90%, noncondensing

Table 41: Firewall Environmental Specifications *(Continued)*

Description	Value
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (40°C) Nonoperating storage temperature in shipping crate: –40°F (–40°C) to 158°F (70°C)
Seismic	Tested to meet Telcordia Technologies Zone 4 earthquake requirements
Maximum thermal output	Standard-Capacity AC and DC power supplies • AC power: 20,160, BTU/hour (5912 W) • DC power: 17,057 BTU/hour (5002 W) **NOTE**: These specifications are estimates and subject to change.
	High-Capacity AC and DC power supplies • AC power: 32,780 BTU/hour (9608 W) • DC power: 33,482 BTU/hour (9813 W) **NOTE**: These specifications are estimates and subject to change.

NOTE: Install the firewall only in restricted areas, such as dedicated equipment rooms and equipment closets, in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.

General Site Guidelines

Efficient device operation requires proper site planning and maintenance. It also requires proper layout of the equipment, rack or cabinet, and wiring closet.

To plan and create an acceptable operating environment for your device and prevent environmentally caused equipment failures:

- Keep the area around the chassis free from dust and conductive material, such as metal flakes.

- Follow the prescribed airflow guidelines to ensure that the cooling system functions properly. Ensure that the exhaust from other equipment does not blow into the intake vents of the device.
- Follow the prescribed electrostatic discharge (ESD) prevention procedures to prevent damaging the equipment. Static discharge can cause components to fail completely or intermittently over time.
- Install the device in a secure area, so that only authorized personnel can access the device.

Site Electrical Wiring Guidelines

Table 42 on page 186 describes the factors you must consider while planning the electrical wiring at your site.

WARNING: You must provide a properly grounded and shielded environment and use electrical surge-suppression devices.

Avertissement Vous devez établir un environnement protégé et convenablement mis à la terre et utiliser des dispositifs de parasurtension.

Table 42: Site Electrical Wiring Guidelines

Site Wiring Factor	Guidelines
Signaling limitations	If your site experiences any of the following problems, consult experts in electrical surge suppression and shielding: • Radio frequency interference (RFI) because of improperly installed wires • Damage from lightning strikes occuring when wires exceed recommended distances or pass between buildings • Electromagnetic pulses (EMPs) caused by lightning damaging unshielded conductors and electronic devices
Radio frequency interference	To reduce or eliminate RFI from your site wiring, do the following: • Use a twisted-pair cable with a good distribution of grounding conductors. • To exceed the recommended distances, use a high-quality twisted-pair cable with one ground conductor for each data signal, when applicable.

Table 42: Site Electrical Wiring Guidelines *(Continued)*

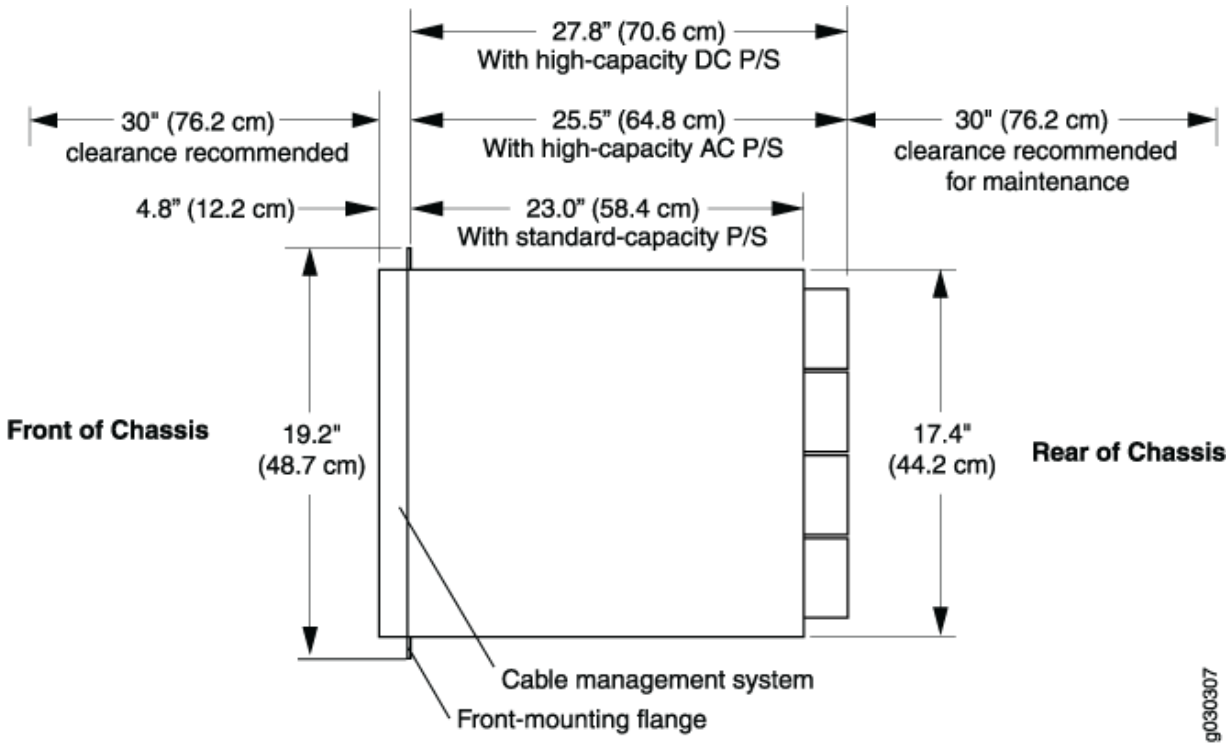
Site Wiring Factor	Guidelines
Electromagnetic compatibility	If your site is susceptible to problems with electromagnetic compatibility (EMC), particularly from lightning or radio transmitters, seek expert advice. Strong sources of electromagnetic interference (EMI) can cause: • Destruction of the signal drivers and receivers in the device. • Electrical hazards as a result of power surges conducted over the lines into the equipment.

Clearance Requirements for SRX5800 Firewall Airflow and Hardware Maintenance

When planning the installation site, you need to allow sufficient clearance around the rack (see Figure 92 on page 188):

- For the cooling system to function properly, the airflow around the chassis must be unrestricted.
- A minimum of 3 in. (7.62 cm) clearance must be provided behind the power supplies for airflow.
- For service personnel to remove and install hardware components, there must be adequate space at the front and back of the firewall. At least 24 in. (61 cm) is required both in front of and behind the firewall. NEBS GR-63 recommends that you allow at least 30 in. (76.2 cm) behind the firewall.
- Airflow must always be from front to back with respect to the rack. If the device has side to rear airflow, then provisions must be made to ensure that fresh air from the front of the rack is supplied to the inlets, and exhaust exits the rear of the rack. The device must not interfere with the cooling of other systems in the rack. Fillers must be used as appropriate in the rack to ensure there is no recirculation of heated exhaust air back to the front of the rack. Care must also be taken around cables to ensure that there is no leakage of air in situations where recirculation might result.

Figure 92: Chassis Dimensions and Clearance Requirements for the Firewall



RELATED DOCUMENTATION

- SRX5800 Firewall Agency Approvals | **522**
- SRX5800 Firewall General Safety Guidelines and Warnings
- SRX5800 Firewall Fire Safety Requirements and Fire Suppression Equipment
- SRX5800 Firewall Definition of Safety Warning Levels
- General Electrical Safety Guidelines and Warnings

SRX5800 Rack and Cabinet Requirements

IN THIS SECTION

SRX5800 Firewall Rack-Mounting Hardware

The rack-mounting hardware for the SRX5800 Firewall includes:

- The large mounting shelf for mounting in four-post racks, cabinets, and open-frame racks
- The small mounting shelf for front-mounting in a four-post rack or cabinet
- Front-mounting flanges on the front of the chassis for front-mounting in a four-post rack or cabinet
- Two center-mounting brackets attached to the center of the chassis for center-mounting in an open-frame rack. For an open-frame rack, center-mounting is preferable because of the more even distribution of weight.

SRX5800 Firewall Rack Size and Strength Requirements

The size, strength, and location of the rack must accommodate the firewall's weight and external dimensions. The location of the rack must allow for the clearance requirements specified in "Clearance Requirements for SRX5800 Firewall Airflow and Hardware Maintenance" on page 187.

The chassis is 17.37 in. (44.11 cm) wide. The firewall is designed for installation in a standard 19-in. rack, as defined in *Cabinets, Racks, Panels, and Associated Equipment* (document number EIA-310-D) published by the Electronics Industry Association (http://www.eia.org). The spacing of the holes between the left and right front-mounting flanges and center-mounting brackets is 18.31 in (465 mm) apart. However, the inside spacing between the rack rails must allow sufficient space for the width of the chassis.

With the use of adapters or approved wing devices to narrow the opening between the rails, the firewall can fit into a 600-mm-wide rack, as defined in the four-part *Equipment Engineering (EE); European telecommunications standard for equipment practice* (document numbers ETS 300 119-1 through 119-4) published by the European Telecommunications Standards Institute (http://www.etsi.org).

Observe these guidelines:

- The rack must have sufficient vertical usable space to accommodate the height of the firewall: 27.75 in. (70.49 cm) high (approximately 16 U). You can stack three firewalls in a rack that is at least 48 U (89.3 in. or 2.24 m) in height.

  NOTE: A *U* is the standard rack unit defined in *Cabinets, Racks, Panels, and Associated Equipment*.

- The location of the rack must provide sufficient space to accommodate the depth of the firewall. The chassis depth from the front mounting flange to the rear of the power supply ranges from 23.0 in. (58.4 cm) to 27.8 in. (70.6 cm) depending on the type of power supply installed.

- The rack must be strong enough to support the weight of the fully configured firewall, up to 400 lb (182 kg). If you stack three fully configured firewalls, it must be capable of supporting up to 1,200 lb (545 kg).

Spacing of Rack-Mounting Bracket Holes for the SRX5800 Firewall

The firewall can be mounted in any rack that provides holes or hole patterns spaced at 1 U (1.75 in.) increments. The mounting brackets used to attach the chassis to a rack are designed (as per EIA-310-D specifications) to fasten to holes spaced at those distances.

Connection to Building Structure for the SRX5800 Firewall Rack

Always secure the rack to the structure of the building. If your geographical area is subject to earthquakes, bolt the rack to the floor. For maximum stability, also secure the rack to ceiling brackets.

SRX5800 Firewall Cabinet Size and Clearance Requirements

The minimum size cabinet that can accommodate the device depends on the type of power supplies installed:

- If only standard-capacity power supplies are installed, the firewall will fit inside a standard 600 mm wide by 800 mm deep cabinet.

- If high-capacity AC or DC power supplies are installed, the firewall must be installed in a cabinet that is at least 600 mm wide by 1000 mm deep.

See "Clearance Requirements for SRX5800 Firewall Airflow and Hardware Maintenance" on page 187 for chassis width and depth dimensions. A cabinet larger than the minimum requirement provides better airflow and reduces the chance of overheating. To accommodate a single device, the cabinet must be at least 16 U high. If you provide adequate cooling air and airflow clearance, you can stack three devices in a cabinet that has at least 48 U (84 in. or 2.13 m) of usable vertical space.

SRX5800 Firewall Cabinet Airflow Requirements

When you mount the firewall in a cabinet, you must ensure that ventilation through the cabinet is sufficient to prevent overheating. Following is a list of requirements to consider when planning for chassis cooling:

- Ensure that the cool air supply you provide through the cabinet can adequately dissipate the thermal output of the device.
- Ensure that the cabinet allows the chassis hot exhaust air to exit from the cabinet without recirculating into the device. An open cabinet (without a top or doors) that employs hot air exhaust extraction from the top allows the best airflow through the chassis. If the cabinet contains a top or doors, perforations in these elements assist with removing the hot air exhaust.
- Install the device as close as possible to the front of the cabinet so that the cable management system just clears the inside of the front door. This maximizes the clearance in the rear of the cabinet for critical airflow.
- Route and dress all cables to minimize the blockage of airflow to and from the chassis.

Calculating Power Requirements for the SRX5800 Firewall

The information in this topic helps you determine which power supplies are suitable for various configurations, as well as which power supplies are not suitable because output power is exceeded. You determine suitability by subtracting the total power draw from the maximum output of the power supplies. Afterward, the required input current is calculated. Finally, you calculate the thermal output.

We recommend that you provision power according to the maximum input current listed in the power supply electrical specifications (see "SRX5800 Firewall AC Power Supply Specifications" on page 39 and "SRX5800 Firewall DC Power Supply Specifications" on page 62).

Use the following procedures to calculate the power requirement:

1. Calculate the power requirement.
2. Evaluate the power budget.
3. Calculate input power.
4. Calculate thermal output (BTUs) for cooling requirements.

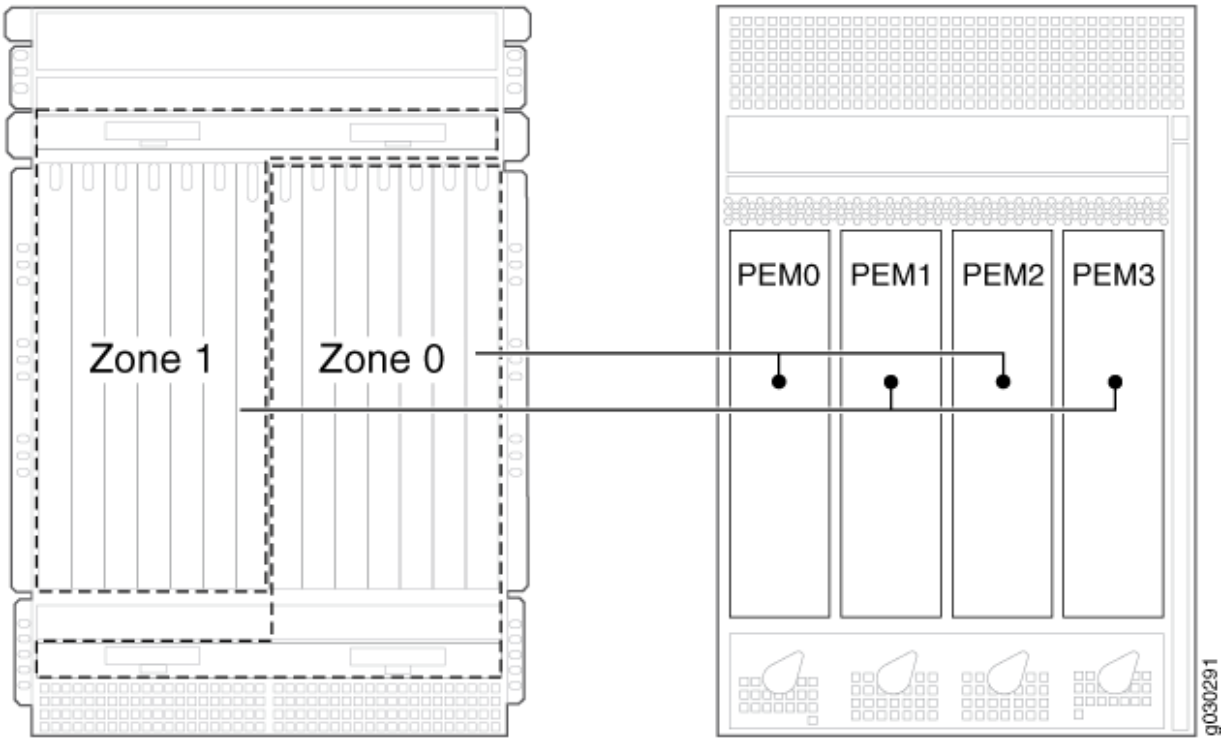
The SRX5800 Firewall chassis with normal-capacity AC power supplies has one overall zone. The SRX5800 Firewall Chassis with high-capacity AC power supplies or either standard- or high-capacity DC power supplies is zoned. Zoning means that certain components are powered by specific power supplies (see Table 43 on page 192 and Figure 93 on page 193 for information on zoning). When calculating power requirements, be sure that there is adequate power for each zone.

Three AC power supplies are mandatory for a SRX5800 Firewall chassis with normal-capacity AC power supplies.

Table 43: SRX5800 Firewall Zoning

Zone	Power Supply (PEM)	Components Receiving Power
Zone 0	PEM 0 or 2	• Bottom fan tray • IOC/SPC slots 6 through 11 • SCB slots 1 through 2
Zone 1	PEM 1 or 3	• Upper fan tray • IOC/SPC slots 0 through 5 • SCB slot 0

Figure 93: Power Distribution from DC and High-Capacity AC Power Supplies in the SRX5800 Firewall Chassis



Sample configuration for SRX5800 Firewall chassis with SRX5K-SCB (SCB1) and SRX5K-RE-13-20 (RE1) or with SRX5K-SCBE (SCB2) and SRX5K-RE-1800X4 (RE2):

- Four high-capacity AC power supplies (using two feeds for each power supply); two supplies are active, two are redundant.
- Two Switch Control Boards (SCBs) with Routing Engines.
- Two SRX5K-MPC (IOC2) Modular Port Concentrator, with two Modular Interface Cards (MICs).
- SRX5K-SPC-4-15-320 (SPC2) Services Processing Cards

> **NOTE**: You must have high-capacity power system (either AC or DC power supplies) and high-capacity cooling system (upper and bottom fan trays) installed in the firewall in order to install and use SPC2. If you do not have high-capacity power supplies and fan trays installed, the firewall will log an alarm condition when it recognizes the SPC.

- High-capacity cooling system (upper and bottom fan trays).

1. Calculate the power requirements (usage) as shown in Table 44 on page 194.

Table 44: Sample Power Requirements for an SRX5800 Firewall with SRX5K-SCB (SCB1) and SRX5K-RE-13-20 (RE1) or with SRX5K-SCBE (SCB2) and SRX5K-RE-1800X4 (RE2)

Chassis Component	Part Number	Power Requirement	Zone 0 Power	Zone 1 Power
Base system	SRX5800BASE-HC-AC	50 W	25 W	25 W
High-capacity cooling system	SRX5800-HC-FAN	320 W * 2 = 640 W	320 W	320 W
SPC - slots 0 through 4	SPC2	585W * 5 = 2925 W		2925 W
MPC - slot 5	IOC2 with two MICs	570 W		570 W
SCB 0 - slot 0	SCB1 with RE1 or SCB2 with RE2	150 W 90 W		240 W
SCB 1- slot 1	SCB1 with RE1 or SCB2 with RE2	150 W 90 W	240 W	
SCB 2/MPC - slot 2/6	IOC2 with two MICs	570 W	570 W	
SPC - slots 7 through 11	SPC2	585W * 5 = 2925 W	2925 W	
Total power requirement		SRX5800 high-capacity AC (not zoned) 8070 W	Zone 0 total: 4080 W	Zone 1 total: 4080 W

For the power consumption specifications of specific SRX5800 Firewall cards, see the *SRX5400, SRX5600, and SRX5800 Firewall Card Guide* at www.juniper.net/documentation/.

2. Evaluate the power budget, including the budget for each zone, if applicable. In this step, we check the required power against the maximum output power of available power supply options.

   Table 45 on page 195 lists the power supplies, their maximum output power, and unused power (or a power deficit).

   Table 45: Calculating Power Budget for SRX5800 Firewall with SRX5K-SCB (SCB1) and SRX5K-RE-13-20 (RE1) or with SRX5K-SCBE (SCB2) and SRX5K-RE-1800X4 (RE2)

Power Supply	Maximum Output Power of Power Supply	Maximum Output Power for System	Zone 0 Unused Power[1]	Zone 1 Unused Power[2]
SRX5800 AC high-capacity	4100 W (two feeds)	8200 W (two feeds)	4100-4080=20 W	4100-4080=20 W
SRX5800 DC high-capacity	4100 W (two feeds)	8200 W (two feeds)	4100-4080=20 W	4100-4080=20 W

   [1] For this configuration, output power is 4080 W.

   [2] For this configuration, output power is 4080 W.

3. Calculate input power. In this step, the input power requirements for the example configuration are calculated. To do this, divide the total output requirement by the efficiency of the power supply as shown in Table 46 on page 195 .

   Table 46: Calculating Input Power for SRX5800 Firewall with SRX5K-SCB (SCB1) and SRX5K-RE-13-20 (RE1) or with SRX5K-SCBE (SCB2) and SRX5K-RE-1800X4 (RE2)

Power Supply	Power Supply Efficiency[1]	Input Power Requirement
SRX5800 AC high-capacity	~88 %	Zone 0: 4080/0.88= 4636 W
		Zone 1: 4080/0.88= 4636 W
SRX5800 DC high-capacity	86 %	Zone 0: 4080/0.86= 4744 W

Table 46: Calculating Input Power for SRX5800 Firewall with SRX5K-SCB (SCB1) and SRX5K-RE-13-20 (RE1) or with SRX5K-SCBE (SCB2) and SRX5K-RE-1800X4 (RE2) *(Continued)*

Power Supply	Power Supply Efficiency[1]	Input Power Requirement
		Zone 1: 4080/0.86= 4744 W

[1] These values are at full load and nominal voltage.

4. Calculate thermal output (BTUs) for the system. To calculate this value, add the total input power requirement (in watts) for the two zones together and multiply the sum by 3.41 as shown in Table 47 on page 196.

Table 47: Calculating Thermal Output for SRX5800 Firewall with SRX5K-SCB (SCB1) and SRX5K-RE-13-20 (RE1) or with SRX5K-SCBE (SCB2) and SRX5K-RE-1800X4 (RE2)

Power Supply	Thermal Output (BTUs per hour)
SRX5800 AC high-capacity	(4636 + 4636) * 3.41 = 31,617 BTU/hr
SRX5800 DC high-capacity	(4744 + 4744) * 3.41 = 32,354 BTU/hr

Sample configuration for SRX5800 Firewall chassis with SRX5K-SCB3 (SCB3) and SRX5K-RE-1800X4 (RE2):

- Four high-capacity AC power supplies (using two feeds for each power supply); two supplies are active, two are redundant.
- Two Switch Control Boards (SCBs) with Routing Engines.
- Two IOC3s (SRX5K-MPC3-40G10G and SRX5K-MPC3-100G10G) Modular Port Concentrator.
- SPC2 Services Processing Card

> **NOTE**: You must have high-capacity power supplies (either AC or DC) and high-capacity fan trays installed in the firewall in order to install and use SPC2. If you do not have high-capacity power supplies and fan trays installed, the firewall will log an alarm condition when it recognizes the SPC.

- High-capacity cooling system (upper and bottom fan trays).

1. Calculate the power requirements (usage) as shown in Table 48 on page 197.

Table 48: Sample Power Requirements for an SRX5800 Firewall SCB3, IOC3, and RE2

Chassis Component	Part Number	Power Requirement	Zone 0 Power	Zone 1 Power
Base system	SRX5800BASE-HC-AC	50 W	25 W	25 W
High-capacity cooling system	SRX5800-HC-FAN	320 W * 2 = 640 W	320 W	320 W
SPC - slots 0 through 3	SPC2	585 W * 4= 2340 W		2340 W
slot 4	Empty			
MPC - slot 5	SRX5K-MPC3-100G10G	607 W		607 W
SCB 0 - slot 0	SCB3 with RE2	185 W 90 W		275 W
SCB 1 - slot 1	SCB3 with RE2	185 W 90 W	275 W	
SCB 2/MPC - slot 2/6	SRX5K-MPC3-40G10G	607 W	607 W	
SPC - slots 7 through 10	SPC2	585 W * 4 = 2340 W	2340 W	
slot 11	Empty			
Total power requirement		SRX5800 high-capacity AC (not zoned) 7249 W	Zone 0 total: 3567 W	Zone 1 total: 3567 W

For the power consumption specifications of specific SRX5800 Firewall cards, see the *SRX5400, SRX5600, and SRX5800 Firewall Card Guide* at www.juniper.net/documentation/.

2. Evaluate the power budget, including the budget for each zone, if applicable. In this step, we check the required power against the maximum output power of available power supply options.

   Table 49 on page 198 lists the power supplies, their maximum output power, and unused power (or a power deficit).

Table 49: Calculating Power Budget for SRX5800 Firewall with SCB3, IOC3,and RE2

Power Supply	Maximum Output Power of Power Supply	Maximum Output Power for System	Zone 0 Unused Power[1]	Zone 1 Unused Power[2]
SRX5800 AC high-capacity	4100 W (two feeds)	8200 W (two feeds)	4100-3567=533 W	4100-3567=533 W
SRX5800 DC high-capacity	4100 W (two feeds)	8200 W (two feeds)	4100-3567=533 W	4100-3567=533 W

[1] For this configuration, output power is 3567 W.

[2] For this configuration, output power is 3567 W.

3. Calculate input power. In this step, the input power requirements for the example configuration are calculated. To do this, divide the total output requirement by the efficiency of the power supply as shown in Table 50 on page 198.

> **NOTE**: Normal-capacity AC and DC power supplies are not included in the following table, because their power budget was exceeded in the sample configuration.

Table 50: Calculating Input Power for SRX5800 Firewall with SCB3, IOC3, and RE2

Power Supply	Power Supply Efficiency[1]	Input Power Requirement
SRX5800 AC high-capacity	~88 %	Zone 0: 3567/0.88= 4053 W
		Zone 1: 3567/0.88= 4053 W

Table 50: Calculating Input Power for SRX5800 Firewall with SCB3, IOC3, and RE2 *(Continued)*

Power Supply	Power Supply Efficiency[1]	Input Power Requirement
SRX5800 DC high-capacity	86 %	Zone 0: 3567/0.86= 4147 W
		Zone 1: 3567/0.86= 4147 W

[1] These values are at full load and nominal voltage.

4. Calculate thermal output (BTUs) for the system. To calculate this value, add the total input power requirement (in watts) for the two zones together and multiply the sum by 3.41 as shown in Table 51 on page 199 .

Table 51: Calculating Thermal Output for SRX5800 Firewall with SCB3, IOC3, and RE2

Power Supply	Thermal Output (BTUs per hour)
SRX5800 AC high-capacity	(4053 + 4053) * 3.41 = 27,641 BTU/hr
SRX5800 DC high-capacity	(4147 + 4147) * 3.41 = 28,282 BTU/hr

Sample configuration for SRX5800 Firewall chassis with six SRX5K-SPC-2-10-40 (SPC2), one SRX5K-SPC3 (SPC3), three SRX5K-IOC4-10G, and two SRX5K-SCB4s (SCB4) with two SRX5K-RE3-128Gs (RE3):

- Four high-capacity AC power supplies (using two feeds for each power supply); two supplies are active, two are redundant.
- Two SRX5K-SCB4s (SCB4) with two SRX5K-RE3-128Gs (RE3) installed in slot number **SCB 0** and **SCB 1** of the chassis.

  NOTE: The two SCB4s fabric mode must be changed from default fabric mode to redundant fabric mode.

- Three SRX5K-IOC4-10Gs (IOC4) Modular Port Concentrator
- Six SPC2s & one SPC3 Services Processing Cards

NOTE: You must have high-capacity power supplies (either AC or DC) and high-capacity fan trays installed in the firewall in order to install and use SPC2 and SPC3. If you do not have high-capacity power supplies and fan trays installed, the firewall will log an alarm condition when it recognizes the SPC.

- High-capacity cooling system (upper and bottom fan trays)

1. Calculate the power requirements (usage) as shown in Table 52 on page 200.

Table 52: Sample Power Requirements

Chassis Component	Part Number	Power Requirement	Zone 0 Power	Zone 1 Power
Base system	SRX5800BASE-HC-AC	50 W	25 W	25 W
High-capacity cooling system	SRX5800-HC-FAN	320 W * 2 = 640 W	320 W	320 W
SPC - slots 0	SPC3	650 W		650 W
SPC - slots 1 through 3	SPC2	585 W * 3= 1755 W		1755 W
slot 4	Empty			
MPC - slot 5	SRX5K-IOC4-10G	500 W		500 W
SCB 0 (For Zone 1)	SCB4 with RE3	425 W 110 W		535 W
SCB 1 (For Zone 0)	SCB4 with RE3	425 W 110 W	535 W	
MPC - SCB 2 / slot 6	SRX5K-IOC4-10G	500 W	500 W	

Table 52: Sample Power Requirements *(Continued)*

Chassis Component	Part Number	Power Requirement	Zone 0 Power	Zone 1 Power
MPC - slot 7	SRX5K-IOC4-10G	500 W	500 W	
SPC - slots 8 through 10	SPC2	585 W * 3= 1755 W	1755 W	
slot 11	Empty			
Total power requirement		SRX5800 (not zoned) 7420 W	Zone 0 total: 3635 W	Zone 1 total: 3785 W

2. Evaluate the power budget, including the budget for each zone, if applicable. In this step, we check the required power against the maximum power output of the available power supply options.

   Table 53 on page 201 lists the power supplies, their maximum power output, and unused power (or a power deficit).

   Table 53: Calculating Power Budget

Power Supply	Maximum Power Output of a Power Supply	Maximum Power Output of a System	Zone 0 Unused Power[1]	Zone 1 Unused Power[2]
SRX5800 AC high-capacity	4100 W (with two feeds)	8200 W (2+2 with two feeds)	4100-3635=465 W unused power	4100-3785=315 W unused power
SRX5800 DC high-capacity	4100 W (with two feeds)	8200 W (2+2 with two feeds)	4100-3635=465 W unused power	4100-3785=315 W unused power

   [1] For this configuration, power output is 3635 W.

   [2] For this configuration, power output is 3785 W.

3. Calculate input power. In this step, the input power requirements for the example configuration are calculated. To do this, divide the total power output requirement by the efficiency of the power supply as shown in Table 54 on page 202.

Table 54: Calculating Input Power

Power Supply	Power Supply Efficiency[1]	Input Power Requirement
SRX5800 AC high-capacity	~88 %	Zone 0: 3635/0.88= 4131 W
		Zone 1: 3785/0.88= 4301 W
SRX5800 DC high-capacity	86 %	Zone 0: 3635/0.86= 4227 W
		Zone 1: 3785/0.86= 4401 W

[1] These values are at full load and nominal voltage.

4. Calculate thermal output (BTUs) for the system. To calculate this value, add the total input power requirement (in watts) for the two zones together and multiply the sum by 3.41 as shown in Table 55 on page 202 .

Table 55: Calculating Thermal Output

Power Supply	Thermal Output (BTUs per hour)
SRX5800 AC high-capacity	(4131 + 4301) * 3.41 = 18,797 BTU/hr
SRX5800 DC high-capacity	(4227 + 4401) * 3.41 = 19,234 BTU/hr

Sample configuration for SRX5800 Firewall chassis with six SRX5K-SPC-2-10-40 (SPC2), one SRX5K-SPC3 (SPC3), three SRX5K-IOC4-MRAT, and two SRX5K-SCB4s (SCB4) with two SRX5K-RE3-128Gs (RE3):

- Four high-capacity AC power supplies (using two feeds for each power supply); two supplies are active, two are redundant.
- Two SRX5K-SCB4s (SCB4) with two SRX5K-RE3-128Gs (RE3) installed in slot number **SCB 0** and **SCB 1** of the chassis.

> **NOTE**: The two SCB4s fabric mode must be changed from default fabric mode to redundant fabric mode.

- Three SRX5K-IOC4-MRATs (IOC4) Modular Port Concentrator
- Six SPC2s & one SPC3 Services Processing Cards

> **NOTE**: You must have high-capacity power supplies (either AC or DC) and high-capacity fan trays installed in the firewall in order to install and use SPC2 and SPC3. If you do not have high-capacity power supplies and fan trays installed, the firewall will log an alarm condition when it recognizes the SPC.

- High-capacity cooling system (upper and bottom fan trays)

> **NOTE**: The high-capacity cooling system satisfies cooling requirements of SPC2 & SPC3 and must be used for proper cooling.

1. Calculate the power requirements (usage) as shown in Table 56 on page 203.

Table 56: Sample Power Requirements

Chassis Component	Part Number	Power Requirement	Zone 0 Power	Zone 1 Power
Base system	SRX5800BASE-HC-AC	50 W	25 W	25 W
High-capacity cooling system	SRX5800-HC-FAN	320 W * 2 = 640 W	320 W	320 W
SPC - slots 0	SPC3	650 W		650 W
SPC - slots 1 through 3	SPC2	585 W * 3= 1755 W		1755 W
slot 4	Empty			
MPC - slot 5	SRX5K-IOC4-MRAT	545 W		545 W

Table 56: Sample Power Requirements *(Continued)*

Chassis Component	Part Number	Power Requirement	Zone 0 Power	Zone 1 Power
SCB 0 (For Zone 1)	SCB4 with RE3	425 W 110 W		535 W
SCB 1 (For Zone 0)	SCB4 with RE3	425 W 110 W	535 W	
MPC - SCB 2 / slot 6	SRX5K-IOC4-MRAT	545 W	545 W	
MPC - slot 7	SRX5K-IOC4-MRAT	545 W	545 W	
SPC - slots 8 through 10	SPC2	585 W * 3= 1755 W	1755 W	
slot 11	Empty			
Total power requirement		SRX5800 (not zoned) 7555 W	Zone 0 total: 3725 W	Zone 1 total: 3830 W

2. Evaluate the power budget, including the budget for each zone, if applicable. In this step, we check the required power against the maximum power output of the available power supply options.

   Table 57 on page 205 lists the power supplies, their maximum power output, and unused power (or a power deficit).

Table 57: Calculating Power Budget

Power Supply	Maximum Power Output of a Power Supply	Maximum Power Output of a System	Zone 0 Unused Power[1]	Zone 1 Unused Power[2]
SRX5800 AC high-capacity	4100 W (with two feeds)	8200 W (2+2 with two feeds)	4100-3725=375 W unused power	4100-3830=270 W unused power
SRX5800 DC high-capacity	4100 W (with two feeds)	8200 W (2+2 with two feeds)	4100-3725=375 W unused power	4100-3830=270 W unused power

[1] For this configuration, power output is 3725 W.

[2] For this configuration, power output is 3830 W.

3. Calculate input power. In this step, the input power requirements for the example configuration are calculated. To do this, divide the total power output requirement by the efficiency of the power supply as shown in Table 58 on page 205.

Table 58: Calculating Input Power

Power Supply	Power Supply Efficiency[1]	Input Power Requirement
SRX5800 AC high-capacity	~88 %	Zone 0: 3725/0.88= 4233 W
		Zone 1: 3830/0.88= 4352 W
SRX5800 DC high-capacity	86 %	Zone 0: 3725/0.86= 4331 W
		Zone 1: 3830/0.86= 4453 W

[1] These values are at full load and nominal voltage.

4. Calculate thermal output (BTUs) for the system. To calculate this value, add the total input power requirement (in watts) for the two zones together and multiply the sum by 3.41 as shown in Table 59 on page 206 .

Table 59: Calculating Thermal Output

Power Supply	Thermal Output (BTUs per hour)
SRX5800 AC high-capacity	(4233 + 4352) * 3.41 = 19,073 BTU/hr
SRX5800 DC high-capacity	(4331 + 4453) * 3.41 = 19,516 BTU/hr

SRX5800 Network Cable and Transceiver Planning

IN THIS SECTION

Routing Engine Interface Cable and Wire Specifications for the SRX5800 Firewall

Table 60 on page 207 lists the specifications for the cables that connect to management ports and the wires that connect to the alarm relay contacts.

Table 60: Cable and Wire Specifications for Routing Engine Management and Alarm Interfaces

Port	Cable Specification	Maximum Length	Routing Engine Receptacle
Routing Engine console or auxiliary interface	RS-232 (EIA-232) serial cable	6 ft (1.83 m)	RJ-45 socket
Routing Engine Ethernet interface	Category 5 cable or equivalent suitable for 100Base-T operation	328 ft (100 m)	RJ-45 autosensing

NOTE: We no longer include the console cable as part of the device package. If the console cable and adapter are not included in your device package, or if you need a different type of adapter, you can order the following separately:

- RJ-45 to DB-9 adapter (JNP-CBL-RJ45-DB9)
- RJ-45 to USB-A adapter (JNP-CBL-RJ45-USBA)
- RJ-45 to USB-C adapter (JNP-CBL-RJ45-USBC)

If you want to use RJ-45 to USB-A or RJ-45 to USB-C adapter you must have X64 (64-Bit) Virtual COM port (VCP) driver installed on your PC. See https://ftdichip.com/drivers/vcp-drivers/ to download the driver.

Signal Loss in Multimode and Single-Mode Fiber-Optic Cable for the SRX5800 Firewall

Multimode fiber is large enough in diameter to allow rays of light to reflect internally (bounce off the walls of the fiber). Interfaces with multimode optics typically use LEDs as light sources. LEDs are not coherent sources, however. They spray varying wavelengths of light into the multimode fiber, which reflects the light at different angles. Light rays travel in jagged lines through a multimode fiber, causing signal dispersion. When light traveling in the fiber core radiates into the fiber cladding, higher-order mode loss (HOL) results. Together these factors limit the transmission distance of multimode fiber compared to single-mode fiber.

Single-mode fiber is so small in diameter that rays of light can reflect internally through one layer only. Interfaces with single-mode optics use lasers as light sources. Lasers generate a single wavelength of

light, which travels in a straight line through the single-mode fiber. Compared with multimode fiber, single-mode fiber has higher bandwidth and can carry signals for longer distances. It is consequently more expensive.

Attenuation and Dispersion in Fiber-Optic Cable for the SRX5800 Firewall

Correct functioning of an optical data link depends on modulated light reaching the receiver with enough power to be demodulated correctly. *Attenuation* is the reduction in power of the light signal as it is transmitted. Attenuation is caused by passive media components, such as cables, cable splices, and connectors. While attenuation is significantly lower for optical fiber than for other media, it still occurs in both multimode and single-mode transmission. An efficient optical data link must have enough light available to overcome attenuation.

Dispersion is the spreading of the signal in time. The following two types of dispersion can affect an optical data link:

- Chromatic dispersion—The spreading of the signal in time resulting from the different speeds of light rays.
- Modal dispersion—The spreading of the signal in time resulting from the different propagation modes in the fiber.

For multimode transmission, modal dispersion, rather than chromatic dispersion or attenuation, usually limits the maximum bit rate and link length. For single-mode transmission, modal dispersion is not a factor. However, at higher bit rates and over longer distances, chromatic dispersion rather than modal dispersion limits maximum link length.

An efficient optical data link must have enough light to exceed the minimum power that the receiver requires to operate within its specifications. In addition, the total dispersion must be less than the limits specified for the type of link in Telcordia Technologies document GR-253-CORE (Section 4.3) and International Telecommunications Union (ITU) document G.957.

When chromatic dispersion is at the maximum allowed, its effect can be considered as a power penalty in the power budget. The optical power budget must allow for the sum of component attenuation, power penalties (including those from dispersion), and a safety margin for unexpected losses.

Calculating Power Budget for Fiber-Optic Cable for the SRX5800 Firewall

To ensure that fiber-optic connections have sufficient power for correct operation, you need to calculate the link's power budget, which is the maximum amount of power it can transmit. When you calculate the power budget, you use a worst-case analysis to provide a margin of error, even though all the parts of an actual system do not operate at the worst-case levels. To calculate the worst-case estimate of power budget (*PB*), you assume minimum transmitter power (*PT*) and minimum receiver sensitivity (*PR*):

PB = PT – PR

The following hypothetical power budget equation uses values measured in decibels (dB) and decibels referred to one milliwatt (dBm):

PB = PT – PR

PB = –15 dBm – (–28 dBm)

PB = 13 dB

Calculating Power Margin for Fiber-Optic Cable for the SRX5800 Firewall

After calculating a link's power budget, you can calculate the power margin (*PM*), which represents the amount of power available after subtracting attenuation or link loss (*LL*) from the power budget (*PB*). A worst-case estimate of *PM* assumes maximum *LL*:

PM = PB – LL

A *PM* greater than zero indicates that the power budget is sufficient to operate the receiver.

Factors that can cause link loss include higher-order mode losses, modal and chromatic dispersion, connectors, splices, and fiber attenuation. Table 61 on page 209 lists an estimated amount of loss for the factors used in the following sample calculations. For information about the actual amount of signal loss caused by equipment and other factors, see your vendor documentation.

Table 61: Estimated Values for Factors That Cause Link Loss

Link-Loss Factor	Estimated Link-Loss Value
Higher-order mode losses	Single-mode—None Multimode—0.5 dB

Table 61: Estimated Values for Factors That Cause Link Loss *(Continued)*

Link-Loss Factor	Estimated Link-Loss Value
Modal and chromatic dispersion	Single-mode—None Multimode—None, if product of bandwidth and distance is less than 500 MHz–km
Connector	0.5 dB
Splice	0.5 dB
Fiber attenuation	Single-mode—0.5 dB/km Multimode—1 dB/km

The following example uses the estimated values in Table 61 on page 209 to calculate link loss (*LL*) for a 2 km-long multimode link with a power budget (*PB*) of 13 dB:

- Fiber attenuation for 2 km @ 1.0 dB/km= 2 dB
- Loss for five connectors @ 0.5 dB per connector = 5(0.5 dB) = 2.5 dB
- Loss for two splices @ 0.5 dB per splice =2(0.5 dB) = 1 dB
- Higher-order loss = 0.5 dB
- Clock recovery module = 1 dB

The power margin (*PM*) is calculated as follows:

PM = PB – LL

PM = 13 dB – 2 km (1.0 dB/km) – 5 (0.5 dB) – 2 (0.5 dB) – 0.5 dB [HOL] – 1 dB [CRM]

PM = 13 dB – 2 dB – 2.5 dB – 1 dB – 0.5 dB – 1 dB

PM = 6 dB

The following sample calculation for an 8 km-long single-mode link with a power budget (*PB*) of 13 dB uses the estimated values from Table 61 on page 209 to calculate link loss (*LL*) as the sum of fiber attenuation (8 km @ 0.5 dB/km, or 4 dB) and loss for seven connectors (0.5 dB per connector, or 3.5 dB). The power margin (*PM*) is calculated as follows:

$P_M = P_B - LL$

PM = 13 dB – 8 km (0.5 dB/km) – 7 (0.5 dB)

PM = 13 dB – 4 dB – 3.5 dB

PM = 5.5 dB

In both examples, the calculated power margin is greater than zero, indicating that the link has sufficient power for transmission and does not exceed the maximum receiver input power.

SRX5800 Alarm and Management Cable Specifications and Pinouts

IN THIS SECTION

Alarm Relay Contact Wire Specifications for the SRX5800 Firewall

Table 62 on page 211 lists the specifications for the wires that connect to the alarm relay contacts.

Table 62: Cable and Wire Specifications for Alarm Interfaces

Port	Cable Specification	Cable/Wire Supplied
Alarm relay contacts	Wire with gauge between 28-AWG and 14-AWG (0.08 and 2.08 mm^2)	No

Console Port Cable and Wire Specifications for the SRX5800 Firewall

Table 63 on page 212 lists the specifications for the cable that connects a **CONSOLE** port on the Routing Engine to a management console.

Table 63: Cable and Wire Specifications for Routing Engine Management and Alarm Interfaces

Port	Cable Specification	Maximum Length	Receptacle
Routing Engine console or auxiliary interface	RS-232 (EIA-232) serial cable	6 ft (1.83 m)	RJ-45/DB-9 plug

NOTE: We no longer include the console cable as part of the device package. If the console cable and adapter are not included in your device package, or if you need a different type of adapter, you can order the following separately:

- RJ-45 to DB-9 adapter (JNP-CBL-RJ45-DB9)
- RJ-45 to USB-A adapter (JNP-CBL-RJ45-USBA)
- RJ-45 to USB-C adapter (JNP-CBL-RJ45-USBC)

If you want to use RJ-45 to USB-A or RJ-45 to USB-C adapter you must have X64 (64-Bit) Virtual COM port (VCP) driver installed on your PC. See https://ftdichip.com/drivers/vcp-drivers/ to download the driver.

RJ-45 Connector Pinouts for the SRX5800 Firewall Routing Engine Ethernet Port

The port on the Routing Engine labeled **ETHERNET** is an autosensing 10/100-Mbps Ethernet RJ-45 receptacle that accepts an Ethernet cable for connecting the Routing Engine to a management LAN (or other device that supports out-of-band management). Table 64 on page 213 describes the RJ-45 connector pinout.

Table 64: RJ-45 Connector Pinout for the Routing Engine ETHERNET Port

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

RJ-45 Connector Pinouts for the SRX5800 Firewall Routing Engine Auxiliary and Console Ports

The ports on the Routing Engine labeled **AUX** and **CONSOLE** are asynchronous serial interfaces that accept an RJ-45 connector. The ports connect the Routing Engine to an auxiliary or console management device. Table 65 on page 213 describes the RJ-45 connector pinout.

Table 65: RJ-45 Connector Pinout for the AUX and CONSOLE Ports

Pin	Signal	Description
1	RTS	Request to Send

Table 65: RJ-45 Connector Pinout for the AUX and CONSOLE Ports *(Continued)*

Pin	Signal	Description
2	DTR	Data Terminal Ready
3	TXD	Transmit Data
4	Ground	Signal Ground
5	Ground	Signal Ground
6	RXD	Receive Data
7	DSR/DCD	Data Set Ready
8	CTS	Clear to Send

CHAPTER 3

Initial Installation and Configuration

Overview of Installing the SRX5800 Firewall

To install the SRX5800 Firewall:

1. Prepare your installation site as described in "Site Preparation Checklist for the SRX5800 Firewall" on page 183.
2. Review the safety guidelines explained in SRX5800 Firewall General Safety Guidelines and Warnings.
3. Unpack the firewall and verify the parts.
   a. "Unpacking the SRX5800 Firewall" on page 217
   b. "Verifying the SRX5800 Firewall Parts Received" on page 219
4. Install the mounting hardware.
   - "Installing the SRX5800 Firewall Mounting Hardware for a Four-Post Rack or Cabinet" on page 223
   - "Installing the SRX5800 Firewall Mounting Hardware in an Open-Frame Rack" on page 225
5. Remove components from the firewall chassis as described in "Removing Components from the SRX5800 Chassis Before Installing It in the Rack" on page 228.
6. Lift the firewall on to the rack as described in "Installing the SRX5800 Firewall Chassis in the Rack" on page 235.
7. Reinstall components into the firewall chassis as described in "Reinstalling Components in the SRX5800 Firewall Chassis After Installing It in the Rack" on page 237.
8. Connect cables to the network and external devices.
   - "Connecting the SRX5800 Firewall to a Management Console or an Auxiliary Device" on page 245
   - "Connecting the SRX5800 Firewall to a Network for Out-of-Band Management" on page 247
   - "Connecting the Alarm Relay Wires to the SRX5800 Firewall Craft Interface" on page 287
9. Connect the grounding cable as described in "Grounding the SRX5800 Firewall" on page 252.

   WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power.

10. Connect the AC power cord or DC power cables:
    - "Connecting Power to an AC-Powered SRX5800 Firewall" on page 254

- "Connecting Power to a DC-Powered SRX5800 Firewall " on page 268

11. Power on the firewall:
    - "Powering On an AC-Powered SRX5800 Firewall" on page 263
    - "Powering On a DC-Powered SRX5800 Firewall " on page 271
12. Perform the initial system configuration as described in "Initially Configuring the SRX5800 Firewall" on page 274.

Unpacking the SRX5800

IN THIS SECTION

Tools and Parts Required to Unpack the SRX5800 Firewall

To unpack the Firewall and prepare for installation, you need the following tools:

- Phillips (+) screwdriver, number 2
- 1/2-in. or 13-mm open-end or socket wrench to remove bracket bolts from the shipping pallet
- Blank panels to cover any slots not occupied by a component

Unpacking the SRX5800 Firewall

The firewall is shipped in a wooden crate. A wooden pallet forms the base of the crate. The firewall chassis is bolted to this pallet. A cardboard accessory box and a *Getting Started Guide* are also included in the shipping crate.

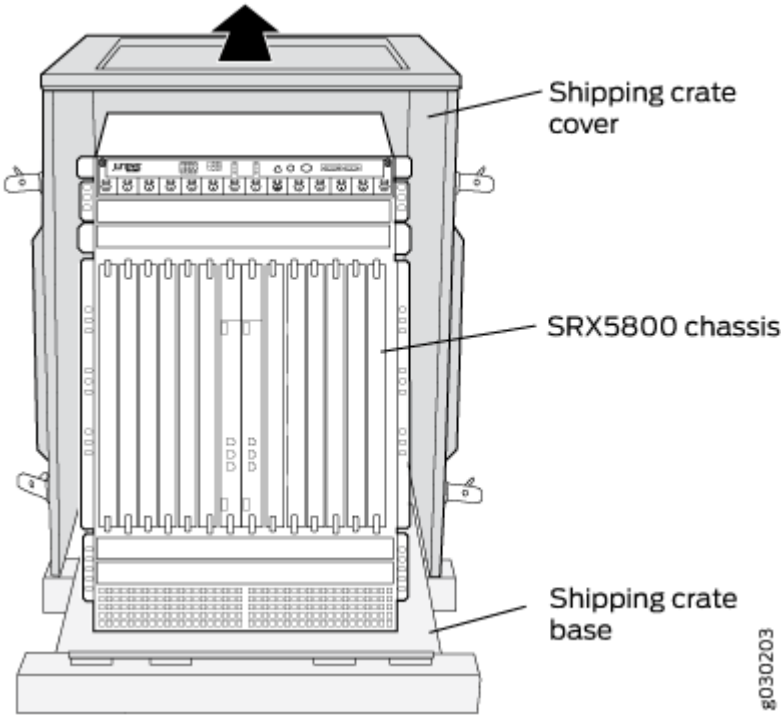
The shipping container measures 33 in. (83.8 cm) high, 30.25 in. (76.8 cm) wide, and 43.25 in. (109.9 cm) deep. The total weight of the container containing the firewall and accessories can range from 270 lb (122.5 kg) to 475 lb (215.5 kg).

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

To unpack the firewall, follow these steps (see Figure 94 on page 219):

1. Move the shipping crate to a staging area as close to the installation site as possible, where you have enough room to remove the components from the chassis. While the chassis is bolted to the pallet, you can use a forklift or pallet jack to move it.
2. Position the shipping crate with the arrows pointing up.
3. Open all the latches on the shipping crate.
4. Remove the front door of the shipping crate cover and set it aside.
5. Slide the remainder of the shipping crate cover off the pallet.
6. Remove the foam covering the top of the firewall.
7. Remove the accessory box and the *SRX5800 Firewall Getting Started Guide*.
8. Verify the parts received as described in "Verifying the SRX5800 Firewall Parts Received" on page 219.
9. Remove the vapor corrosion inhibitor (VCI) packs attached to the pallet, being careful not to break the VCI packs open.
10. To remove the brackets holding the chassis on the pallet, use a 1/2-in. socket wrench and a number 2 Phillips screwdriver to remove the bolts and screws from the brackets.
11. Store the brackets and bolts inside the accessory box.
12. Save the shipping crate cover, pallet, and packing materials in case you need to move or ship the firewall at a later time.

Figure 94: Contents of the Shipping Crate



Verifying the SRX5800 Firewall Parts Received

A packing list is included in each shipment. Check the parts in the shipment against the items on the packing list. The packing list specifies the part numbers and descriptions of each part in your order.

If any part is missing, contact a customer service representative.

A fully configured firewall contains the firewall chassis with installed components, listed in Table 66 on page 219, and an accessory box, which contains the parts listed in Table 67 on page 220. The parts shipped with your firewall can vary depending on the configuration you ordered.

Table 66: Parts List for a Fully Configured Firewall

Component	Quantity
Chassis, including midplane, craft interface, and rack-mounting brackets	1

Table 66: Parts List for a Fully Configured Firewall *(Continued)*

Component	Quantity
IOCs, Flex IOCs, and MPCs	Up to 11
SPCs	Up to 11
Routing Engines	1 or 2
SCBs	Up to 3
Power supplies	Up to 4
Fan trays	2
Air filter	1
Air filter tray	1
Getting Started Guide	1
Large mounting shelf	1
Small mounting shelf	1
Blank panels for slots without components installed	One blank panel for each slot not occupied by a component

Table 67: Accessory Box Parts List

Part	Quantity
Screws to mount chassis	14

Table 67: Accessory Box Parts List *(Continued)*

Part	Quantity
Screws to connect grounding cable (1/4-20 thread, 1/2 in. length)	2
Split washers for connecting grounding cable	2
DC power terminal Lugs, 6-AWG	8
Terminal block plug, 3 pole, 5.08 mm spacing, 12A, to connect the device alarms	2
720-029106 Assy, Cbl, Fiber Optic, Duplex, LC/LC, Multimode, 3 m, UL94V-0	2
740-011613 SFP, GbE, 850 nm, 550 m Reach, SX, DDM, -10°C to 85°C Temp	2
Label, accessories contents, SRX5800	1
USB flash drive with Junos OS	1
Read me first document	1
Affidavit for T1 connection	1
Juniper Networks Product Warranty	1
End User License Agreement	1
Document sleeve	1
3" x 5" pink bag	2
9" x 12" pink bag, ESD	2

Table 67: Accessory Box Parts List *(Continued)*

Part	Quantity
Accessory Box, 19 x 12 x 3"	1
ESD wrist strap with cable	1

NOTE: We no longer include the console cable as part of the device package. If the console cable and adapter are not included in your device package, or if you need a different type of adapter, you can order the following separately:

- RJ-45 to DB-9 adapter (JNP-CBL-RJ45-DB9)
- RJ-45 to USB-A adapter (JNP-CBL-RJ45-USBA)
- RJ-45 to USB-C adapter (JNP-CBL-RJ45-USBC)

If you want to use RJ-45 to USB-A or RJ-45 to USB-C adapter you must have X64 (64-Bit) Virtual COM port (VCP) driver installed on your PC. See https://ftdichip.com/drivers/vcp-drivers/ to download the driver.

Installing the SRX5800 Mounting Hardware

IN THIS SECTION

"Initially Configuring the SRX5800 Firewall" on page 274

Tools Required to Install the SRX5800 Firewall

To install the firewall, you need the following tools:

- Mechanical lift
- Phillips (+) screwdrivers, number 2
- Electrostatic discharge (ESD) grounding wrist strap

Installing the SRX5800 Firewall Mounting Hardware for a Four-Post Rack or Cabinet

If you are installing the firewall in a front-mount four-post rack or cabinet, you must first install the large mounting shelf, followed by the small mounting shelf.

Table 68 on page 223 specifies the holes in which you insert cage nuts and screws to install the mounting hardware required in a four-post or cabinet rack (an *X* indicates a mounting hole location). The hole distances are relative to one of the standard "U" divisions on the rack. The bottom of all mounting shelves is at 0.04 in. (0.02 U) above a "U" division.

Table 68: Four-Post Rack or Cabinet Mounting Hole Locations

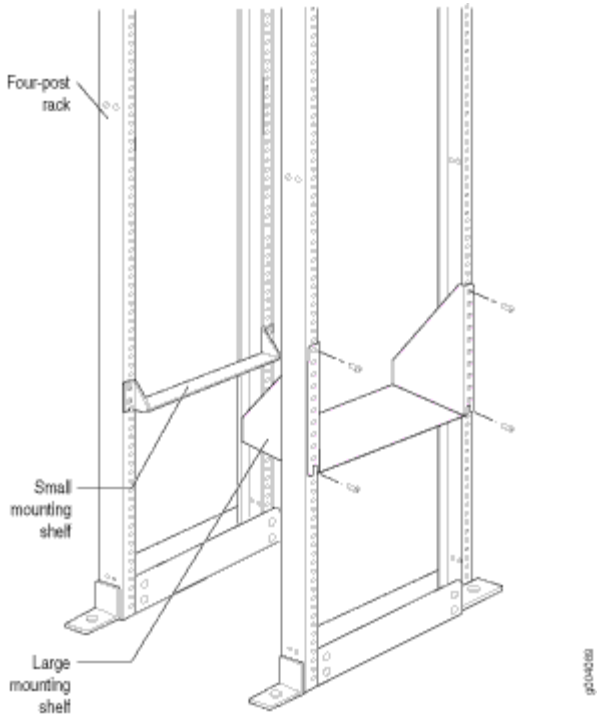
Hole	Distance Above "U" Division		Large Shelf	Small Shelf
3	1.51 in. (3.8 cm)	0.86 U		X
2	0.88 in. (2.2 cm)	0.50 U	X	X
1	0.25 in. (0.6 cm)	0.14 U		X

To install the mounting shelves (see Figure 95 on page 224):

1. On the front rack rails, install cage nuts in the holes specified in Table 68 on page 223 for the large shelf.

2. On the front of each front rack rail, partially insert a mounting screw into the hole containing the lowest cage nut.
3. Install the large shelf on the front rack rails. Rest the bottom slot of each ear on a mounting screw.
4. Partially insert a mounting screw into the top hole in each ear of the large shelf.
5. Tighten all the screws completely.
6. On the rear rack rails, install cage nuts in the holes specified in Table 68 on page 223 for the small shelf.
7. On the back of each rear rack rail, partially insert a mounting screw into the hole containing the lowest cage nut.
8. Install the small shelf on the back rack rails. Rest the bottom slot of each ear on a mounting screw. The small shelf installs on the back of the rear rails, extending toward the center of the rack. The bottom of the small shelf should align with the bottom of the large shelf.
9. Partially insert screws into the open holes in the ears of the small shelf.
10. Tighten all the screws completely.

Figure 95: Installing the Mounting Hardware for a Four-Post Rack or Cabinet



Installing the SRX5800 Firewall Mounting Hardware in an Open-Frame Rack

Before installing the firewall in an open-frame rack, install the large mounting shelf on the rack. The small mounting shelf is not needed.

If you are front-mounting the firewall, also remove the center-mounting brackets located on each side of the chassis.

Table 69 on page 225 specifies the holes in which you insert screws to install the mounting hardware in an open-frame rack (an *X* indicates a mounting hole location). The hole distances are relative to one of the standard "U" divisions on the rack. For reference, the bottom of all mounting shelves is at 0.04 in. (0.02 U) above a "U" division.

Table 69: Open-Frame Rack Mounting Hole Locations

Hole	Distance Above "U" Division		Large Shelf
30	17.26 in. (43.8 cm)	9.86 U	X
27	15.51 in. (39.4 cm)	8.86 U	X
24	13.76 in. (34.9 cm)	7.86 U	X
21	12.01 in. (30.5 cm)	6.86 U	X
18	10.26 in. (26.0 cm)	5.86 U	X
15	8.51 in. (21.6 cm)	4.86 U	X
12	6.76 in. (17.1 cm)	3.86 U	X
9	5.01 in. (12.7 cm)	2.86 U	X
6	3.26 in. (8.3 cm)	1.86 U	X
3	1.51 in. (3.8 cm)	0.86 U	X

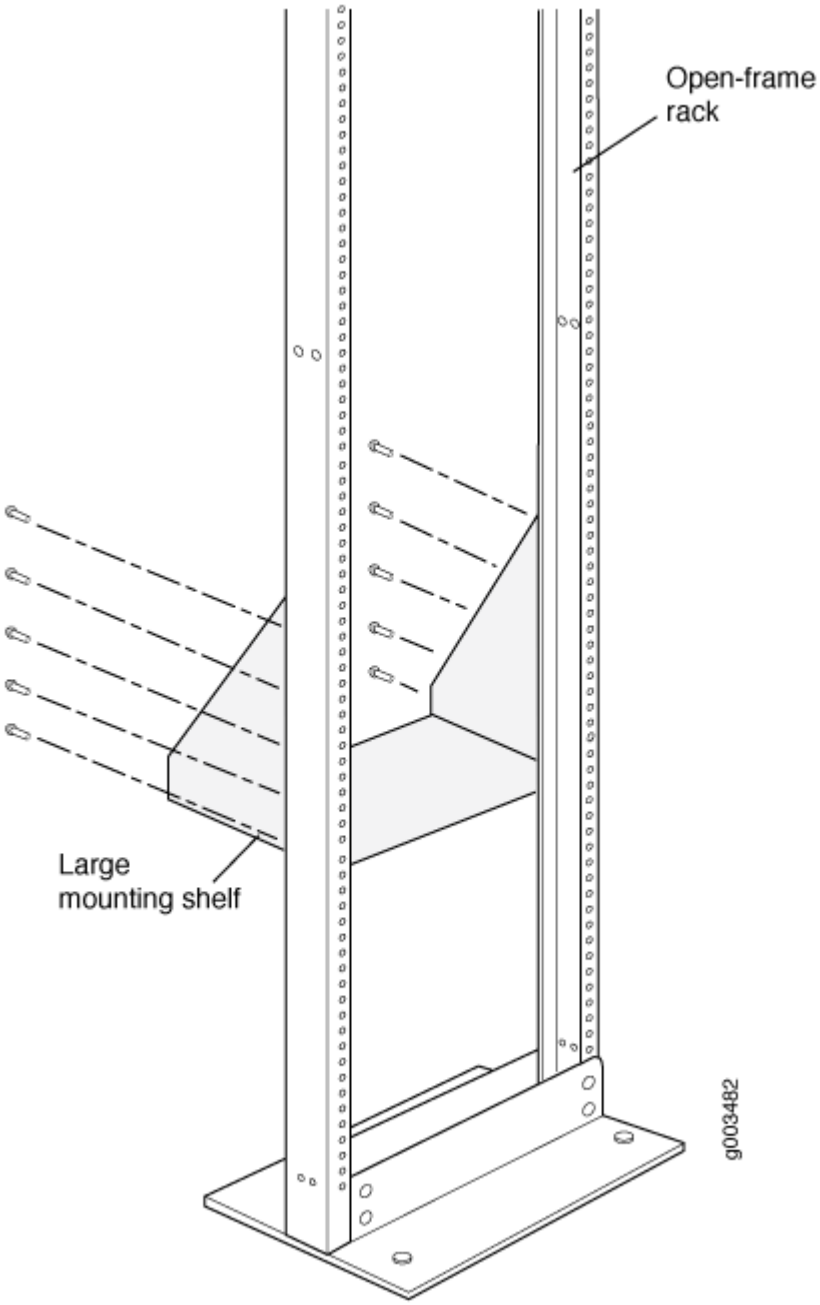
Table 69: Open-Frame Rack Mounting Hole Locations *(Continued)*

Hole	Distance Above “U” Division		Large Shelf
2	0.88 in. (2.2 cm)	0.50 U	X
1	0.25 in. (0.6 cm)	0.14 U	

To install the large mounting shelf (see Figure 96 on page 227):

1. On the rear of each rack rail, partially insert a mounting screw into the highest hole specified in Table 69 on page 225 for the large shelf.
2. Install the large shelf on the rack. Hang the shelf over the mounting screws using the keyhole slots located near the top of the large shelf flanges.
3. Partially insert screws into the open holes in the ears of the large shelf.
4. Tighten all the screws completely.

Figure 96: Installing the Mounting Hardware for an Open-Frame Rack



After the mounting hardware is installed, proceed to "Installing the SRX5800 Firewall Chassis in the Rack" on page 235.

Removing Components from the SRX5800 Chassis Before Installing It in the Rack

IN THIS SECTION

Before installing the firewall in the rack, you must first remove components from the chassis to make it light enough to safely maneuver into the rack. With components removed, the chassis weighs approximately 150 lb (68 kg). You reinstall the components into the chassis after it is installed in the rack.

Removing the Power Supplies Before Installing the SRX5800 Firewall Chassis

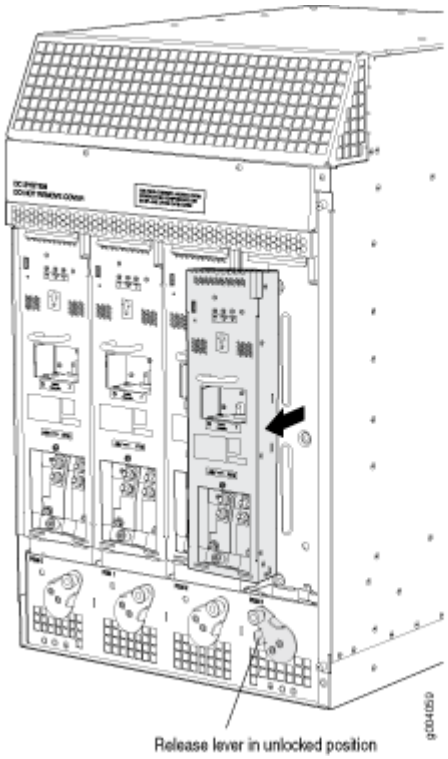
Remove the leftmost power supply first and then work your way to the right. To remove each AC or DC power supply (see Figure 3):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Switch off the firewall power supplies:
   - For an AC-powered firewall, move the AC input switch on the chassis above each AC power supply to the off (**O**) position. If the firewall is equipped with high-capacity AC power supplies, you must also move the AC input switch on each power supply to the off (**O**) position.
   - For DC-powered firewall, move the DC circuit breaker on each power supply faceplate to the off (**O**) position.

   We recommend switching off the power supplies even though they are not connected to power sources.
3. While grasping the handle on the power supply faceplate with one hand, use your other hand to pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever counterclockwise until it stops.
4. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
5. Pull the power supply straight out of the chassis.

WARNING: Do not touch the power connector on the top of the power supply. It can contain dangerous voltages.

Figure 97: Removing a Power Supply Before Installing the Firewall (Standard-Capacity Power Supply Shown, High-Capacity Similar)

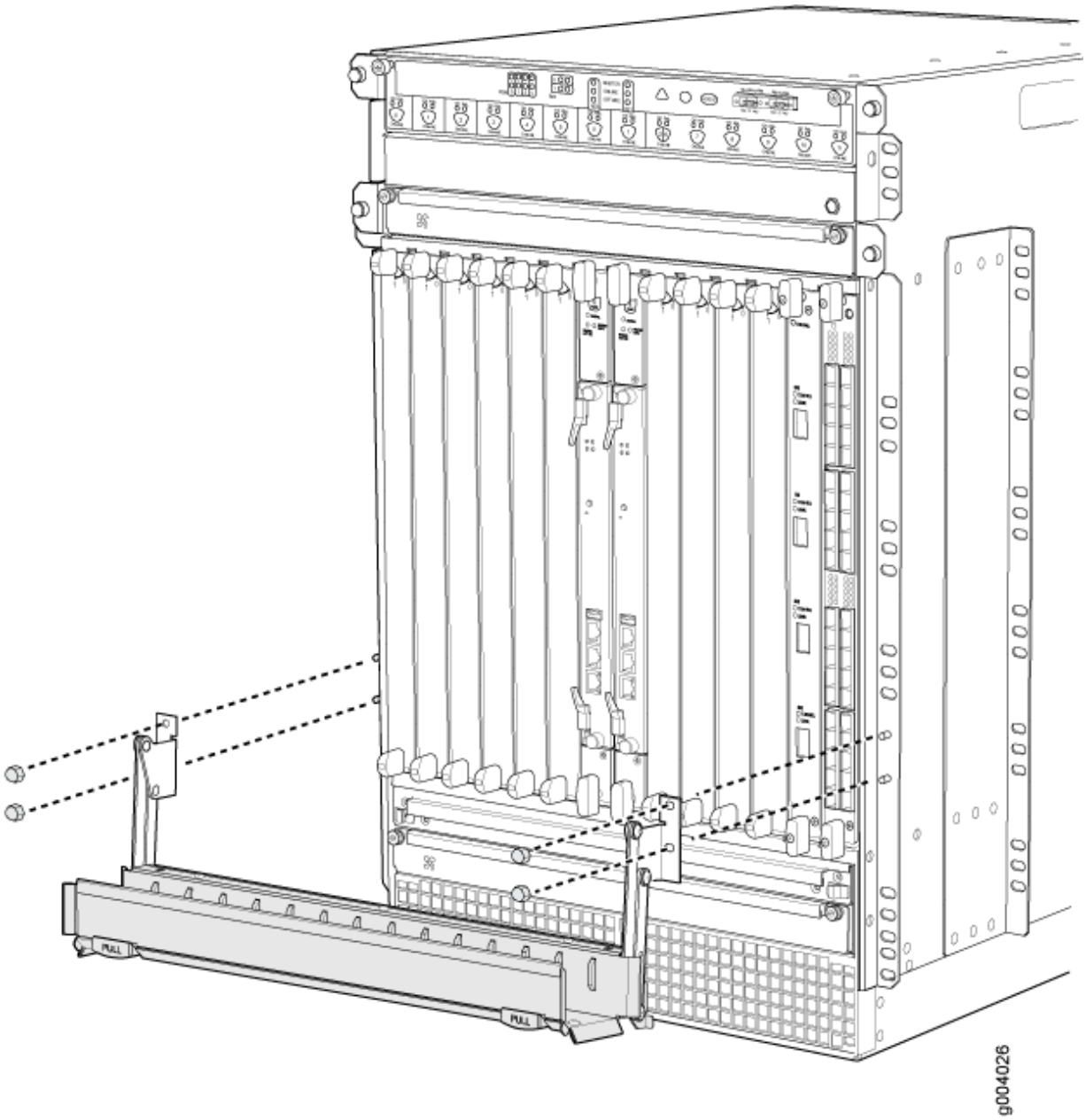


Removing the Cable Manager Before Installing the SRX5800 Firewall Chassis

To remove the cable manager (see Figure 4):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Using a 7/16-in. nut driver, unscrew the nuts on the corners of the cable manager.
3. Grasp the bottom of the cable manager and pull it straight out from the studs on the front of the chassis.

Figure 98: Removing the Cable Manager



Removing Fan Trays Before Installing the SRX5800 Firewall Chassis

To remove the upper or bottom fan tray (see Figure 5 and Figure 6, which illustrate the upper and bottom fan trays):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Loosen the captive screw on each side of the fan tray faceplate.

3. Grasp both sides of the fan tray and pull it out approximately 1 to 3 inches.
4. Press on the two latches located on the inside of the fan tray to release the fan tray from the chassis.
5. Place one hand under the fan tray to support it and pull the fan tray completely out of the chassis.

Figure 99: Removing an Upper Fan Tray

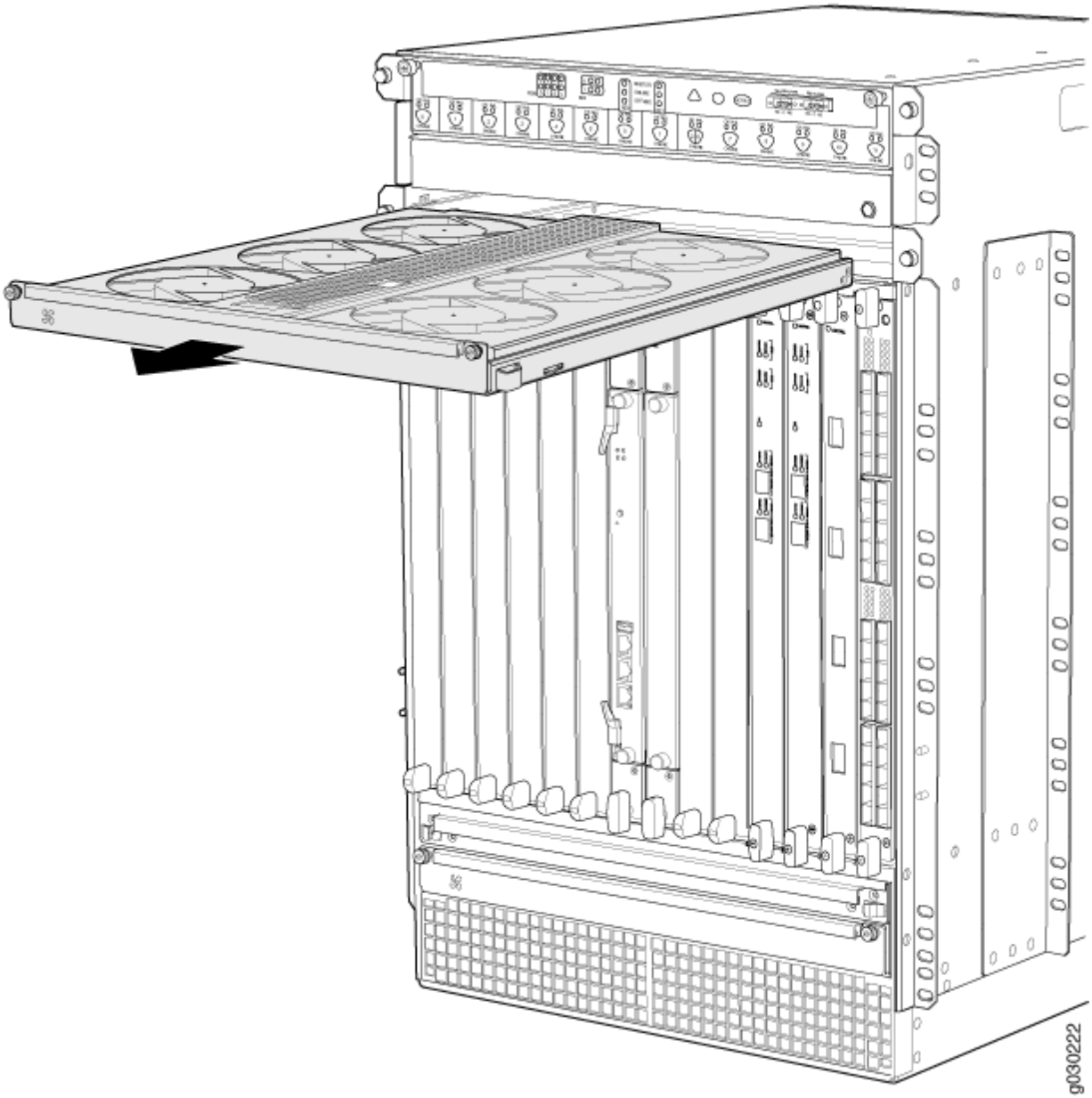
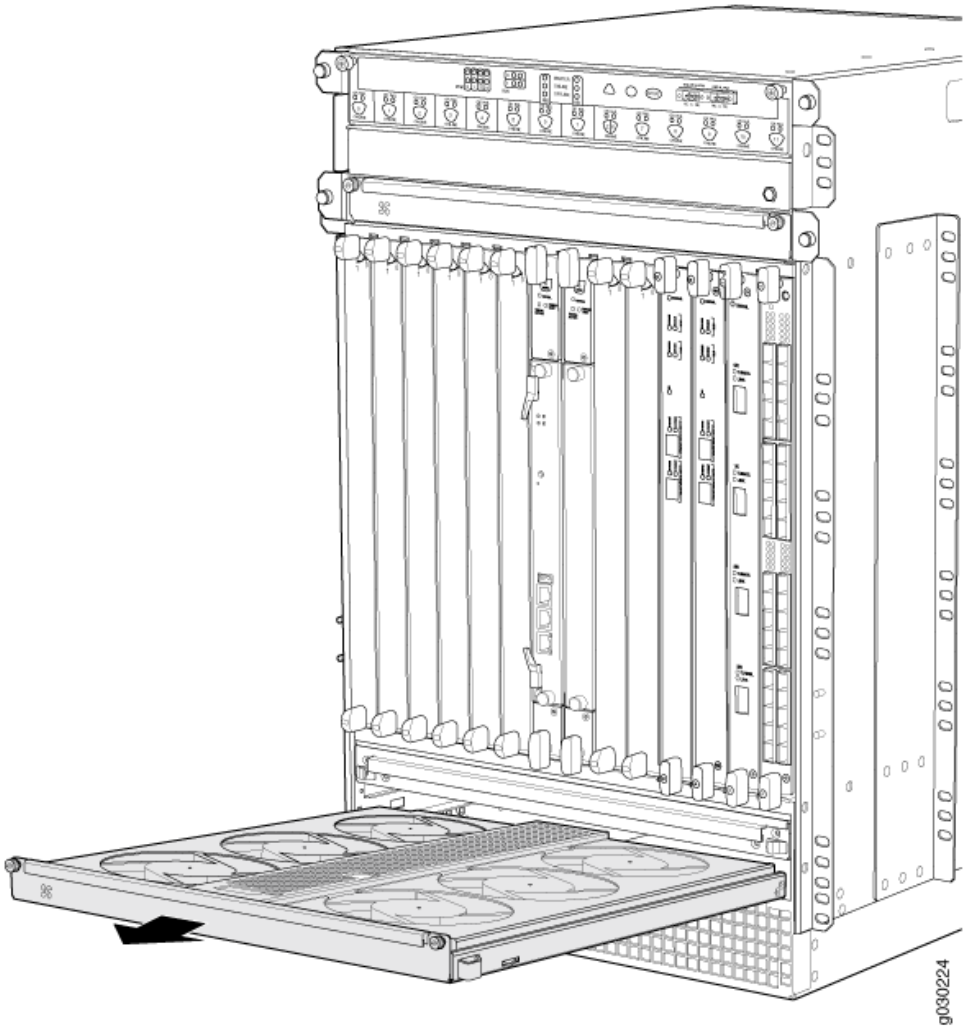


Figure 100: Removing the Bottom Fan Tray



Removing Cards Before Installing the SRX5800 Firewall Chassis

The firewall holds up to twelve cards (IOCs, Flex IOCs, MPCs, SCBs, and SPCs), which are installed horizontally in the front of the device. Each card weighs up to 18.3 lb (8.3 kg), be prepared to accept its full weight.

To remove a card (see Figure 7):

1. Have ready an antistatic mat for the card. Also have ready rubber safety caps for each port using an optical interface on the card that you are removing.
2. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
3. Label the cables connected to each port on the card so that you can later reconnect the cables to the correct ports.

4. If a card uses fiber-optic cable, immediately cover each transceiver and the end of each cable with a rubber safety cap. Arrange the disconnected cables in the cable management system, to prevent the cables from developing stress points.

   LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

   CAUTION: Do not leave a fiber-optic transceiver uncovered, except when you are inserting or removing cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

   CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

5. For SCBs, observe these points regarding the ejector handles:

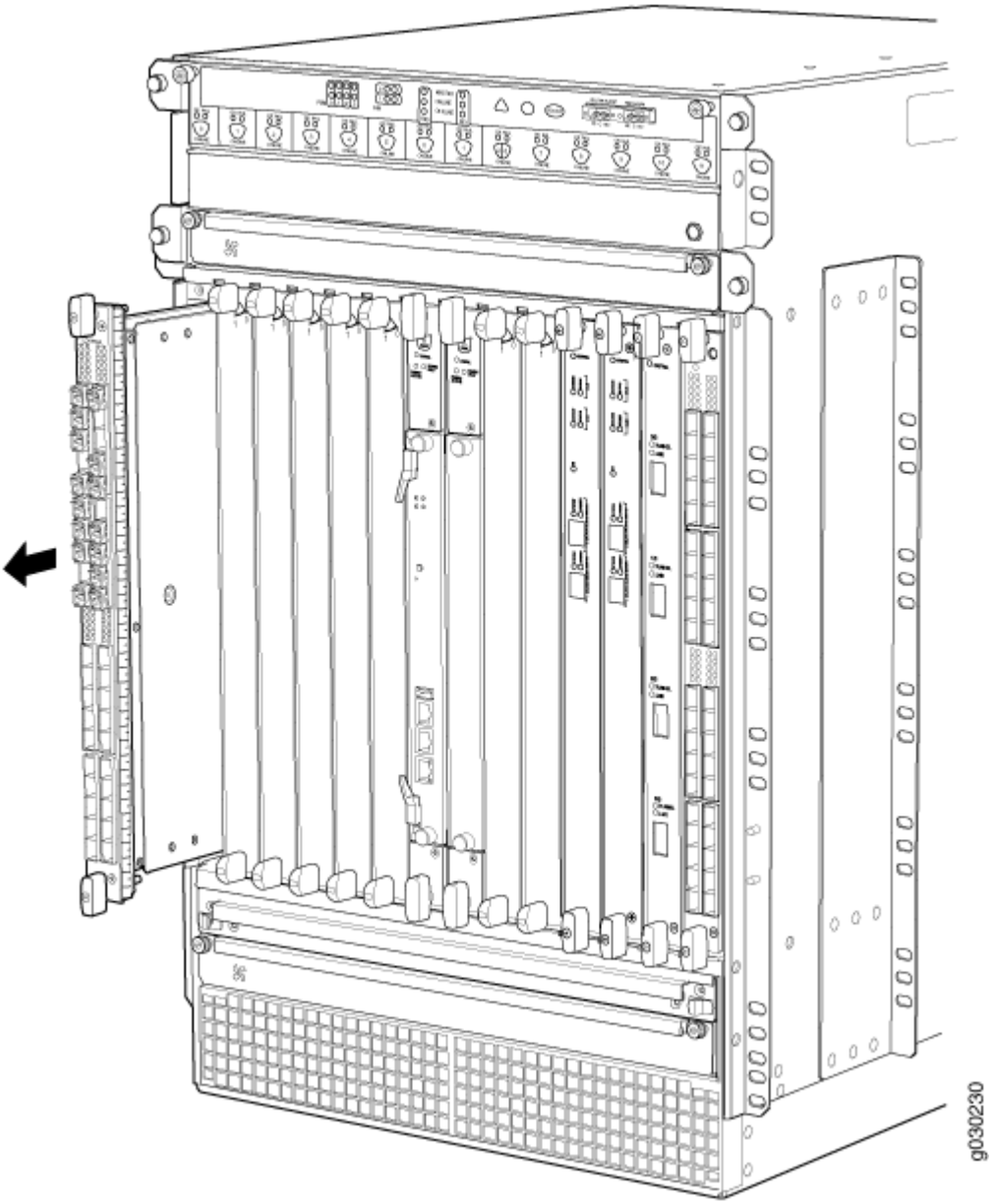
   - When removing or inserting an SCB, ensure that the SCBs or blank panels in adjacent slots are fully inserted to avoid hitting them with the ejector handles. The ejector handles require that all adjacent components be completely inserted so the ejector handles do not hit them, which could result in damage.
   - The ejector handles have a center of rotation and need to be stored toward the center of the board. Ensure the long ends of the ejectors located at both the top and the bottom of the board are vertical and pressed as far as possible toward the center of the board. Once you have installed an SCB, place the ejector handles in their proper position, vertically and toward the center of the board. To avoid blocking the visibility of the LEDs, position the ejectors over the PARK icon.
   - To insert or remove the SCB card, slide the ejector across the SCB horizontally, rotate it, and slide it again another quarter of a turn. Turn the ejector again and repeat as necessary. Use the indexing feature to maximize leverage and to avoid hitting any adjacent components.

6. Simultaneously turn both the ejector handles counterclockwise to unseat the card.
7. Grasp the handles and slide the card straight out of the card cage halfway.
8. Place one hand around the front of the card and the other hand under it to support it. Slide the IOC completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

CAUTION: The weight of the card is concentrated in the back end. Be prepared to accept the full weight—up to 13.1 lb (5.9 kg)—as you slide the card out of the chassis. When the card is out of the chassis, do not hold it by the ejector handles, bus bars, or edge connectors. They cannot support its weight.

Do not stack cards on top of one another after removal. Place each one individually in an electrostatic bag or on its own antistatic mat on a flat, stable surface.

Figure 101: Removing a Card (IOC Shown, Other Card Types Similar)



Installing the SRX5800 Firewall Chassis in the Rack

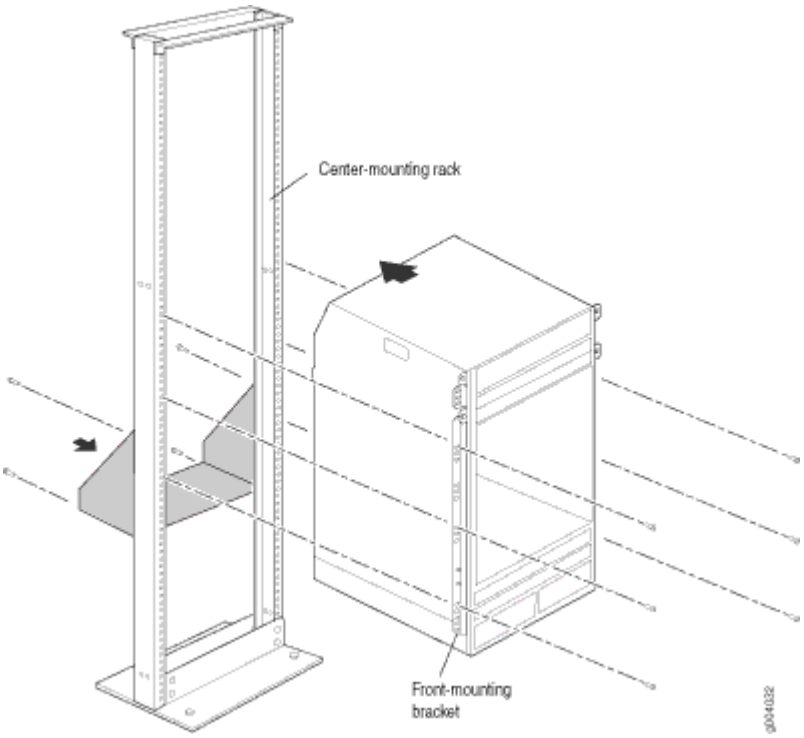
Because of the firewall's size and weight—up to 400 lb (182 kg) depending on the configuration—you must install the firewall using a mechanical lift.

CAUTION: Before front mounting the firewall in a rack, have a qualified technician verify that the rack is strong enough to support the firewall's weight and is adequately supported at the installation site.

To install the firewall using a lift (see Figure 102 on page 237):

1. Ensure the rack is in its permanent location and is secured to the building. Ensure that the installation site allows adequate clearance for both airflow and maintenance.
2. Load the firewall onto the lift, making sure it rests securely on the lift platform.
3. Using the lift, position the firewall in front of the rack or cabinet, centering it in front of the mounting shelves.
4. Lift the chassis approximately 0.75 in. above the surface of the mounting shelves and position it as close as possible to the shelves.
5. Carefully slide the firewall onto the mounting shelves so that the bottom of the chassis and the mounting shelves overlap by approximately two inches.
6. Slide the firewall onto the mounting shelves until the center-mounting brackets or front-mounting flanges contact the rack rails. The shelves ensure that the holes in the center-mounting brackets and the front-mounting flanges of the chassis align with the holes in the rack rails.
7. Move the lift away from the rack.
8. To install the firewall in an open-frame rack, install a mounting screw into each of the open mounting holes aligned with the rack, starting from the bottom.
9. Visually inspect the alignment of the firewall. If the firewall is installed properly in the rack, all the mounting screws on one side of the rack should be aligned with the mounting screws on the opposite side and the firewall should be level.

Figure 102: Installing the Firewall in the Rack



NOTE: This illustration depicts the firewall being installed in an open-frame rack.

Reinstalling Components in the SRX5800 Firewall Chassis After Installing It in the Rack

IN THIS SECTION

After the firewall is installed in the rack, reinstall the removed components before booting and configuring the firewall. You reinstall components first in the rear of the chassis, and then in the front:

Reinstalling Power Supplies After Installing the SRX5800 Firewall Chassis

Reinstall the rightmost power supply first and then work your way to the left. To reinstall the AC or DC power supplies, follow this procedure for each power supply (see Figure 9, which shows the installation of the DC power supplies):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.

   Verify that the power supplies are switched off:

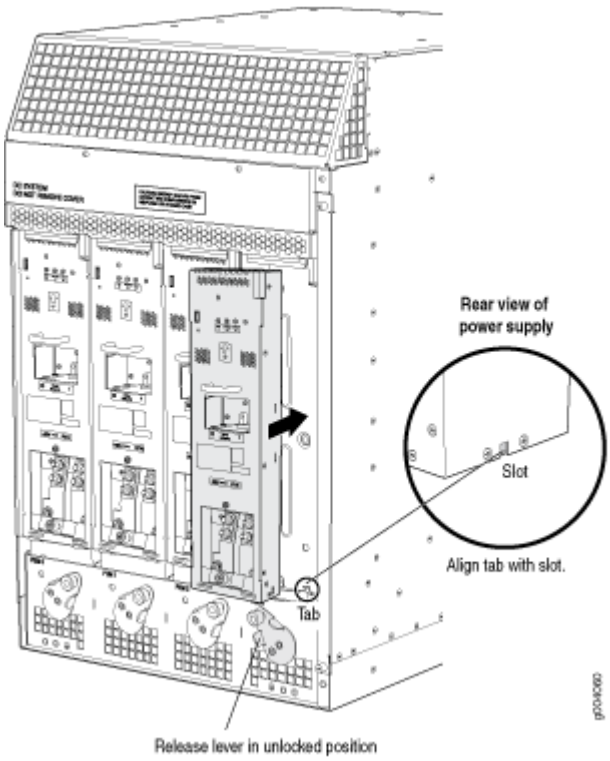
   - For an AC-powered firewall, verify that the AC input switch on the chassis above each AC power supply is in the off (**O**) position. If the firewall is equipped with high-capacity AC power supplies, also verify that the AC input switch on each power supply is in the off (**O**) position.
   - For DC-powered firewall, verify that the DC circuit breaker on each power supply faceplate is in the off (**O**) position.

   We recommend verifying that the power supplies are switched off even though they are not connected to power sources.
2. Ensure that the release lever below the empty power supply slot is locked in the counterclockwise position (see Figure 9).

   If necessary, pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever counterclockwise until it stops. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
3. Using both hands, slide the power supply straight into the chassis until the power supply is fully seated in the chassis slot. The power supply faceplate should be flush with any adjacent power supply faceplates.

   The small tab on the metal housing that is controlled by the release lever must be inside of the corresponding slot at the bottom of the power supply. This tab is used to pull the power supply down in the chassis slot, prior to removing the power supply.
4. While firmly pushing the handle on the power supply faceplate with one hand, use your other hand to pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever clockwise until it stops.
5. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.

Figure 103: Reinstalling a Power Supply (Standard-Capacity Shown, High-Capacity Similar)



Reinstalling Fan Trays After Installing the SRX5800 Firewall Chassis

To reinstall the fan trays (see Figure 10 and Figure 11):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Grasp the fan tray on each side and insert it straight into the chassis. Note the correct orientation by the "this side up" label on the top surface of the fan tray.
3. Tighten the captive screws on each side of the fan tray faceplate to secure it in the chassis.
4. Lower the standard cable manager back into position, if necessary.

Figure 104: Installing an Upper Fan Tray

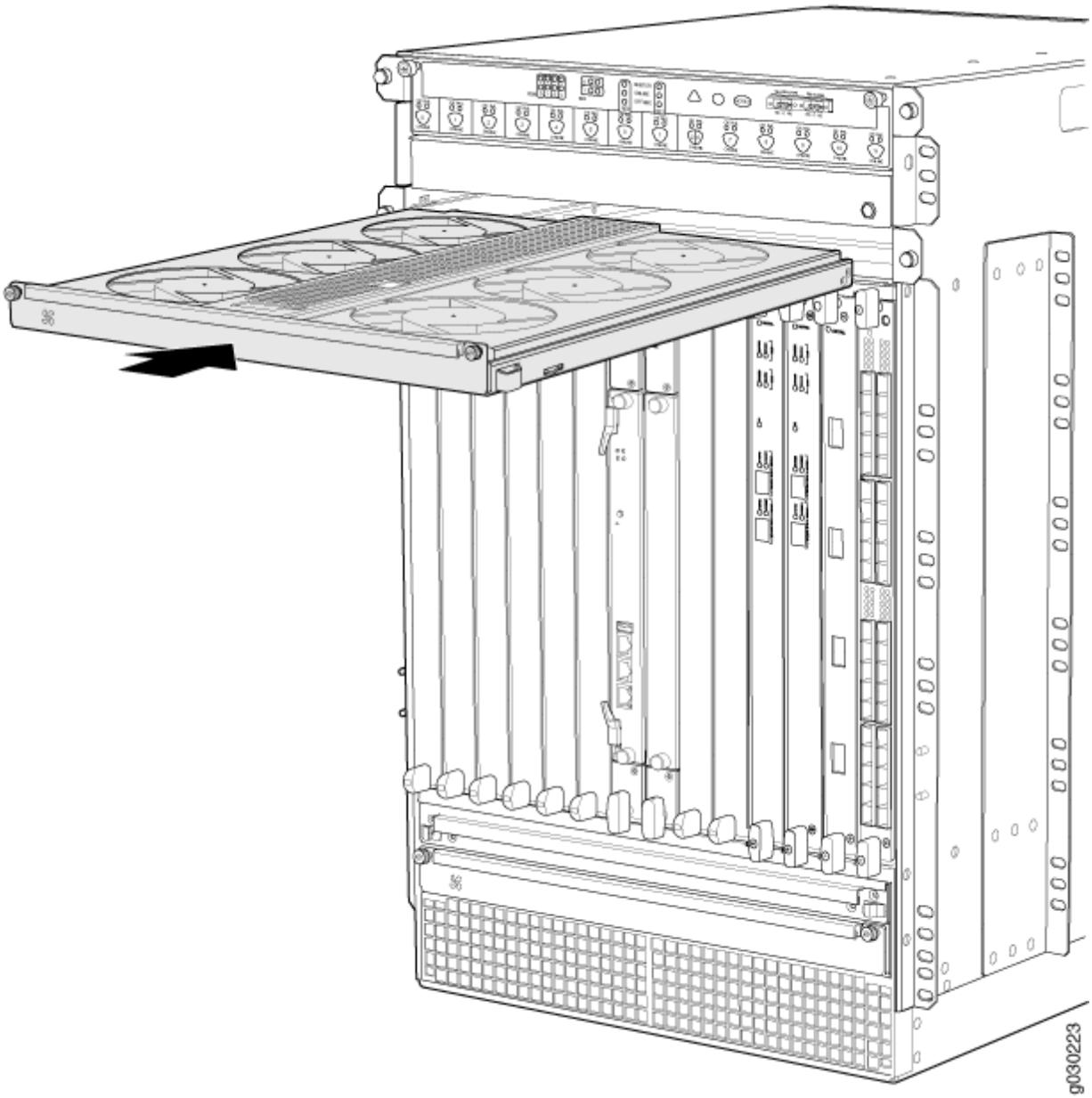
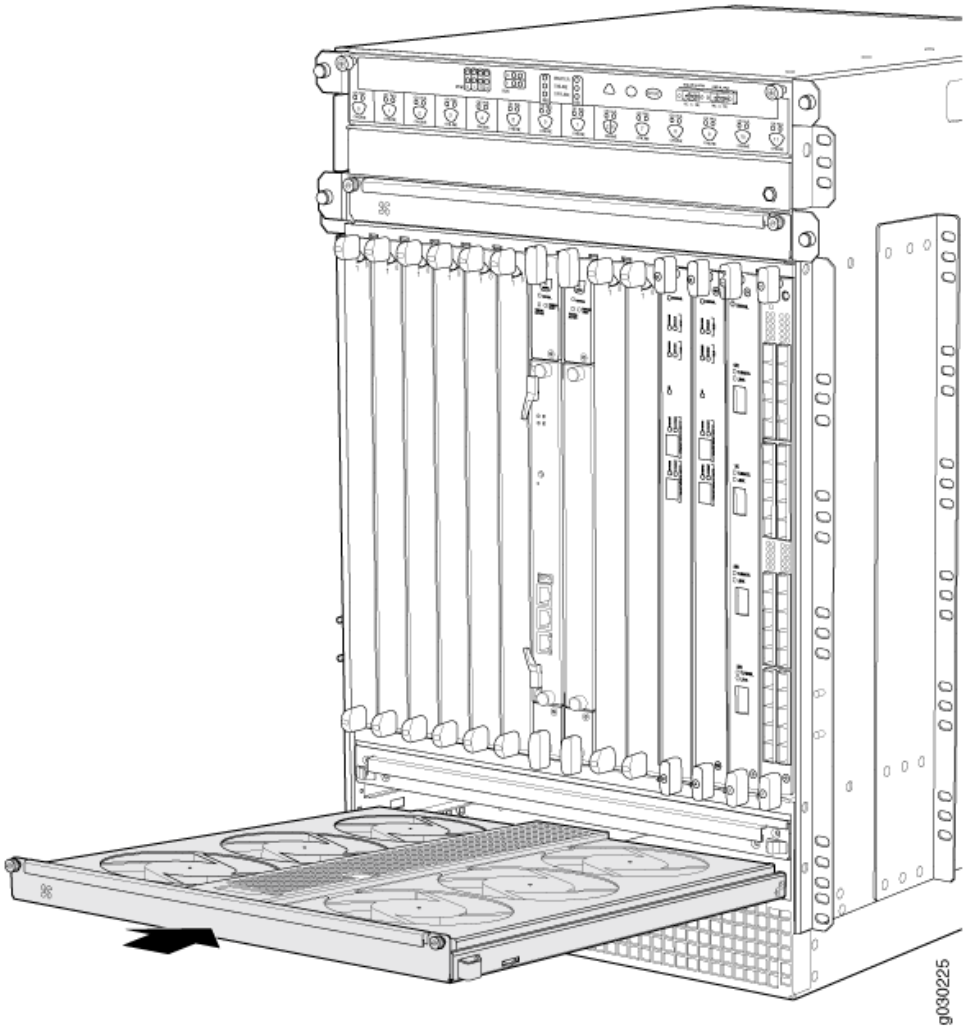


Figure 105: Installing the Bottom Fan Tray



Reinstalling Cards After Installing the SRX5800 Firewall Chassis

To reinstall cards (IOCs, Flex IOCs, MPCs, SPCs, and SCBs (see Figure 12):

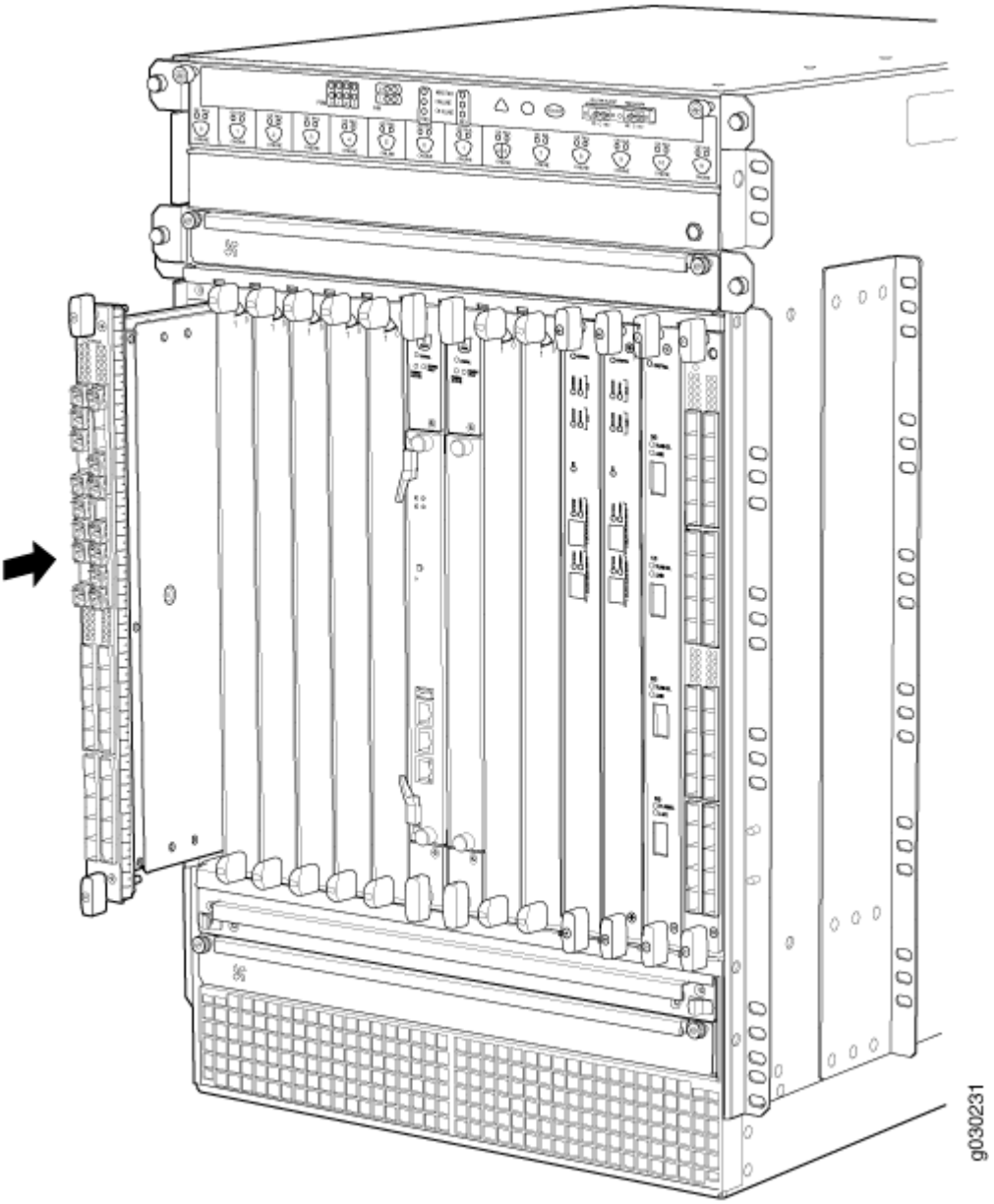
1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Take each card to be installed out of its electrostatic bag and identify the slot on the card cage where it will be connected.
3. Verify that each fiber-optic port has a rubber safety cap covering the transceiver. If it does not, cover the transceiver with a safety cap.
4. Locate the slot in the card cage in which you plan to install the card.
5. Ensure the card is right-side up, with the text on the faceplate of the card facing upward.

6. Lift the card into place and carefully align first the bottom, then the top of the card with the guides inside the card cage.
7. Slide the card all the way into the card cage until you feel resistance.
8. For SCBs, observe these points regarding the ejector handles:
   - When removing or inserting an SCB, ensure that the SCBs or blank panels in adjacent slots are fully inserted to avoid hitting them with the ejector handles. The ejector handles require that all adjacent components be completely inserted so the ejector handles do not hit them, which could result in damage.
   - The ejector handles have a center of rotation and need to be stored toward the center of the board. Ensure the long ends of the ejectors located at both the top and the bottom of the board are vertical and pressed as far as possible toward the center of the board. Once you have installed an SCB, place the ejector handles in their proper position, vertically and toward the center of the board. To avoid blocking the visibility of the LEDs,position the ejectors over the PARK icon.
   - To insert or remove the SCB card, slide the ejector across the SCB horizontally, rotate it, and slide it again another quarter of a turn. Turn the ejector again and repeat as necessary. Use the indexing feature to maximize leverage and to avoid hitting any adjacent components.
9. Grasp both ejector handles and rotate them simultaneously clockwise until the card is fully seated.
10. Insert the appropriate cable into the cable connector ports on each card. Secure each cable so that it is not supporting its own weight. Place excess cable out of the way in a neatly coiled loop, using the cable management system. Placing fasteners on a loop helps to maintain its shape.

CAUTION: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

Figure 106: Installing an IOC

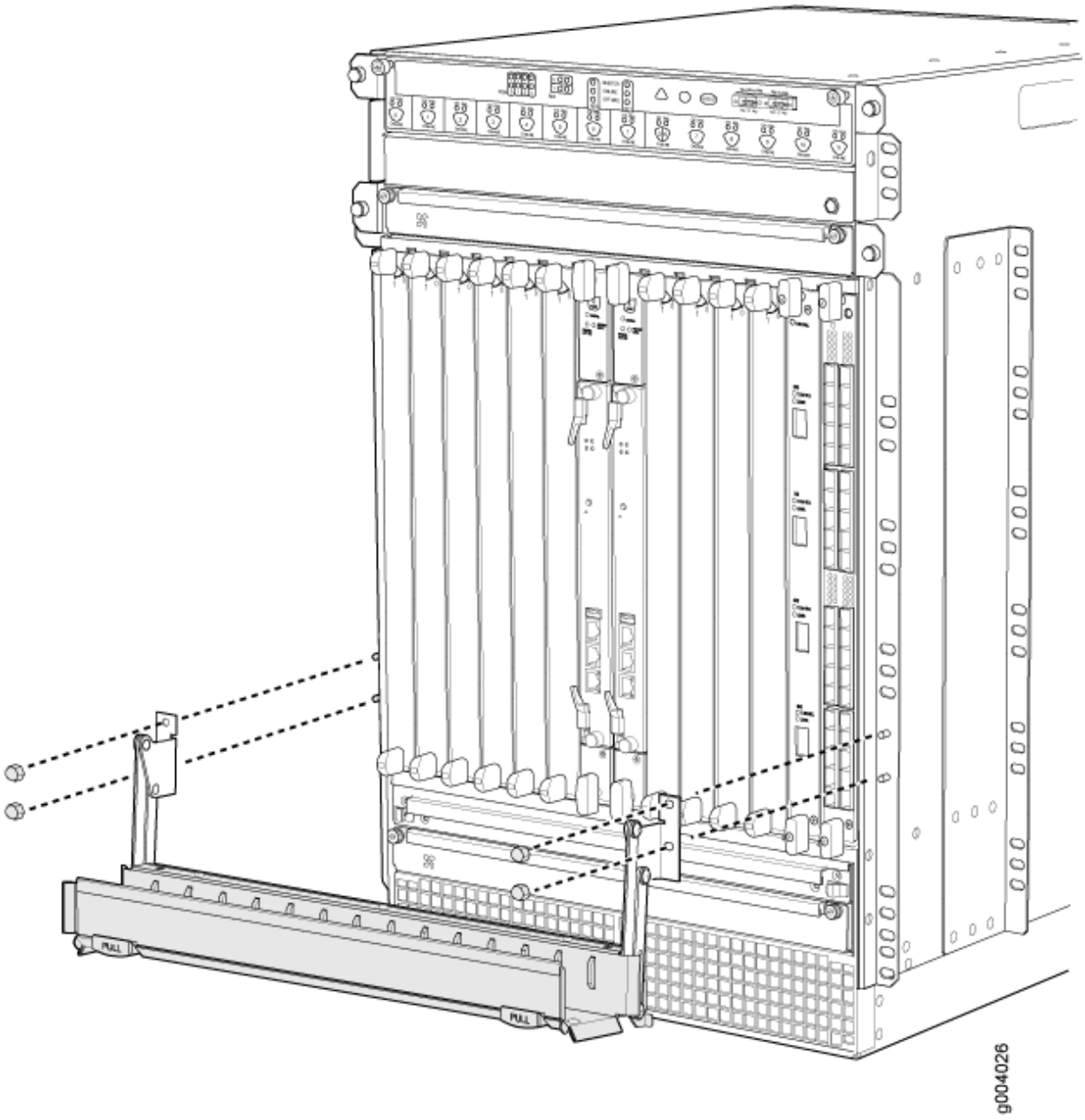


Reinstalling the Cable Manager After Installing the SRX5800 Firewall Chassis

To reinstall the cable manager (see Figure 13):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Position the cable manager on the studs on the lower front of the chassis.
3. Insert the nuts on the corners in the cable manager onto the studs on the chassis.
4. Using a 7/16-in. nut driver, tighten the nuts securely.

Figure 107: Reinstalling the Cable Manager



Connecting the SRX5800 to External Devices

IN THIS SECTION

Tools and Parts Required for SRX5800 Firewall Connections

To connect the device to management devices and IOCs, you need the following tools and parts:

- Phillips (+) screwdrivers, numbers 1 and 2
- 2.5-mm flat-blade (-) screwdriver
- 2.5 mm Phillips (+) screwdriver
- Electrostatic discharge (ESD) grounding wrist strap

Connecting the SRX5800 Firewall to a Management Console or an Auxiliary Device

To use a system console to configure and manage the Routing Engine, connect it to the appropriate **CONSOLE** port on the Routing Engine. To use a laptop, modem, or other auxiliary device, connect it to the **AUX** port on the Routing Engine. Both ports accept a cable with an RJ-45 connector. To connect a device to the **CONSOLE** port and another device to the **AUX** port, you must supply two separate cables.

NOTE: We no longer include the console cable as part of the device package. If the console cable and adapter are not included in your device package, or if you need a different type of adapter, you can order the following separately:

- RJ-45 to DB-9 adapter (JNP-CBL-RJ45-DB9)
- RJ-45 to USB-A adapter (JNP-CBL-RJ45-USBA)
- RJ-45 to USB-C adapter (JNP-CBL-RJ45-USBC)

If you want to use RJ-45 to USB-A or RJ-45 to USB-C adapter you must have X64 (64-Bit) Virtual COM port (VCP) driver installed on your PC. See https://ftdichip.com/drivers/vcp-drivers/ to download the driver.

To connect a management console or auxiliary device:

1. Plug the RJ-45 end of the serial cable (Figure 108 on page 246 shows the connector) into the **AUX** port or **CONSOLE** port on the Routing Engine. Figure 109 on page 246 shows the ports.

Figure 108: Routing Engine Console and Auxiliary Cable Connector

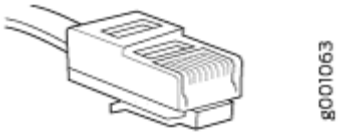
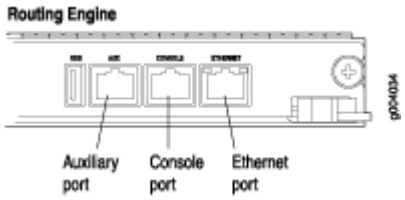


Figure 109: Auxiliary and Console Ports



2. Plug the socket DB-9 end into the device's serial port.

NOTE: For console devices, configure the serial port to the following values:

- Baud rate—9600
- Parity—N
- Data bits—8

- Stop bits—1
- Flow control—none

Connecting the SRX5800 Firewall to a Network for Out-of-Band Management

To connect the Firewall Routing Engine to a network for out-of-band management, connect an Ethernet cable with RJ-45 connectors to the **ETHERNET** port on the Routing Engine. To connect to the **ETHERNET** port on the Routing Engine:

1. Plug one end of the Ethernet cable (Figure 110 on page 247 shows the connector) into the **ETHERNET** port on the Routing Engine. Figure 111 on page 247 shows the port.
2. Plug the other end of the cable into the network device.

Figure 110: Routing Engine Ethernet Cable Connector

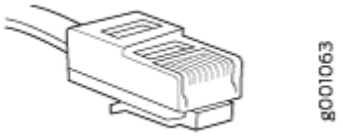
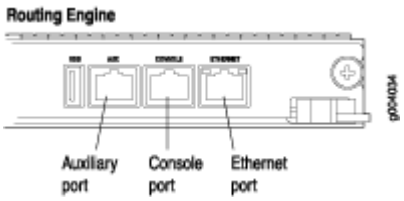


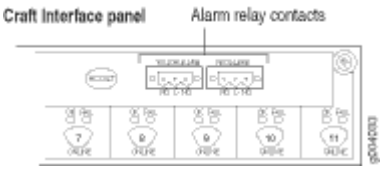
Figure 111: Ethernet Port



Connecting an SRX5800 Firewall to an External Alarm-Reporting Device

To connect the firewall to external alarm-reporting devices, attach wires to the **RED** and **YELLOW** relay contacts on the craft interface. (See Figure 112 on page 248.) A system condition that triggers the red or yellow alarm LED on the craft interface also activates the corresponding alarm relay contact.

Figure 112: Alarm Relay Contacts

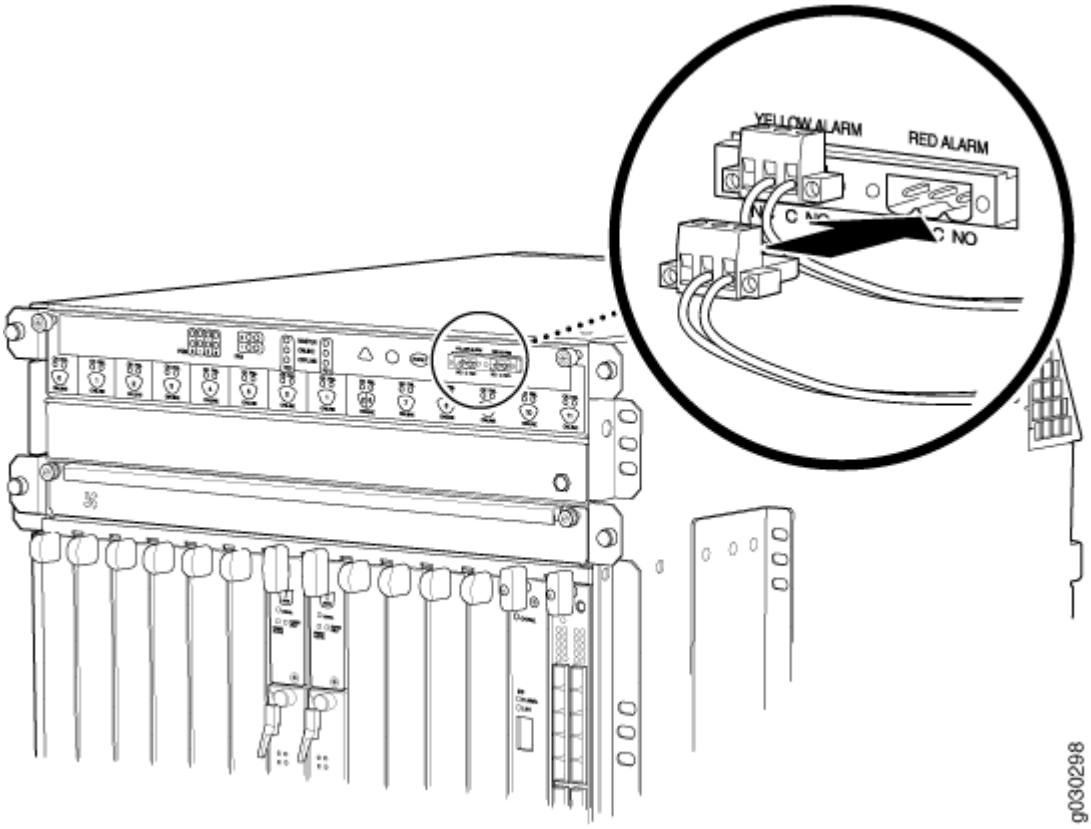


The terminal blocks that plug into the alarm relay contacts are supplied with the firewall. They accept wire of any gauge between 28-AWG and 14-AWG (0.08 and 2.08 mm^2), which is not provided. Use the gauge of wire appropriate for the external device you are connecting.

To connect an external device to an alarm relay contact (see Figure 112 on page 248):

1. Prepare the required length of wire with gauge between 28-AWG and 14-AWG (0.08 and 2.08 mm^2).
2. While the terminal block is not plugged into the relay contact, use a 2.5-mm flat-blade screwdriver to loosen the small screws on its top. With the small screws on its top facing upward, insert wires into the slots in the front of the block based on the wiring for the external device. Tighten each screw to secure the corresponding wire.
3. Plug the terminal block into the relay contact, and use a 2.5-mm flat-blade screwdriver to tighten the screws on the face of the block. See Figure 113 on page 249.

Figure 113: Connecting an External Alarm-Reporting Device



4. Attach the other end of the wires to the external device.

To attach a reporting device for the other kind of alarm, repeat the procedure.

Connecting Network Cables to SRX5800 Firewall IOCs and Port Modules

To connect the IOCs, MPCs, and port modules to the network (see Figure 114 on page 251):

1. Have ready a length of the type of cable used by the component.
2. Remove the rubber safety plug from the cable connector port.

LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

CAUTION: Do not leave a fiber-optic transceiver uncovered, except when inserting or removing a cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

3. Insert the cable connector into the cable connector port on the faceplate.

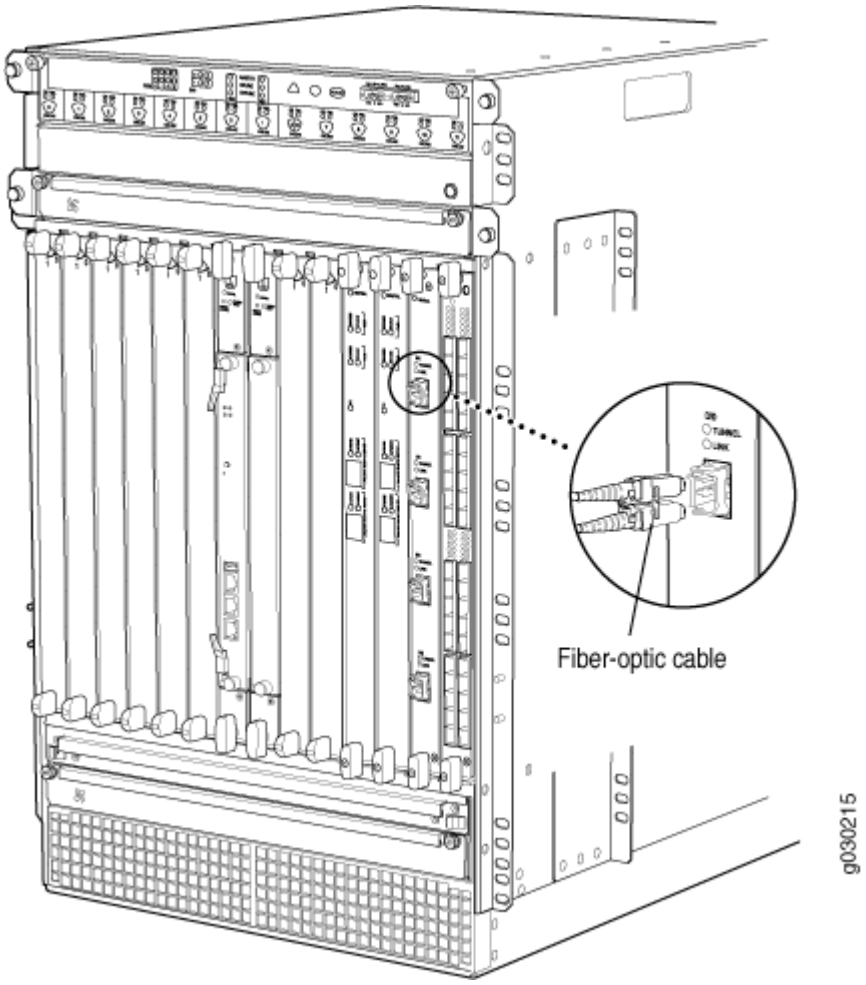
NOTE: The XFP cages and optics on the components are industry standard parts that have limited tactile feedback for insertion of optics and fiber. You need to insert the optics and fiber firmly until the latch is securely in place.

4. Arrange the cable in the standard or extended cable manager to prevent it from dislodging or developing stress points. Secure the cable so that it is not supporting its own weight as it hangs to the floor. Place excess cable out of the way in a neatly coiled loop. Placing fasteners on the loop helps to maintain its shape.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

CAUTION: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

Figure 114: Attaching a Cable to an IOC



Connecting the SRX5800 to Power

IN THIS SECTION

"Connecting Power to an AC-Powered SRX5800 Firewall" on page 254

Tools and Parts Required for SRX5800 Firewall Grounding and Power Connections

To ground and provide power to the firewall, you need the following tools and parts:

- Phillips (+) screwdrivers, numbers 1 and 2
- 2.5-mm flat-blade (–) screwdriver
- 7/16-in. hexagonal-head external drive socket wrench, or nut driver, with a torque range between 23 lb-in. (2.6 Nm) and 25 lb-in. (2.8 Nm) tightening torque, for tightening nuts to terminal studs on each power supply on a DC-powered firewall.
- Wire cutters
- Electrostatic discharge (ESD) grounding wrist strap

Grounding the SRX5800 Firewall

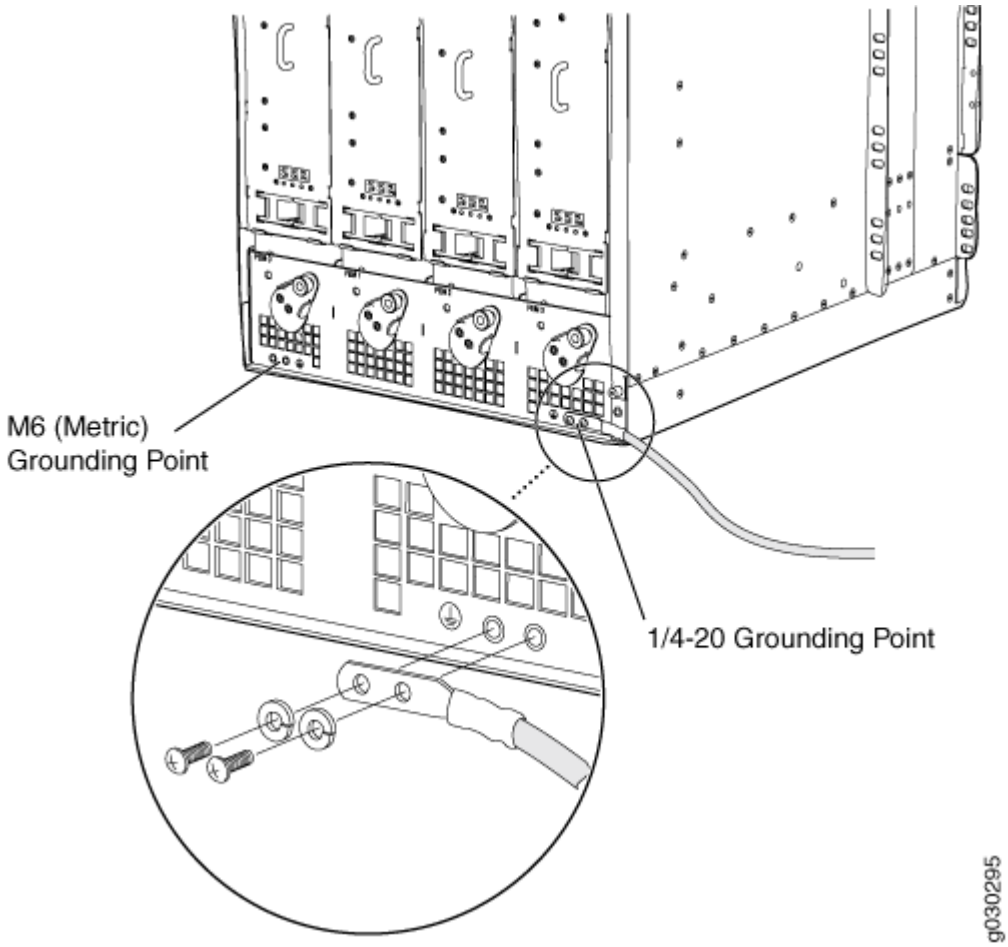
WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power. You must install the SRX8500 device in a restricted-access location and ensure that the chassis is always properly grounded. The SRX5800 device has a two-hole protective grounding terminal provided on the chassis. See Figure 115 on

page 254. Under all circumstances, use this grounding connection to ground the chassis. For AC-powered systems, you must also use the grounding wire in the AC power cord along with the two-hole grounding lug connection. This tested system meets or exceeds all applicable EMC regulatory requirements with the two-hole protective grounding terminal.

You ground the firewall by connecting a grounding cable to earth ground and then attaching it to one of the chassis grounding points using two screws. You must provide the grounding cable (the cable lug is supplied with the firewall).

1. Verify that a licensed electrician has attached the cable lug provided with the firewall to the grounding cable.
2. Attach an ESD grounding strap to your bare wrist and connect the strap to an approved site ESD grounding point. See the instructions for your site.
3. Ensure that all grounding surfaces are clean and brought to a bright finish before grounding connections are made.
4. Connect the grounding cable to a proper earth ground.
5. Detach the ESD grounding strap from the site ESD grounding point.
6. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
7. Place the grounding cable lug over one of the two grounding points. The right pair is sized for UNC 1/4-20 screws and 1/4 in. split washers, which are provided in the accessory box. The left pair is sized for M6 metric screws. If you wish to use the metric-sized grounding point, you must provide appropriate screws and split washers.
8. Secure the grounding cable lug to the grounding point, first with the washers, and then with the screws as shown in Figure 115 on page 254.

Figure 115: Connecting the Grounding Cable



9. Dress the grounding cable and verify that it does not touch or block access to firewall components, and that it does not drape where people could trip on it.

Connecting Power to an AC-Powered SRX5800 Firewall

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power. See "Grounding the SRX5800 Firewall" on page 252 for instructions.

CAUTION: Do not mix AC and DC power supplies within the same firewall. Damage to the firewall might occur.

You connect AC power to the device by attaching power cords from the AC power sources to the AC appliance inlets located on the chassis above the power supplies. If the firewall is powered by high-capacity power supplies, you also connect AC feeds to AC appliance inlets located on the power supplies themselves. The power cords are not provided with the firewall; you must order them separately.

To connect the AC power cords to the firewall (see Figure 116 on page 256 and Figure 117 on page 257):

1. Locate or obtain the power cords you will use with the firewall. The power cords must have a plug appropriate for your geographical location.
2. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
3. Move the AC input switch on the chassis above each power supply to the off (**O**) position. If the firewall is equipped with high-capacity AC power supplies, you must also move the AC input switch on each power supply to the off (**O**) position.
4. For each installed AC power supply, connect a power cord to the appliance inlet on the chassis directly above the power supply.
5. If your firewall is equipped with high-capacity AC power supplies, you must also connect a power cord to the appliance inlet located on each power supply.
6. Insert the power cord plugs into an external AC power source receptacle.

   NOTE: Each power supply must be connected to a dedicated AC power feed and a dedicated customer site circuit breaker. We recommend that you use a 15 A (250 VAC) minimum, or as required by local code.

7. Dress the power cords appropriately. Verify that the power cords do not block the air exhaust and access to firewall components, or drape where people could trip on them.
8. Repeat Step 3 through Step 7 for the remaining power supplies.

Figure 116: Connecting AC Power to the Firewall (Standard-Capacity Power Supplies)

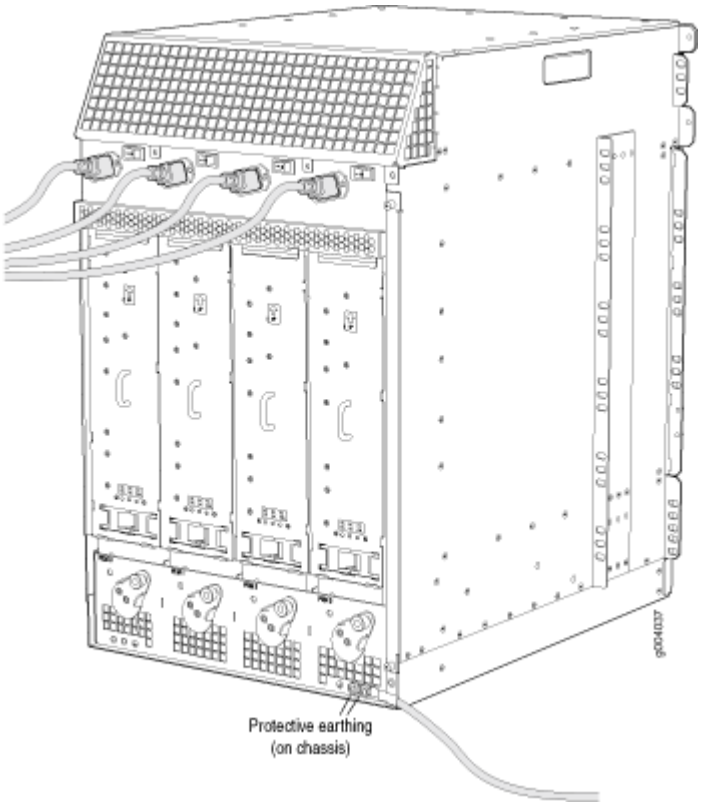
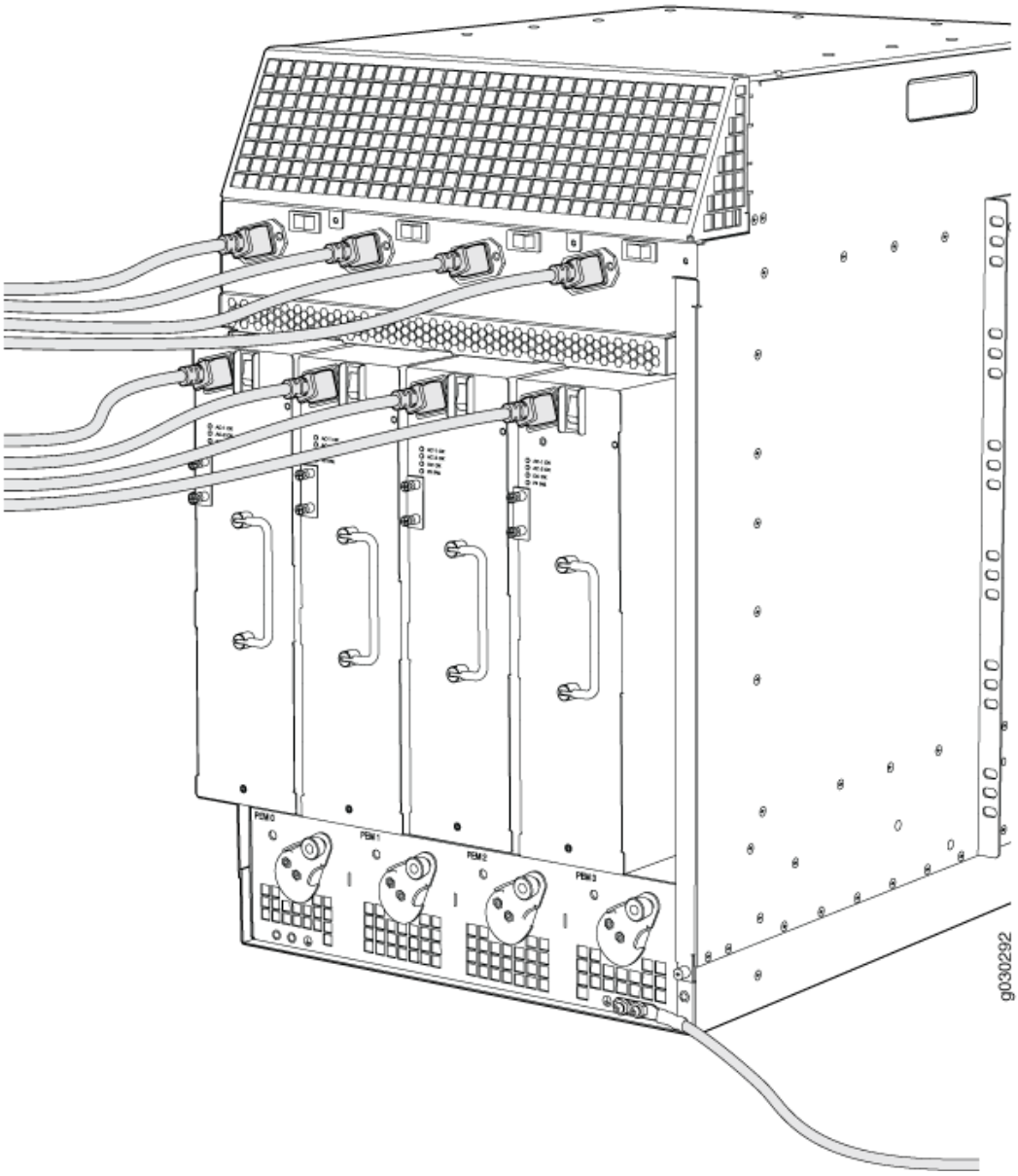


Figure 117: Connecting AC Power to the Firewall (High-Capacity Power Supplies)



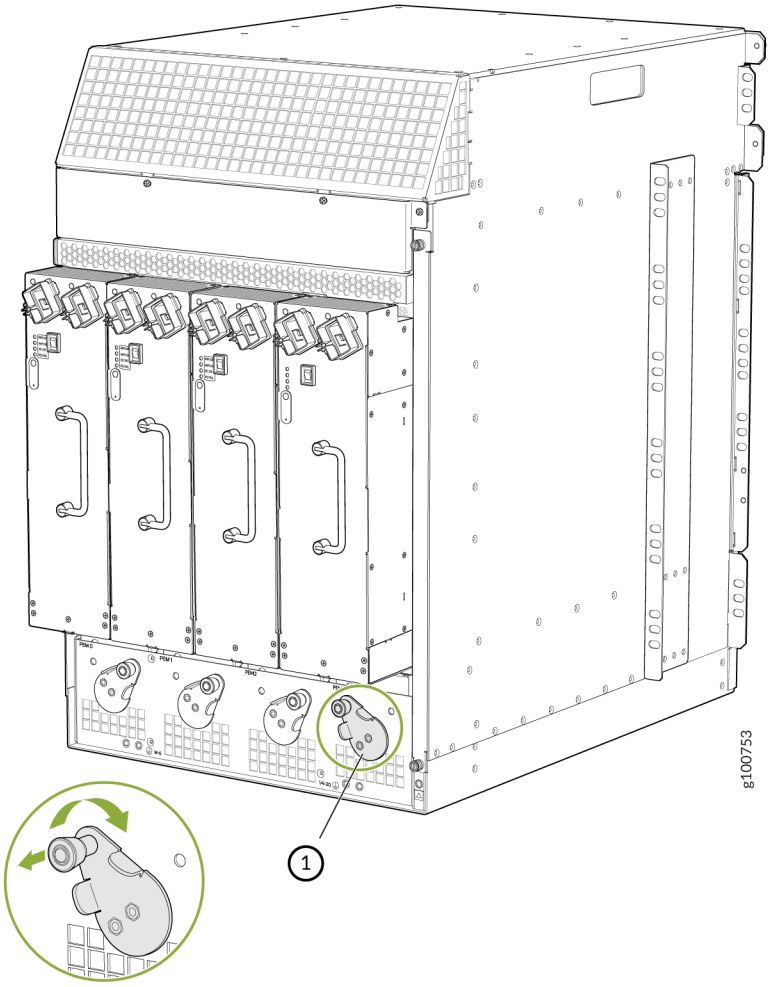
Connect Power to an SRX5800 Firewall with High-Capacity Second-Generation Power Supplies

A minimum of two AC nominal 220 VAC 20 amp power cords are required for this procedure.

To install and power on an SRX5800 Firewall with High-Capacity Second-Generation AC (MX960-PSM-5K-AC) power supply, use the following procedure.

1. Verify that the power switch on the power supply is in the off (**O**) position.
2. Ensure that the release lever below the empty power supply slot is locked in the counterclockwise position (see Figure 118 on page 258).

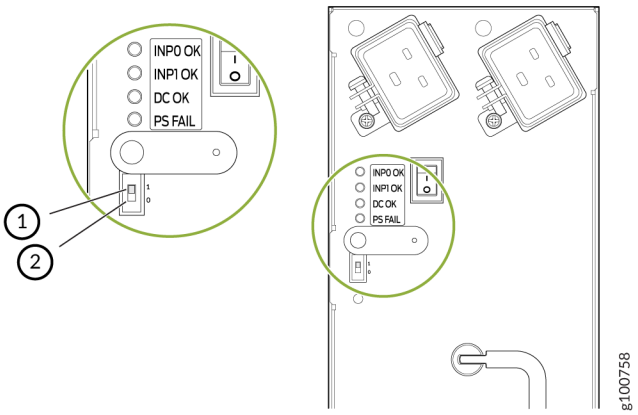
Figure 118: SRX5800 Firewall with High-Capacity Second Generation AC Power Supplies Installed



If necessary, pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever counterclockwise until it stops. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.

3. On the power supply, rotate the metal cover away from the input mode switch to expose the switch.
4. Move the input mode switch to position 0 if you plan to connect one feed, or position 1 if you plan to connect two feeds (see Figure 119 on page 259).

Figure 119: SRX5800 High-Capacity Second-Generation AC Power Input Mode Switch



1– **1** (if you connect two feeds)	2– **0** (if you connect one feed)

CAUTION: Do not use a pencil, because fragments can break off and cause damage to the power supply.

5. Using both hands, slide the power supply straight into the chassis until the power supply is fully seated in the chassis slot. The power supply faceplate will protrude beyond the chassis.

   The small tab on the metal housing that is controlled by the release lever must be inside of the corresponding slot at the bottom of the power supply (see Figure 118 on page 258). This tab is used to pull the power supply down in the chassis slot, prior to removing the power supply.
6. While firmly pushing the handle on the power supply faceplate with one hand, use your other hand to pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever clockwise until it stops.
7. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
8. Make sure the cover is attached on the power distribution unit on the chassis.
9. Make sure the grounding cable is attached, See .
10. Locate a power cord with the type of plug appropriate for your geographical location (see).
11. Plug the power cord into the corresponding appliance inlet located in the chassis directly on the power supply. If using the power supply in two-feed mode, plug the second power cord into the receptacle on the power supply.

    Using a screwdriver, tighten the screw on the retainer to prevent the AC cord from getting lose. See Figure 120 on page 260.

NOTE: Each power supply must be connected to a dedicated AC power feed and a dedicated customer site circuit breaker.

NOTE: To use high-capacity second-generation AC power supplies with full capacity you have to switch them to two feed mode and use two power cords per power supply. See Figure 120 on page 260.

Figure 120: SRX5800 with One High-Capacity Second-Generation AC Power Feed Connected

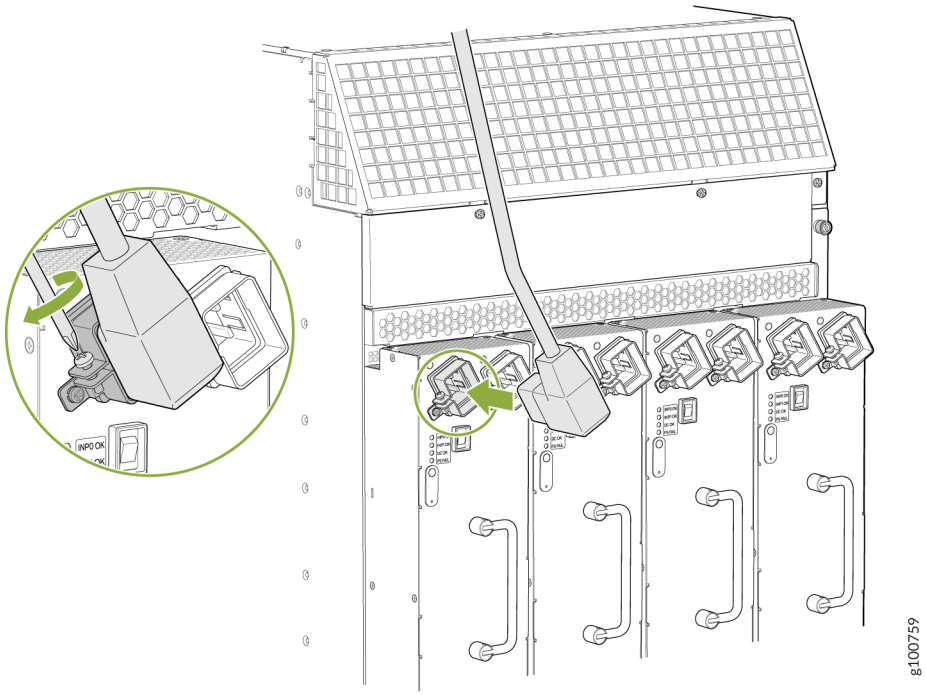
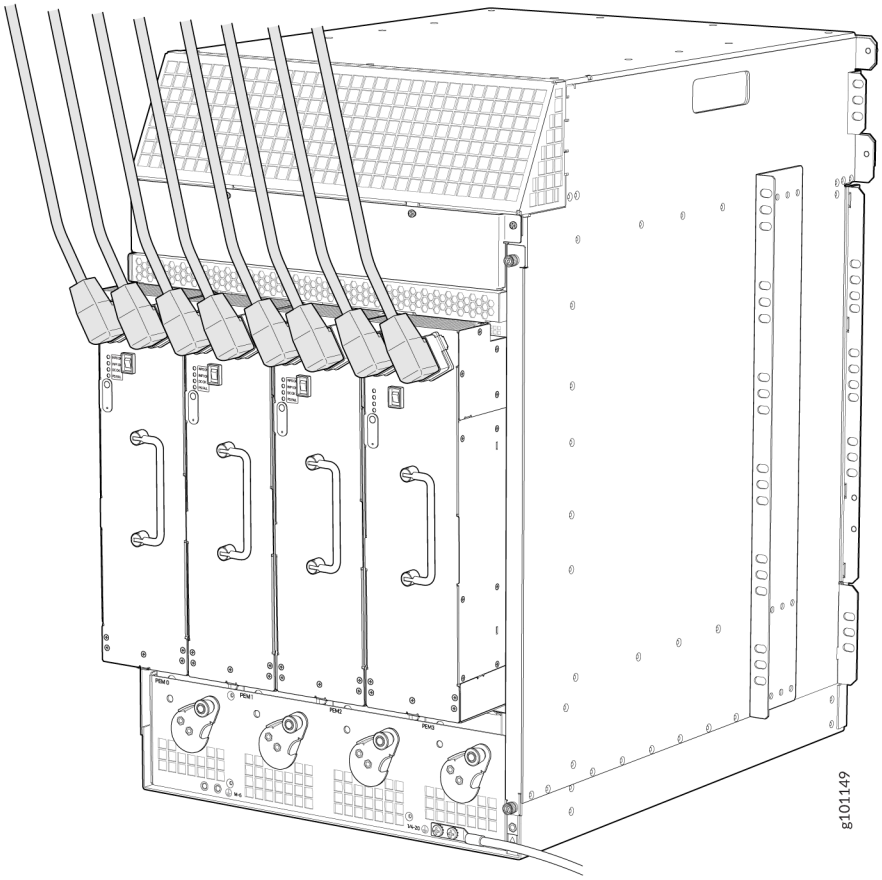
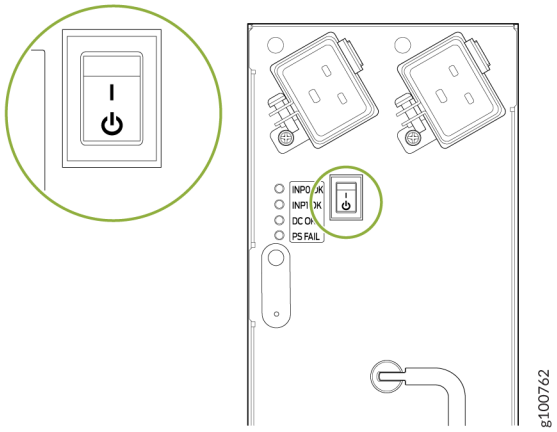


Figure 121: SRX5800 with Both High-Capacity Second-Generation AC Power Feeds Connected



12. Dress the power cords appropriately. Verify that the power cord does not block the air exhaust and access to router components, and that they do not drape where people could trip on them.
13. Move the AC input switch above the power supply to the on (—) position. See Figure 122 on page 262. This is the only switch you have to turn on.

Figure 122: SRX5800 with High-Capacity Second-Generation AC Power Supplies Input Switch



14. If the power supply is correctly installed and functioning normally, the **IN1 OK**, **IN2 OK** (two-feed mode only) **DC OK** LEDs light steadily, and the **PS FAIL** LED is not lit. See Table 70 on page 262.

Table 70: High-Capacity Second-Generation AC Power Supply DIP Switch Position and LEDs Behaviour

Connected Inputs	DIP Switch Position	LEDs			
		INP0 OK	**INP1 OK**	**DC OK**	**PS FAIL**
INP0 connected, INP1 disconnected	0 (1 input)	Green	Off	Green	Off
INP0 disconnected, INP1 connected	0 (1 input)	Off	Green	Green	Off
INP0 connected, INP1 connected	0 (1 input)	Green	Green	Green	Off

Table 70: High-Capacity Second-Generation AC Power Supply DIP Switch Position and LEDs Behaviour *(Continued)*

Connected Inputs	DIP Switch Position	LEDs			
		INP0 OK	**INP1 OK**	**DC OK**	**PS FAIL**
INP0 connected, INP1 disconnected	1 (2 inputs)	Green	Off	Off	Red
INP0 disconnected, INP1 connected	1 (2 inputs)	Off	Green	Off	Red
INP0 connected, INP1 connected	1 (2 inputs)	Green	Green	Green	Off

15. Repeat steps 1-12 for installing power supplies in the other slot as required.

Powering On an AC-Powered SRX5800 Firewall

To power on an AC-powered firewall:

1. Verify that the power supplies are fully inserted in the chassis.
2. Verify that each AC power cord is securely inserted into its appliance inlet.
3. Verify that an external management device is connected to one of the Routing Engine ports (**AUX**, **CONSOLE**, or **ETHERNET**).
4. Turn on the power to the external management device.
5. Switch on the dedicated customer site circuit breakers. Follow the ESD and safety instructions for your site.
6. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.

7. Switch the AC switch in the chassis above each power supply to the on (—) position.
8. If the firewall has high-capacity power supplies installed, you must also move the AC switch at the top of each power supply to the on (|) position.
9. Verify the following LED indications for each installed power supply:
   - For standard-capacity AC power supplies, verify that the **AC OK** and **DC OK** LEDs light steadily and the **PS FAIL** LED is not lit.
   - For high-capacity AC power supplies, verify that the **DC OK** LED lights steadily, and the **PS FAIL** LED is not lit. In addition, the **AC-1 OK** LED should light green steadily if the upper AC feed (on the chassis above the power supply) is connected and receiving power, and the **AC-2 OK** LED should light green steadily if the lower AC feed (on the power supply itself) is connected and receiving power.

   NOTE: After a power supply is powered on, it can take up to 60 seconds for status indicators—such as the status LEDs on the power supply and the **show chassis** command display—to indicate that the power supply is functioning normally. Ignore error indicators that appear during the first 60 seconds.

   If any of the status LEDs indicates that the power supply is not functioning normally, repeat the installation and cabling procedures.
10. On the external management device connected to the Routing Engine, monitor the startup process to verify that the system has booted properly.

    NOTE: If the system is completely powered off when you power on the power supply, the Routing Engine boots as the power supply completes its startup sequence. Normally, the firewall boots from the Junos OS imageon the CompactFlash card.

    After you have powered on a power supply, wait at least 60 seconds before you power it off.

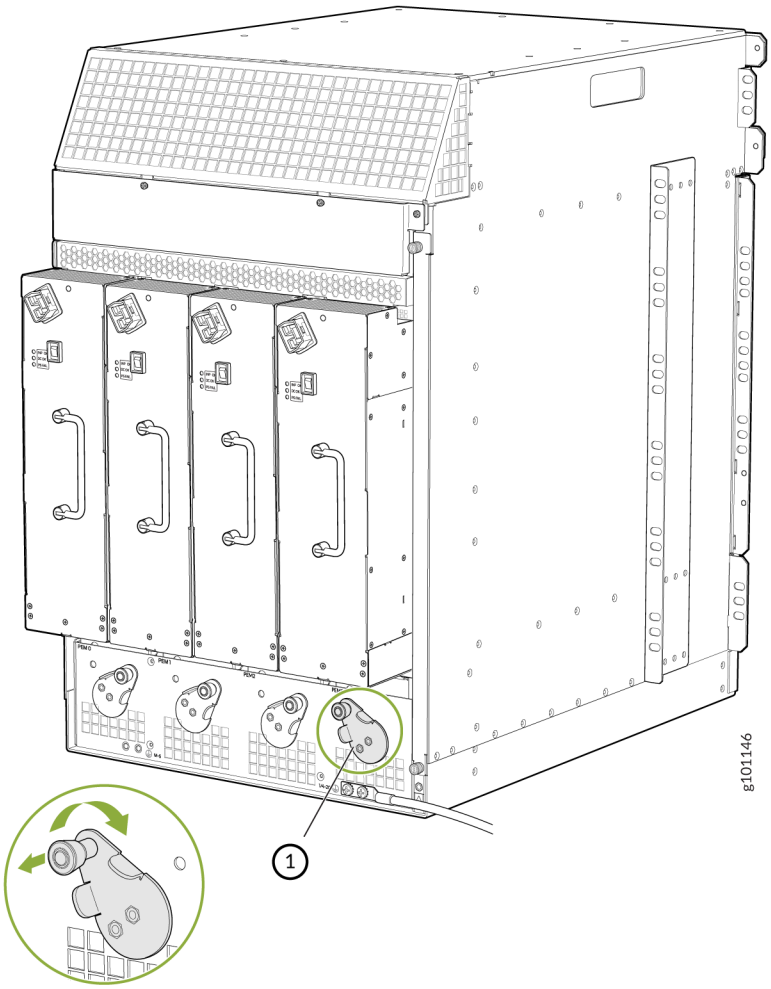
Connect Power to an SRX5800 Firewall with High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supplies

To install and power on an High-Voltage Second-Generation Universal (HVAC/HVDC) power supply, use the following procedure.

1. Verify that the power switch on the power supply is in the off (O) position.

2. Ensure that the release lever below the empty power supply slot is locked in the counterclockwise position (see Figure 123 on page 265).

Figure 123: SRX5800 Firewall with High-Voltage Second-Generation Universal (HVAC or HVDC) Installed



If necessary, pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever counterclockwise until it stops. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.

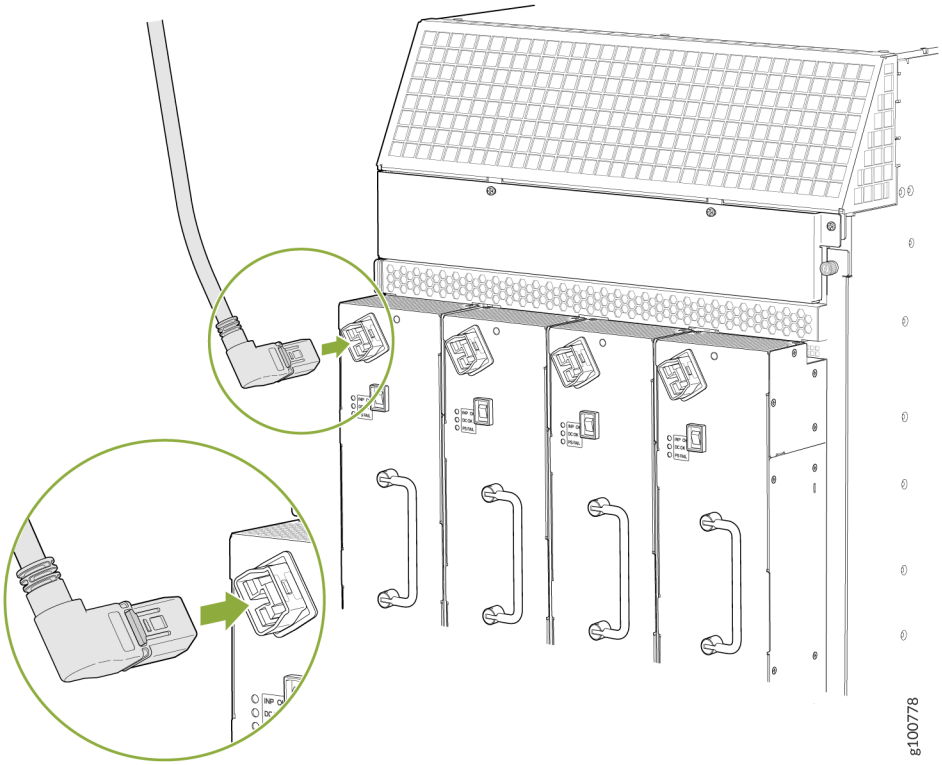
3. On the power supply, rotate the metal cover away from the input mode switch to expose the switch.
4. Using both hands, slide the power supply straight into the chassis until the power supply is fully seated in the chassis slot. The power supply faceplate protrudes beyond the chassis.

The small tab on the metal housing that is controlled by the release lever must be inside of the corresponding slot at the bottom of the power supply. This tab is used to pull the power supply down in the chassis slot, prior to removing the power supply.

5. While firmly pushing the handle on the power supply faceplate with one hand, use your other hand to pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever clockwise until it stops.
6. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
7. Make sure the cover is attached on the power distribution unit on the chassis on the high-voltage second-generation universal (HVAC or HVDC) power supply.
8. Make sure the grounding cable is attached,
9. Locate a power cord with the type of plug appropriate for your geographical location.
10. Plug the power cord into the corresponding appliance inlet located in the chassis directly on the power supply.

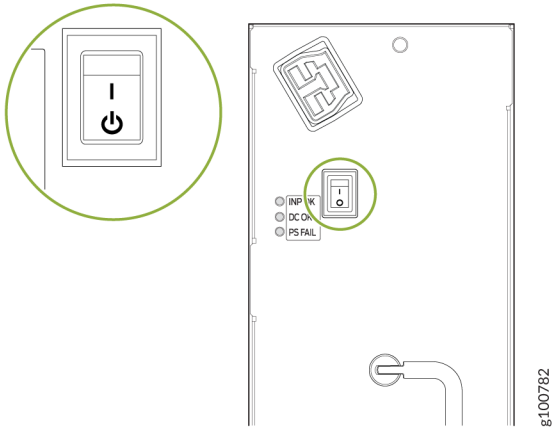
> **NOTE**: Each power supply must be connected to a dedicated power feed and a dedicated customer site circuit breaker.

Figure 124: SRX5800 Firewall with One High-Voltage Second-Generation (HVAC or HVDC) Power Feed Connected



11. Dress the power cords appropriately. Verify that the power cord does not block the air exhaust and access to router components, and that they do not drape where people could trip on them.
12. Move the input switch above the power supply to the on (—) position.

Figure 125: High-Voltage Second-Generation (HVAC or HVDC)MX960 AC Power Input Mode Switch



13. If the power supply is correctly installed and functioning normally, the **INP OK**, **DC OK** LEDs light steadily, and the **PS FAIL** LED is not lit.
14. Repeat steps 1-12 for installing power supplies in slots 1, 2, and 3, where required.

Connecting Power to a DC-Powered SRX5800 Firewall

WARNING: Before you perform DC power procedures, ensure there is no power to the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the off position, and tape the switch handle of the circuit breaker in the off position.

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power. See "Grounding the SRX5800 Firewall" on page 252 for instructions.

CAUTION: Do not mix AC and DC power supplies within the same firewall. Damage to the firewall might occur.

You connect DC power to the firewall by attaching power cables from the external DC power sources to the terminal studs on the power supply faceplates. You must provide the power cables (the cable lugs are supplied with the firewall).

To connect the DC source power cables to the firewall:

1. Switch off the dedicated customer site circuit breakers. Ensure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cable leads might become active during installation.
2. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
3. Move the DC circuit breaker on the power supply faceplate to the off (**O**) position.
4. Remove the clear plastic cover protecting the terminal studs on the faceplate.
5. Verify that the DC power cables are correctly labeled before making connections to the power supply. In a typical power distribution scheme where the return is connected to chassis ground at the battery plant, you can use a multimeter to verify the resistance of the **–48V** and **RTN** DC cables to chassis ground:
   - The cable with very large resistance (indicating an open circuit) to chassis ground is **–48V**.
   - The cable with very low resistance (indicating a closed circuit) to chassis ground is **RTN**.

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

   To install heat-shrink tubing:

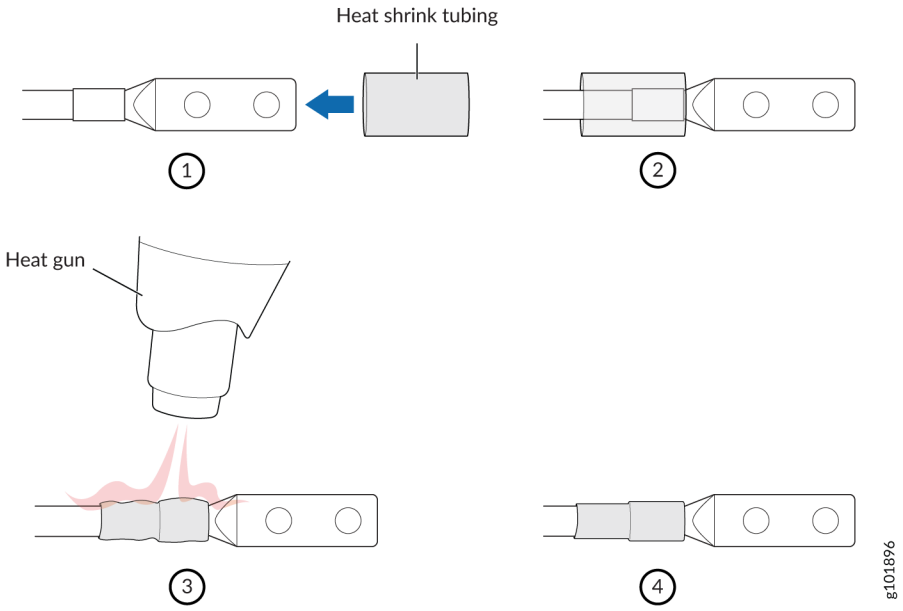
   a. Slide the tubing over the portion of the cable where it is attached to the lug barrel. Ensure that tubing covers the end of the wire and the barrel of the lug attached to it.

   b. Shrink the tubing with a heat gun. Ensure that you heat all sides of the tubing evenly so that it shrinks around the cable tightly.

   Figure 126 on page 270 shows the steps to install heat-shrink tubing.

   NOTE: Do not overheat the tubing.

Figure 126: How to Install Heat-Shrink Tubing



7. Remove the nuts and washers from the terminal studs. (Use a 7/16-in. nut driver or socket wrench.)
8. Secure each power cable lug to the terminal studs, first with the split washer, then with the nut (see Figure 127 on page 271). Apply between 23 lb-in. (2.6 Nm) and 25 lb-in. (2.8 Nm) of torque to each nut. (Use a 7/16-in. nut driver or socket wrench.)

   a. Secure each positive (+) DC source power cable lug to the **RTN** (return) terminal.

   b. Secure each negative (–) DC source power cable lug to the **–48V** (input) terminal.

   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.
9. For standard-capacity DC power supplies, secure each DC power cable to its strain relief bracket as follows:

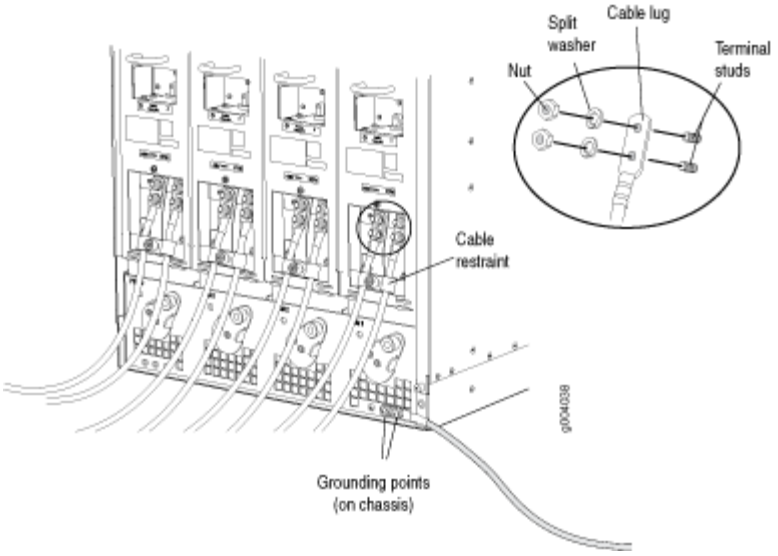
   a. Loosen the captive screw on the cable restraint on the lower edge of the power supply faceplate.

   b. Route the positive and negative DC power cables through the left and right sides of the cable restraint.

   c. Tighten the cable restraint captive screw to hold the power cables in place.
10. Replace the clear plastic cover over the terminal studs on the faceplate.

11. Verify that the power cables are connected correctly, that they are not touching or blocking access to firewall components, and that they do not drape where people could trip on them.
12. Repeat Steps 3 through 11 for the remaining power supplies.

Figure 127: Connecting DC Power to the Firewall (Standard-Capacity SHown, High-Capacity Similar)



Powering On a DC-Powered SRX5800 Firewall

To power on a DC-powered firewall:

1. Verify that an external management device is connected to one of the Routing Engine ports (**AUX**, **CONSOLE**, or **ETHERNET**).
2. Turn on the power to the external management device.
3. Verify that the power supplies are fully inserted in the chassis.
4. Verify that the source power cables are connected to the appropriate terminal: the positive (+) source cable to the return terminal (labeled **RTN**) and the negative (–) source cable to the input terminal (labeled **–48V**).
5. Switch on the dedicated customer site circuit breakers to provide power to the DC power cables. Follow your site's procedures.
6. Check the **INPUT OK** LED is lit steadily green to verify that power is present.
7. If power is not present:
   - Verify that the fuse is installed correctly and turn on the breaker at the battery distribution fuse board or fuse bay.

- Check the voltage with a meter at the terminals of the power supply for correct voltage level and polarity.

8. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
9. Move the DC circuit breaker on the DC power supplies to the on (|) position.
10. Verify that the **BREAKER ON** LED is lit green steadily.
11. Verify that the **PWR OK** LED is lit green steadily, indicating the power supply is correctly installed and functioning normally.

> **NOTE**: After a power supply is powered on, it can take up to 60 seconds for status indicators—such as the status LEDs on the power supply and the `show chassis` command display—to indicate that the power supply is functioning normally. Ignore error indicators that appear during the first 60 seconds.

If any of the status LEDs indicates that the power supply is not functioning normally, repeat the installation and cabling procedures .

12. On the external management device connected to the Routing Engine, monitor the startup process to verify that the system has booted properly.

> **NOTE**: If the system is completely powered off when you power on the power supply, the Routing Engine boots as the power supply completes its startup sequence. Normally, the firewall boots from the Junos OS image on the CompactFlash card.
>
> After powering on a power supply, wait at least 60 seconds before turning it off.

Powering Off the SRX5800 Firewall

> **NOTE**: After powering off a power supply, wait at least 60 seconds before turning it back on.

To power off the firewall:

1. On the external management device connected to the Routing Engine, issue the **request system halt** operational mode command. The command shuts down the Routing Engine cleanly, so its state information is preserved.

```
user@host> request system halt
```

2. Wait until a message appears on the console confirming that the operating system has halted.

   For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

3. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
4. Switch off the power supplies:
   - For an AC-powered firewall, move the AC input switch on the chassis above each AC power supply to the off (**O**) position. If the firewall is equipped with high-capacity AC power supplies, you must also move the AC input switch on each power supply to the off (**O**) position.
   - For a DC-powered firewall, move the DC circuit breaker on each DC power supply faceplate to the off (**O**) position.

Performing the Initial Software Configuration for the SRX5800

IN THIS SECTION

SRX5800 Firewall Software Configuration Overview

The firewall is shipped with the Junos operating system (Junos OS) preinstalled and ready to be configured when the device is powered on. There are three copies of the software: one on a

CompactFlash card (if installed) in the Routing Engine, one on the hard disk in the Routing Engine, and one on a USB flash drive that can be inserted into the slot in the Routing Engine faceplate.

When the device boots, it first attempts to start the image on the USB flash drive. If a USB flash drive is not inserted into the Routing Engine or the attempt otherwise fails, the device next tries the CompactFlash card (if installed), and finally the hard disk.

You configure the firewall by issuing Junos OS command-line interface (CLI) commands, either on a console device attached to the **CONSOLE** port on the Routing Engine, or over a telnet connection to a network connected to the **ETHERNET** port on the Routing Engine.

Gather the following information before configuring the device:

- Name the device will use on the network
- Domain name the device will use
- IP address and prefix length information for the Ethernet interface
- IP address of a default router
- IP address of a DNS server
- Password for the root user

Initially Configuring the SRX5800 Firewall

This procedure connects the device to the network but does not enable it to forward traffic. For complete information about enabling the device to forward traffic, including examples, see the appropriate Junos OS configuration guides.

To configure the software:

1. Verify that the device is powered on.
2. Log in as the root user. There is no password.
3. Start the CLI.

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

4. Enter configuration mode.

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

5. Set the root authentication password by entering either a cleartext password, an encrypted password, or an SSH public key string (DSA or RSA).

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

6. Configure an administrator account on the device. When prompted, enter the password for the administrator account.

```
[edit]
root@# set system login user admin class super-user authentication plain-text-password
New password: password
Retype new password: password
```

7. Commit the configuration to activate it on the device.

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

8. Log in as the administrative user you configured in Step 6.
9. Configure the name of the device. If the name includes spaces, enclose the name in quotation marks (“ ”).

```
configure
[edit]
admin@# set system host-name host-name
```

10. Configure the IP address and prefix length for the Ethernet management interface on the firewall's Routing Engine.

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

11. Configure the traffic interface.

```
[edit]
admin@# set interfaces ge-6/2/0 unit 0 family inet address address/prefix-length
admin@# set interfaces ge-6/3/5 unit 0 family inet address address/prefix-length
```

12. Configure the default route.

```
[edit]
admin@# set routing-options static route 0.0.0.0/0 next-hop gateway
```

13. Configure basic security zones and bind them to traffic interfaces.

```
[edit]
admin@# set security zones security-zone trust interfaces ge-6/3/5
admin@# set security zones security-zone untrust interfaces ge-6/2/0
```

14. Configure basic security policies.

```
[edit]
admin@# set security policies from-zone trust to-zone untrust policy policy-name match
source-address any destination-address any application any
root@# set security policies from-zone trust to-zone untrust policy policy-name then permit
```

15. Check the configuration for validity.

```
[edit]
admin@# commit check
configuration check succeeds
```

16. Commit the configuration to activate it on the device.

```
[edit]
admin@# commit
commit complete
```

17. Optionally, display the configuration to verify that it is correct.

```
admin@# show
## Last changed: 2008-05-07 22:43:25 UTC
version "9.2I0 [builder]";
system {
    autoinstallation;
    host-name henbert;
    root-authentication {
        encrypted-password "$1$oTVn2KY3$uQe4xzQCxpR2j7sKuV.Pa0"; ## SECRET-DATA
    }
    login {
        user admin {
            uid 928;
            class super-user;
            authentication {
                encrypted-password "$1$cdOPmACd$QvreBsJkNR1EF0uurTBkE."; ## SECRET-DATA
            }
        }
    }
    services {
        ssh;
       web-management {
            http {
                interface ge-0/0/0.0;
            }
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any any;
            authorization info;
        }
```

```
        file interactive-commands {
            interactive-commands any;
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0;
    }
    ge-6/2/0 {
        unit 0 {
            family inet {
                address 5.1.1.1/24;
            }
        }
    }
    ge-6/3/5 {
        unit 0 {
            family inet {
                address 192.1.1.1/24;
            }
        }
    }
    fxp0 {
        unit 0 {
            family inet {
                address 192.168.10.2/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 5.1.1.2;
    }
}
security {
    zones {
```

```
        security-zone trust {
            interfaces {
                ge-6/3/5.0;
            }
        }
        security-zone untrust {
            interfaces {
                ge-6/2/0.0;
            }
        }
    }
    policies {
        from-zone trust to-zone untrust {
            policy bob {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
}
```

18. Commit the configuration to activate it on the device.

```
[edit]
admin@# commit
```

19. Optionally, configure additional properties by adding the necessary configuration statements. Then commit the changes to activate them on the device.

```
[edit]
admin@# commit
```

20. When you have finished configuring the device, exit configuration mode.

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

Performing Initial Software Configuration Using J-Web

IN THIS SECTION

Configuring Root Authentication and the Management Interface from the CLI

Before you can use J-Web to configure your device, you must access the CLI to perform the initial configuration.

To configure root authentication and the management interface:

1. Log in as root. There is no password.
2. Start the CLI and enter configuration mode.

```
root@% cli
root@>configure
root@#
```

3. Set the root authentication password by entering a cleartext password, an encrypted password, or an SSH public key string (DSA or RSA).

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

4. Commit the configuration to activate it on the device.

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

5. Configure the IP address and prefix length for the Ethernet management interface on the device.

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

6. Configure the default route.

```
[edit]
root@# set routing-options static route 0.0.0.0/0 next-hop gateway
```

7. Enable Web access to launch J-Web.

```
[edit]
root@# set system services web-management http
```

8. Commit the configuration changes.

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

Configuring Interfaces, Zones, and Policies with J-Web

IN THIS SECTION

You can configure hostnames, interfaces, zones, and security policies using J-Web.

NOTE: You cannot use J-Web to configure SRX5400, SRX5600, and SRX5800 Firewalls in Junos OS Release 15.1X49-D10.

Before you begin:

- Ensure you have configured the IP address, root authentication, and default route. See "Performing Initial Software Configuration Using J-Web " on page 280
- Enable HTTP on the device to access J-Web. See "Performing Initial Software Configuration Using J-Web " on page 280

Configure the device with J-Web using the following procedures.

Configuring the Hostname

To configure the hostname:

1. Launch a Web browser from the management device.
2. Enter the IP address of the device in the URL address field.
3. Specify the default username as root and enter the password. See "Performing Initial Software Configuration Using J-Web " on page 280.
4. Click **Log In**. The J-Web Dashboard page appears.
5. Select **Configure>System Properties>System Identity**, and then select **Edit**. The Edit System Identity dialog box appears.
6. Enter the hostname and click **OK**.
7. Select **Commit Options>Commit** to apply the configuration changes.

You have successfully configured the hostname for the system.

Configuring Interfaces

To configure two physical interfaces:

1. From the J-Web Dashboard page, select **Configure>Interfaces** and select a physical interface you want to configure.
2. Select **Add>Logical Interface**. The Add interface dialog box appears.
3. Set **Unit** = **0**.
4. Select the check box for **IPv4 Address** to enable IPv4 addressing.
5. Click **Add** and enter the IPv4 address.
6. Click **OK**.

A message appears after your configuration changes are validated successfully.

7. Click **OK**.
8. Select **Commit Options>Commit** to apply the configuration changes.

   A message appears after your configuration changes are applied successfully.
9. Click **OK**.

You have successfully configured the physical interface. Repeat these steps to configure the second physical interface for the device.

Configuring Zones and Assigning Interfaces

To assign interfaces within a trust zone and an untrust zone:

1. From the J-Web Dashboard page, select **Configure>Security>Zones/Screens** and click **Add**. The Add Zone dialog box appears.
2. In the Main tab, enter **trust** for zone name and enter the description.
3. Set the zone type to **Security**.
4. Select the interfaces listed under Available and move them under Selected.
5. Click **OK**.

   A message appears after your configuration changes are validated successfully.
6. Click **OK**.
7. Select **Commit Options>Commit** to apply the configuration changes.

   A message appears after your configuration changes are applied successfully.
8. Click **OK**.
9. Repeat Step 1 through Step 8 and assign another interface to an untrust zone.

You have successfully configured interfaces in a trust zone and in an untrust zone.

Configuring Security Policies

To configure security policies:

1. From the J-Web Dashboard page, select **Configure>Security>Security Policy** and click **Add**. The Add Policy dialog box appears.
2. In the Policy tab, enter the policy name and set the policy action to **permit**. Then select **Zone** and set the From Zone to **trust** and the To Zone to **untrust**.
3. Configure the source IP address by selecting **any** listed under Available and moving it under Selected.
4. Configure the destination IP address by selecting **any** listed under Available and moving it under Selected.
5. Configure the application by selecting **any** listed under Available and moving it under Selected.

6. Click **OK**.

   A message appears after your configuration changes are validated successfully.
7. Click **OK**.
8. Select **Commit Options>Commit** to apply the configuration changes.

   A message appears after your configuration changes are applied successfully.
9. Click **OK**.

You have successfully configured the security policy.

4

CHAPTER

Maintaining Components

Maintaining the SRX5800 Chassis

IN THIS SECTION

Routine Maintenance Procedures for the SRX5800 Firewall

IN THIS SECTION

Purpose

For optimum firewall performance, perform preventive maintenance procedures regularly.

Action

- Inspect the installation site for moisture, loose wires or cables, and excessive dust. Make sure that airflow is unobstructed around the device and into the air intake vents.
- Check the status-reporting devices on the craft interface—System alarms and LEDs.
- Inspect the air filter at the bottom front of the firewall, replacing it every six months for optimum cooling system performance. Do not run the device for more than a few minutes without the air filter in place.

Replacing the SRX5800 Firewall Craft Interface

IN THIS SECTION

To replace the craft interface, perform the following procedures in sequence:

Disconnecting the Alarm Relay Wires from the SRX5800 Firewall Craft Interface

Before you begin disconnecting the alarm relay wires from the firewall and an alarm-reporting device:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

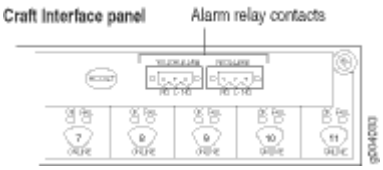
Ensure that you have the following available:

- ESD grounding strap
- 2.5-mm flat-blade screwdriver

To disconnect the alarm relay wires from the firewall and an alarm-reporting device (see Figure 1):

1. Disconnect the existing wire at the external device.
2. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
3. Using a 2.5-mm flat-blade screwdriver, loosen the small screws on the face of the terminal block and remove the block from the relay contact.
4. Using the 2.5-mm flat-blade screwdriver, loosen the small screws on the side of the terminal block. Remove existing wires from the slots in the front of the block.

Figure 128: Alarm Relay Contacts



Removing the SRX5800 Firewall Craft Interface

Before you begin removing the craft interface from the firewall:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

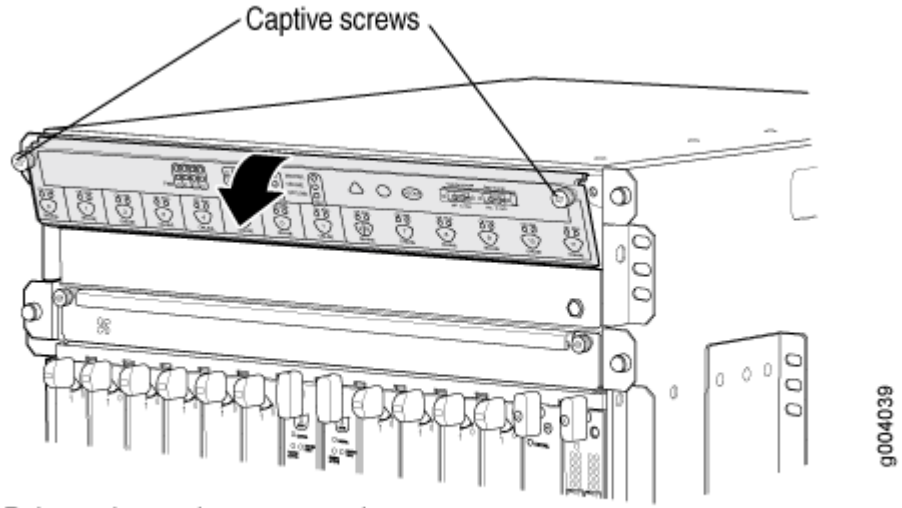
Ensure that you have the following available:

- ESD grounding strap
- Phillips (+) number 2 screwdriver

To remove the craft interface (see Figure 2):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Detach any external devices connected to the craft interface.
3. Using the Phillips (+) number 2 screwdriver loosen the captive screws at the left and right corners of the craft interface faceplate.
4. Grasp the craft interface faceplate and carefully tilt it toward you until it is horizontal.
5. Disconnect the ribbon cable from the back of the faceplate by gently pressing on both sides of the latch with your thumb and forefinger. Remove the craft interface from the chassis.

Figure 129: Removing the Craft Interface



Installing the SRX5800 Firewall Craft Interface

Before you begin installing the craft interface into the firewall:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

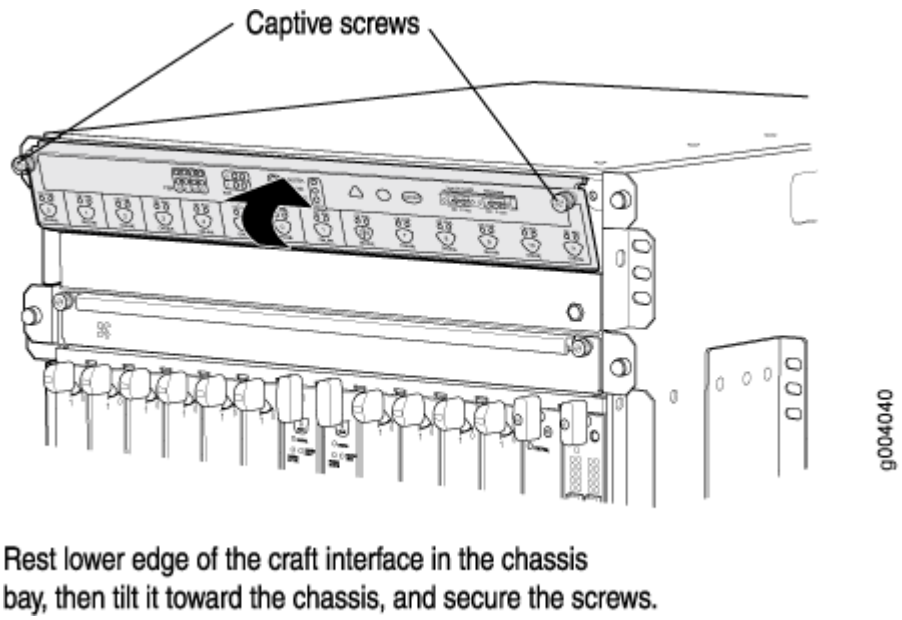
Ensure that you have the following available:

- ESD grounding strap
- Phillips (+) number 2 screwdriver

To install the craft interface (see Figure 3):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Grasp the craft interface with one hand and hold the bottom edge of the craft interface with the other hand to support its weight.
3. Orient the ribbon cable so that it plugs into the connector socket. The connector is keyed and can be inserted only one way.
4. Align the bottom of the craft interface with the sheet metal above the card cage and press it into place.
5. Using the Phillips (+) number 2 screwdriver tighten the screws on the left and right corners of the craft interface faceplate.
6. Reattach any external devices connected to the craft interface.

Figure 130: Installing the Craft Interface



Connecting the Alarm Relay Wires to the SRX5800 Firewall Craft Interface

Before you begin connecting the alarm relay wires to the firewall and an alarm-reporting device :

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

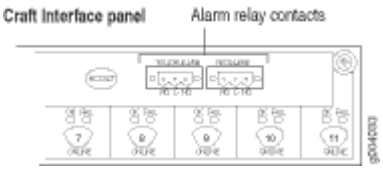
Ensure that you have the following available:

- ESD grounding strap
- 2.5-mm flat-blade screwdriver

To connect the alarm relay wires between a firewall and an alarm-reporting device (see Figure 4):

1. Prepare the required length of replacement wire with gauge between 28-AWG and 14-AWG (0.08 and 2.08 mm^2).
2. Insert the replacement wires into the slots in the front of the block. Use a 2.5-mm flat-blade screwdriver to tighten the screws and secure the wire.
3. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
4. Plug the terminal block into the relay contact, and use a 2.5-mm flat-blade screwdriver to tighten the screws on the face of the block.
5. Attach the other end of the wires to the external device.

Figure 131: Alarm Relay Contacts



Maintaining the SRX5800 Cooling System

IN THIS SECTION

Maintaining the Fan Trays on the SRX5800 Firewall

IN THIS SECTION

Purpose

For optimum cooling, verify the condition of the fans.

Action

- Monitor the status of the fans. A fan tray contains multiple fans that work in unison to cool the firewall components. If one fan fails, the host subsystem adjusts the speed of the remaining fans to maintain proper cooling. A major alarm is triggered when a fan fails, and a minor alarm and major alarm is triggered when a fan tray is removed.
- To display the status of the cooling system, issue the `show chassis environment` command.

```
user@host> show chassis environment
```

NOTE: In the Junos OS command-line interface (CLI):

- The `show chassis environment` command output displays the fan trays as `Upper Fan Tray` and `Bottom Fan Tray`.
- The `show chassis hardware` command output displays the fan trays as `Fan Tray 0` for the upper fan tray and `Fan Tray 1` for the bottom fan tray.

NOTE: The fan numbers are stamped into the fan tray sheet metal next to each fan.

Replacing an SRX5800 Firewall Fan Tray

IN THIS SECTION

The fan trays are hot-insertable and hot-removable. To replace a fan tray, perform the following procedures in sequence:

Removing an SRX5800 Firewall Fan Tray

Before you begin to remove the fan tray:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Phillips (+) number 2 screwdriver

NOTE: To prevent overheating, install the replacement fan tray immediately after removing the existing fan tray. Do not operate the firewall for more than two minutes without both fan trays installed.

To remove the upper or bottom fan tray (see Figure 1 and Figure 2):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Reposition the cable manager before removing the bottom front fan tray:
   a. Unwrap any cables on the cable manager and remove the cables from the tray. Arrange the cables so that they do not block the front of the cable manager and tray, and secure them with temporary fasteners so that they are not supporting their own weight as they hang from the connector.
   b. Simultaneously pull the two releases labeled PULL on the cable manager. Lift it up and outward to lock it in place.
3. Using the Phillips (+) number 2 screwdriver loosen the captive screw on each side of the fan tray faceplate.
4. Grasp both sides of the fan tray and pull it out approximately 1 to 3 inches.

   WARNING: To prevent injury, keep tools and your fingers away from the fans as you slide the fan module out of the device. The fans might still be spinning.

5. Pause for approximately 15 seconds to allow the fans to stop spinning.
6. When the fans stop spinning, press on the two latches located on the inside of the fan tray.
7. Place one hand under the fan tray to support it and pull the fan tray completely out of the chassis.
8. Proceed to "Installing an SRX5800 Firewall Fan Tray" on page 292 to install the replacement fan tray.

Figure 132: Removing an Upper Fan Tray (Standard-Capacity Shown, High-Capacity Similar)

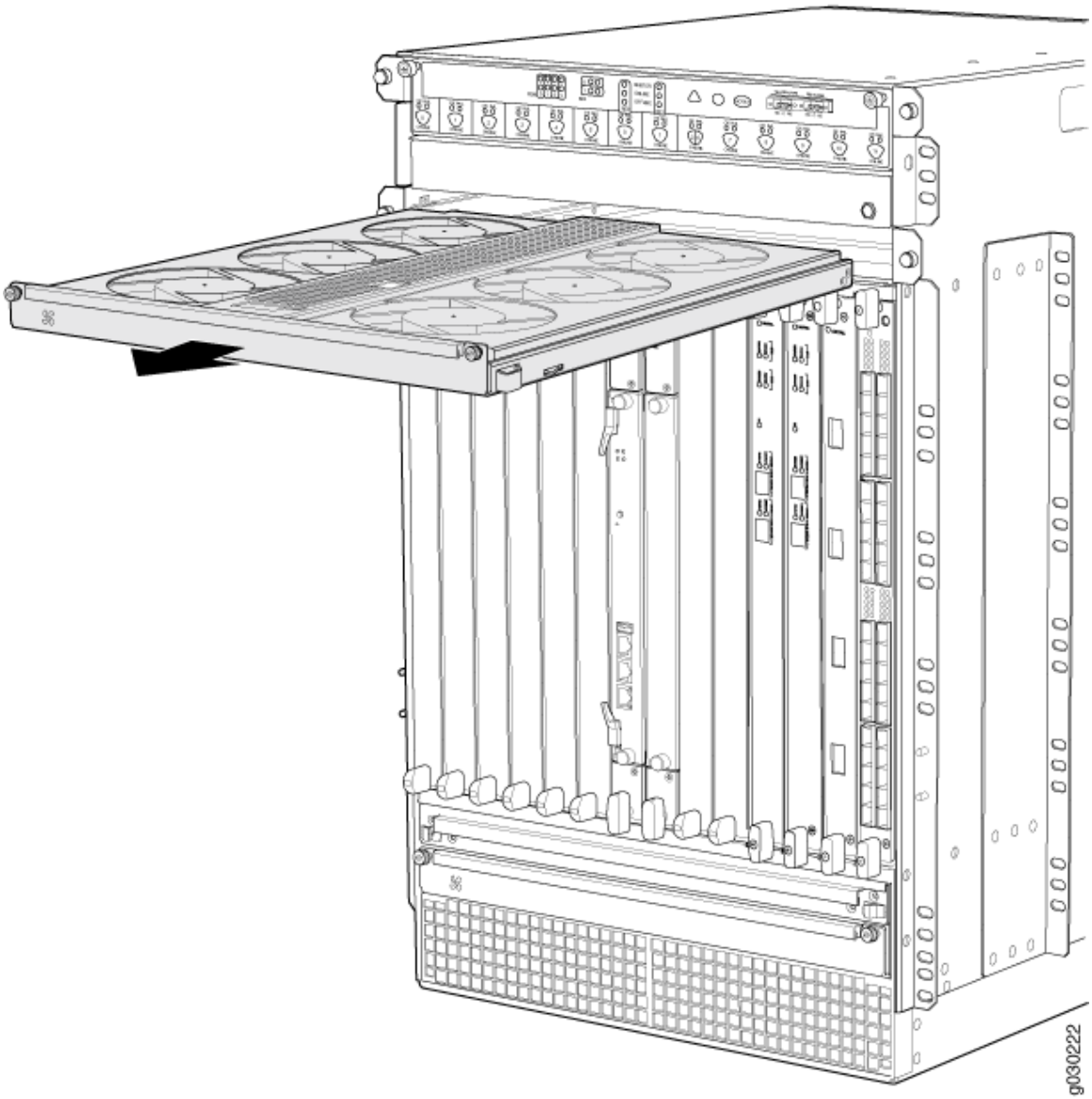
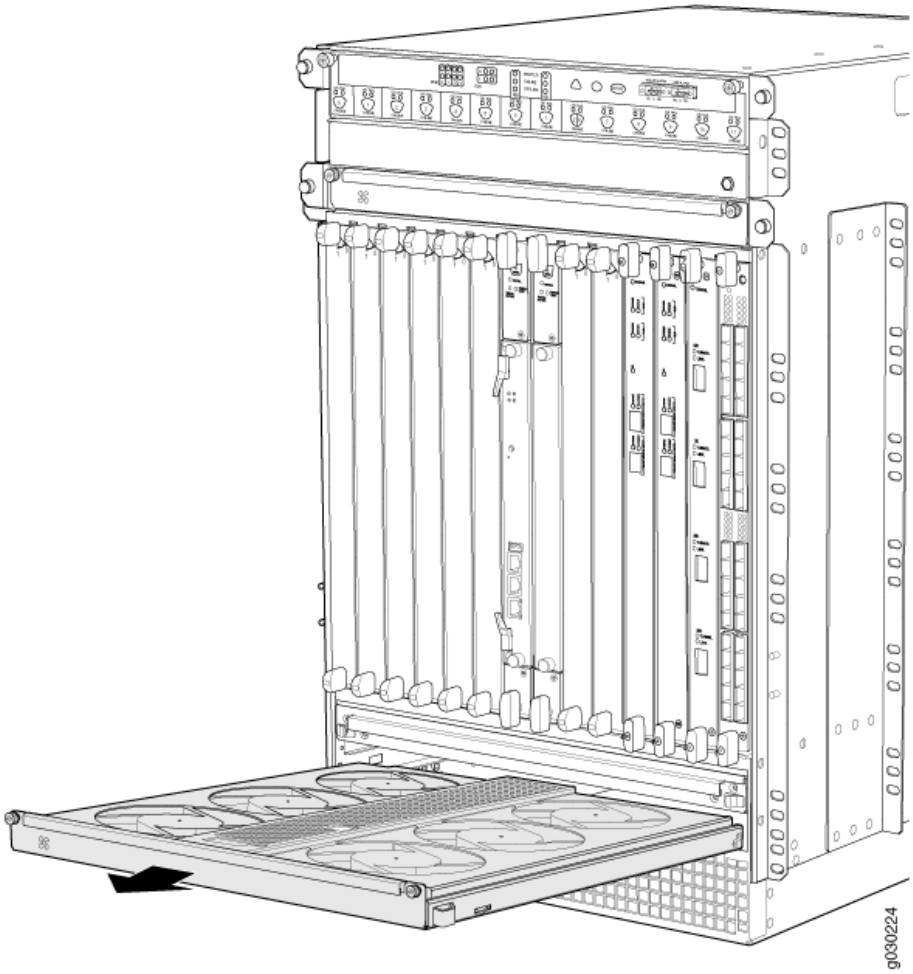


Figure 133: Removing the Bottom Fan Tray (Standard-Capacity Shown, High-Capacity Similar)



Installing an SRX5800 Firewall Fan Tray

Before you begin to install the fan tray:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Phillips (+) number 2 screwdriver

NOTE: To prevent overheating, install the replacement fan tray immediately after removing the existing fan tray. Do not operate the firewall for more than two minutes without both fan trays installed.

To install a fan tray (see Figure 3 and Figure 4):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Grasp the fan tray on each side and insert it straight into the chassis. Note the correct orientation by the "this side up" label on the top surface of the fan tray.
3. Using the Phillips (+) number 2 screwdriver tighten the captive screws on each side of the fan tray faceplate to secure it in the chassis.
4. Lower the cable manager back into position, if necessary.

Figure 134: Installing an Upper Fan Tray (Standard-Capacity Shown, High-Capacity Similar)

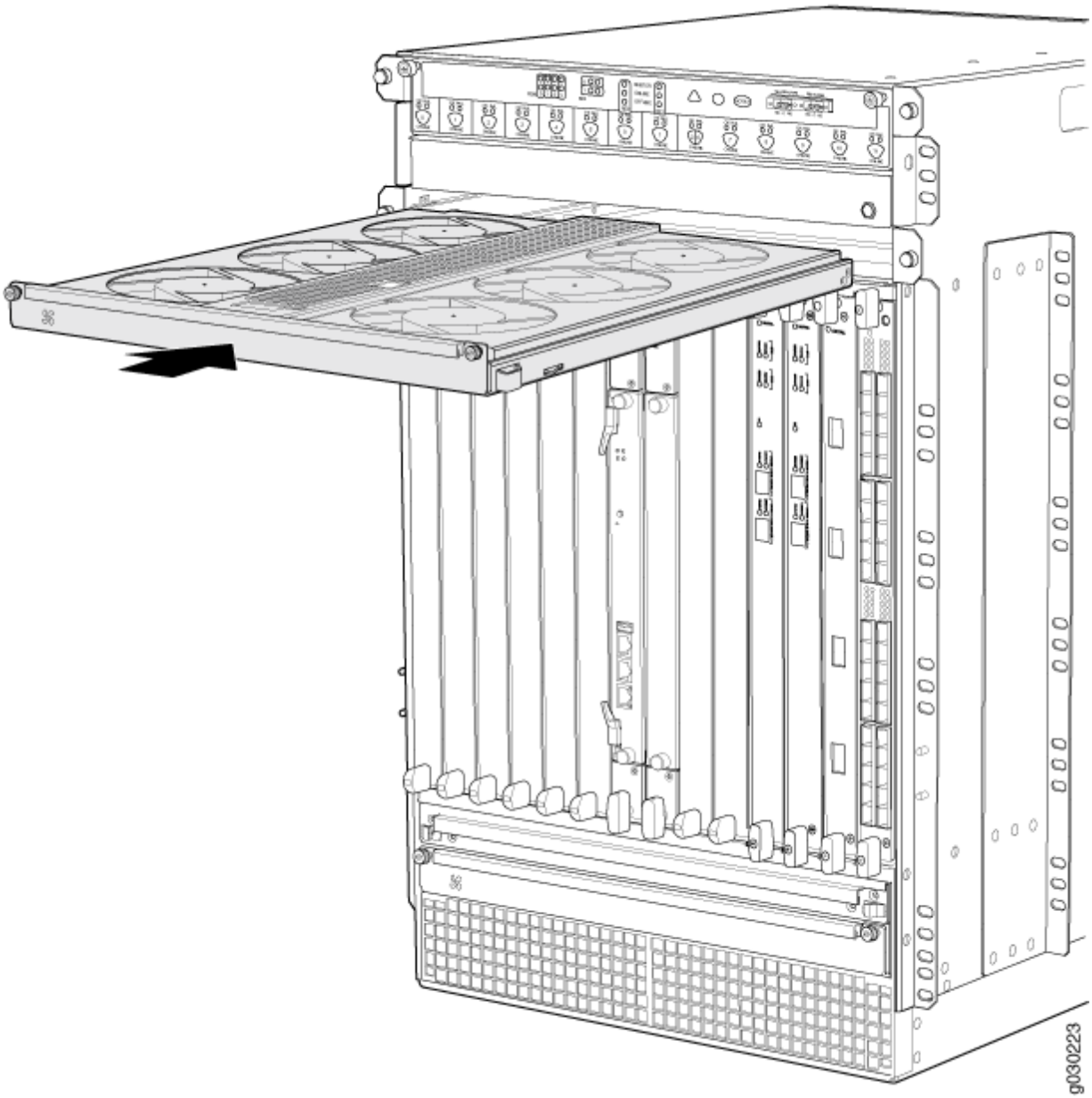
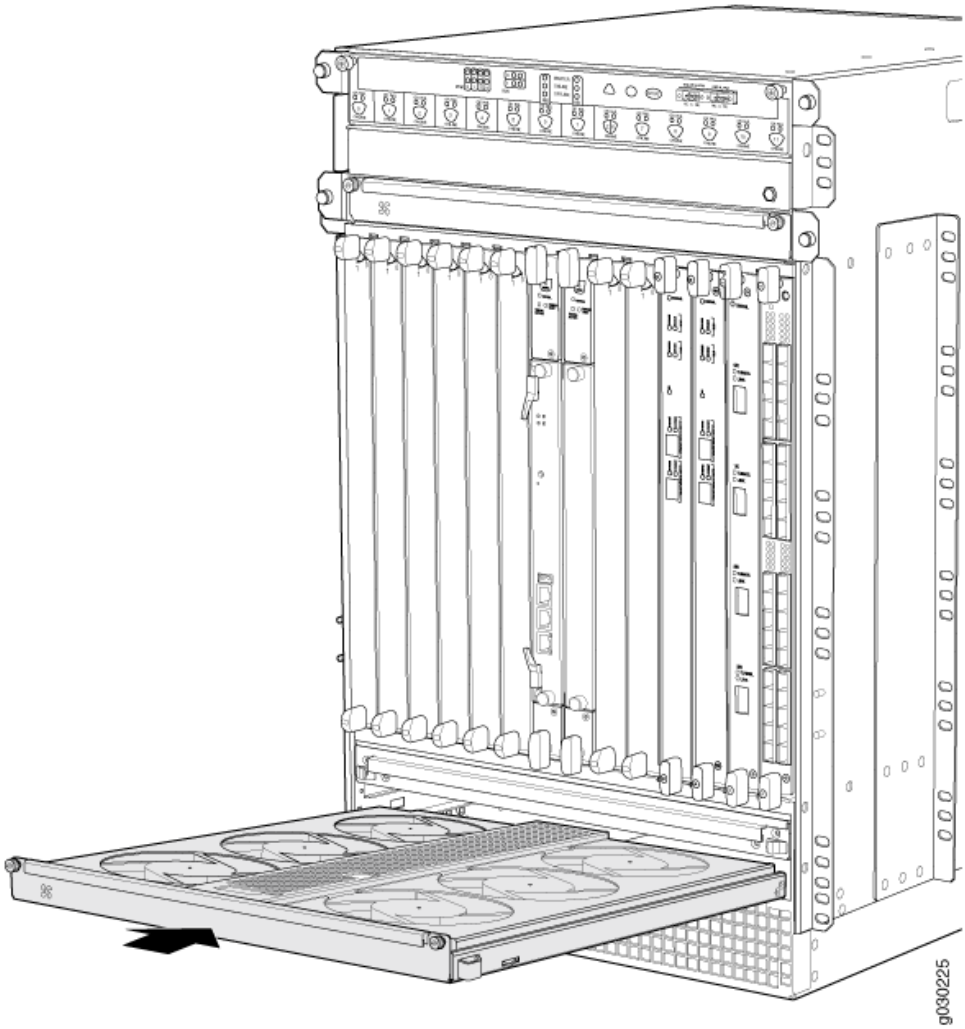


Figure 135: Installing the Bottom Fan Tray (Standard-Capacity Shown, High-Capacity Similar)



Maintaining the Air Filter on the SRX5800 Firewall

IN THIS SECTION

Purpose

For optimum cooling, verify the condition of the air filters.

Action

- Regularly inspect the air filter. A dirty air filter restricts airflow in the unit, impeding the ventilation of the chassis. The filter degrades over time. Periodically replace the filter in use, as well as spares. We recommend that you replace the filter every six months. Discard used filters, do not attempt to clean and reuse them.

  NOTE: Air filters will not be replaced by Juniper Networks under the Juniper Networks Hardware Replacement Support Plan, you need to purchase them for replacement.

  CAUTION: Always keep the air filter in place while the firewall is operating. Because the fans are very powerful, they could pull small bits of wire or other materials into the firewall through the unfiltered air intake. This could damage the firewall components.

- The shelf life of polyurethane filter varies from two years to five years depending on the storage conditions. Store in a cool, dry, and dark environment. Wrap the media in plastic and store in an environment with relative humidity between 40%- 80% and temperature between 40°F (4° C) to 90°F (32° C). Note that if the material flakes, or becomes brittle when rubbed or deformed, it is no longer usable.

Replacing the SRX5800 Firewall Air Filter

IN THIS SECTION

You should change the air filter every six months. To replace the air filter, perform the following procedures in sequence:

Removing the SRX5800 Firewall Air Filter

Before you begin to remove the air filter:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap

> ⚠ **CAUTION**: Do not run the firewall for more than two minutes without the air filter in place.

> ⚠ **CAUTION**: Always keep the air filter in place while the firewall is operating, except during replacement. Because the fans are very powerful, they could pull small bits of wire or other materials into the firewall through the unfiltered air intake. This could damage the firewall components.

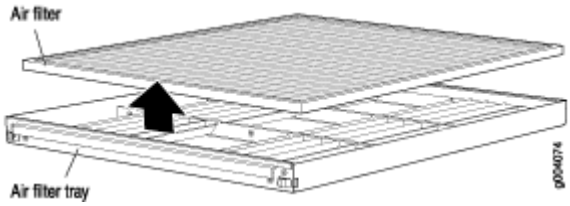
To remove the air filter (see Figure 5):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Unwrap any cables on the cable manager and remove the cables from the tray. Arrange the cables so that they do not block the front of the cable manager and tray, and secure them with temporary fasteners so that they are not supporting their own weight as they hang from the connector.

   > ⚠ **CAUTION**: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

3. Simultaneously pull the two releases labeled **PULL** on the cable manager. Lift it up and outward to lock it in place to access the air filter.
4. Slide the air filter tray out of the chassis.
5. Lift the air filter out of the air filter tray.

Figure 136: Removing the Air Filter (Standard-Capacity Filter Tray Shown, High-Capacity Similar)



Installing the SRX5800 Firewall Air Filter

Before you begin to install the air filter:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

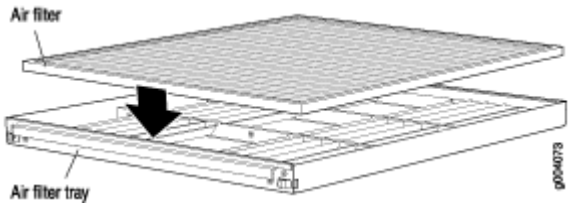
- ESD grounding strap

You should change the air filter every six months.

To install the air filter (see Figure 6):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Ensure the air filter is right side up.
3. Place the air filter into the air filter tray.
4. Insert the air filter tray into the chassis by sliding it straight into the chassis until it stops.
5. Lower the cable manager back into position.
6. Rearrange the cables in the cable manager.

Figure 137: Installing the Air Filter Standard-Capacity Filter Tray Shown, High-Capacity Similar)



Maintaining the SRX5800 Power System

IN THIS SECTION

Maintaining SRX5800 Firewall Power Supplies

IN THIS SECTION

Purpose

For optimum firewall performance, verify the condition of the power supplies.

Action

On a regular basis:

- To check the status of the power supplies, issue the `show chassis environment pem` command. The output is similar to the following:

```
user@host> show chassis environment pem
PEM 0 status:
  State                     Online
  Temperature               OK
  AC Input:                 OK
  DC Output             Voltage   Current       Power    Load
                          50        6             300      17
PEM 1 status:
  State                     Online
  Temperature               OK
  AC Input:                 OK
  DC Output             Voltage   Current       Power    Load
                          50        3             150      8
```

- Make sure that the power and grounding cables are arranged so that they do not obstruct access to other firewall components.
- Routinely check the status LEDs on the power supply faceplates and the craft interface to determine if the power supplies are functioning normally.
- Check the red and yellow alarm LEDs on the craft interface. Power supply failure or removal triggers an alarm that causes one or both of the LEDs to light. You can display the associated error messages by issuing the following command:

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

- Periodically inspect the site to ensure that the grounding and power cables connected to the device are securely in place and that there is no moisture accumulating near the device.

Replacing an SRX5800 Firewall AC Power Supply or High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supply

IN THIS SECTION

To replace an AC or High-Voltage Second-Generation Universal (HVAC/HVDC) power supply, perform the following procedures:

Removing an SRX5800 Firewall AC Power Supply or High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supply

Before you remove a power supply, be aware of the following:

NOTE: The minimum number of power supplies must be present in the firewall at all times.

⚠ **CAUTION**: To maintain proper cooling and prevent thermal shutdown of the operating power supply unit, each power supply slot must contain either a power supply or a blank panel. If you remove a power supply, you must install a replacement power supply or a blank panel shortly after the removal.

NOTE: After powering off a power supply, wait at least 60 seconds before turning it back on.

Before you begin to remove the AC power supply:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

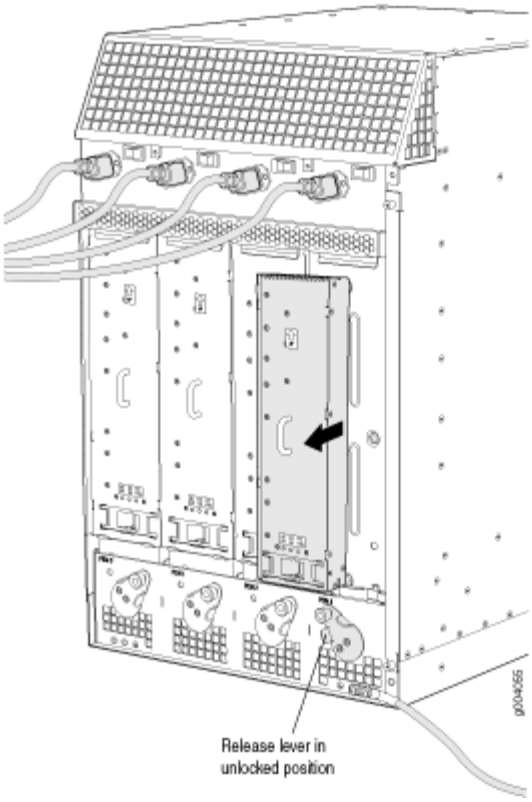
Ensure that you have the following available:

- ESD grounding strap

To remove an AC power supply (see Figure 1):

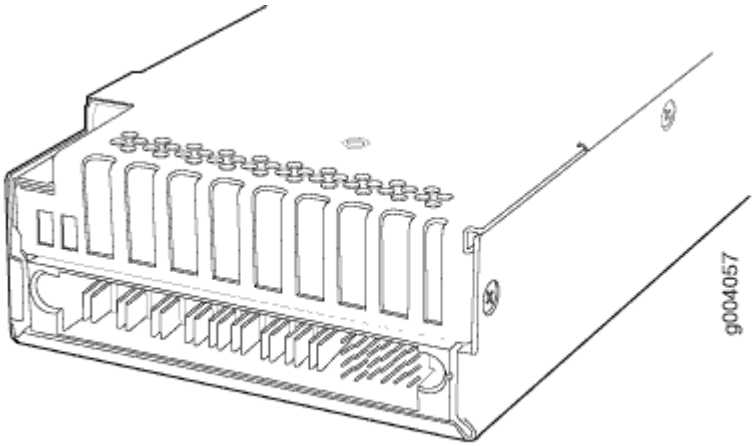
1. Switch off the dedicated customer site circuit breaker for the power supply, and remove the power cord from the AC power source. If the firewall is equipped with high-capacity AC power supplies, remove both of the power cords for the power supply. Follow the ESD and disconnection instructions for your site.
2. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
3. Move the AC input switch on the chassis above the AC power supply to the off (**O**) position. If the firewall is equipped with high-capacity AC power supplies you must also move the AC input switch on the power supply itself to the off (**O**) position.
4. While grasping the handle on the power supply faceplate with one hand, use your other hand to pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever counterclockwise until it stops.
5. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
6. Pull the power supply straight out of the chassis. The power supply can weigh up to 12 lb (5.5 kg). Be prepared to accept its full weight.

Figure 138: Removing an AC Power Supply (Standard-Capacity Shown, High-Capacity Similar)



WARNING: Do not touch the power connector on the top of the power supply (see Figure 2). It can contain dangerous voltages.

Figure 139: Top of the Power Supply Showing Midplane Connector



Connector end of AC or DC power supply

Figure 140: Removing a High-Capacity Second-Generation AC Power Supply

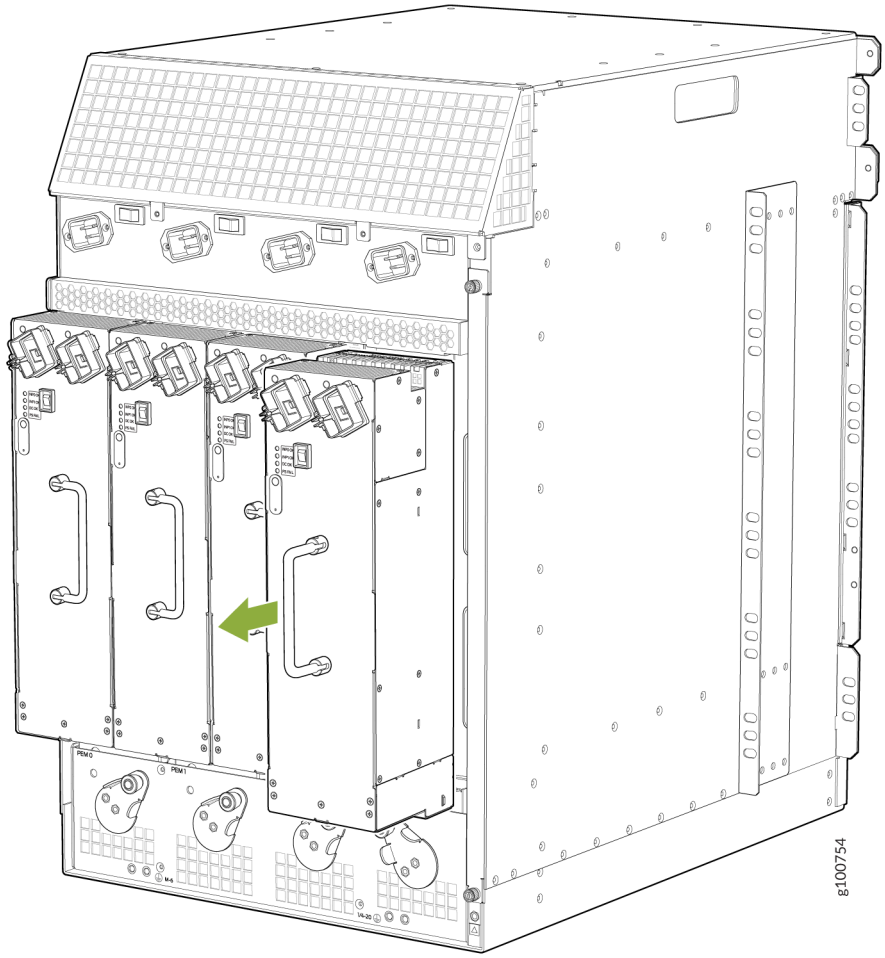
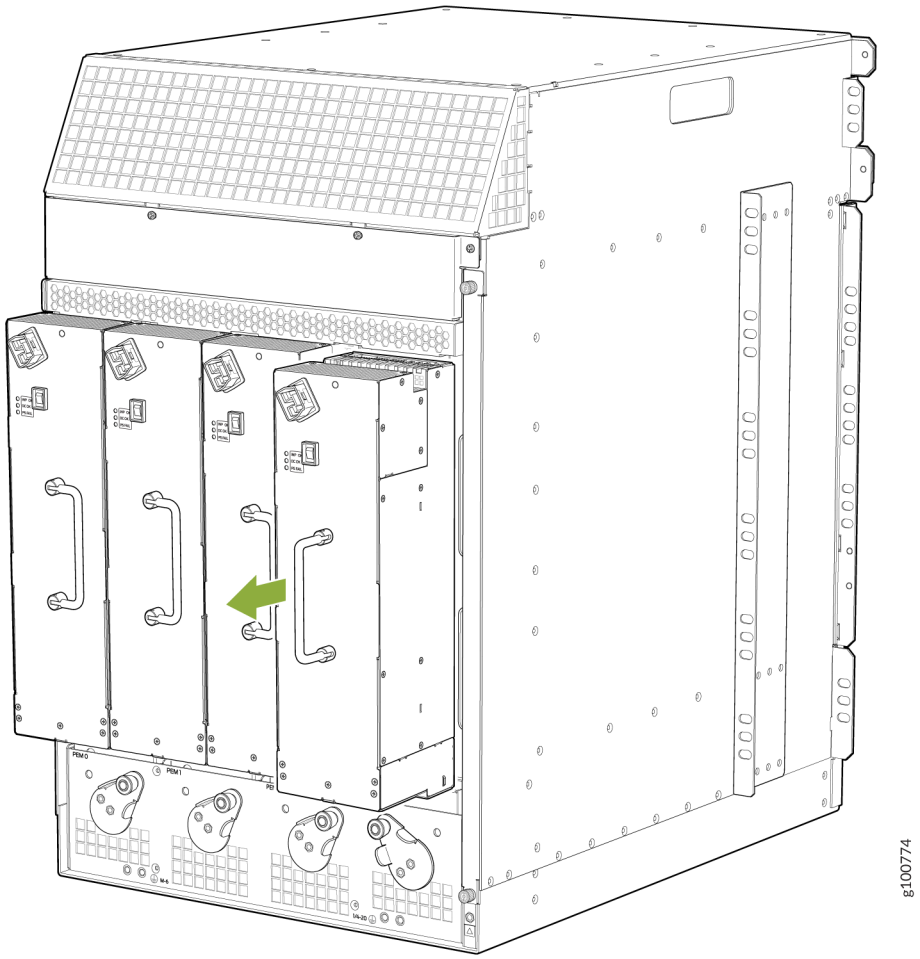


Figure 141: Removing a High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supply



Installing an SRX5800 Firewall AC Power Supply or High-Voltage Second-Generation Universal (HVAC or HVDC) Power Supply

Before you begin to install an AC high-voltage second-generation universal (HVAC/HVDC) power supply:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap

To install an AC the high-voltage second-generation universal (HVAC/HVDC) power supply:

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. If you have not already done so, move the AC input switch in the chassis above the empty power supply slot to the off (**O**) position.
3. For each high-capacity or high-capacity second-generation AC power supply, move the input mode switch to position **0** for one feed or position **1** for two feeds (see Figure 5). We recommend that you use two AC power feeds and set the mode input switch to **1**.

Figure 142: High-Capacity AC Power Supply Input Mode Switch

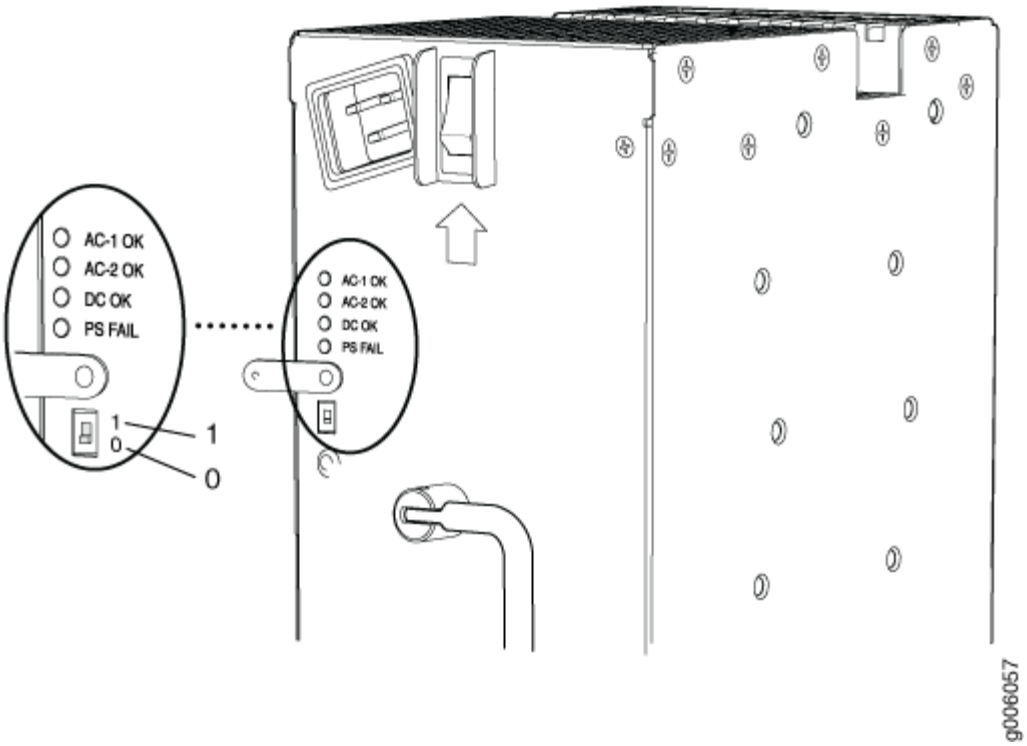
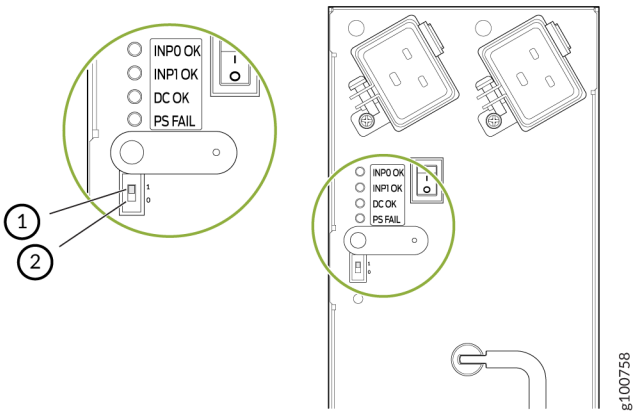


Figure 143: High-Capacity Second-Generation AC Power Supply Input Mode Switch



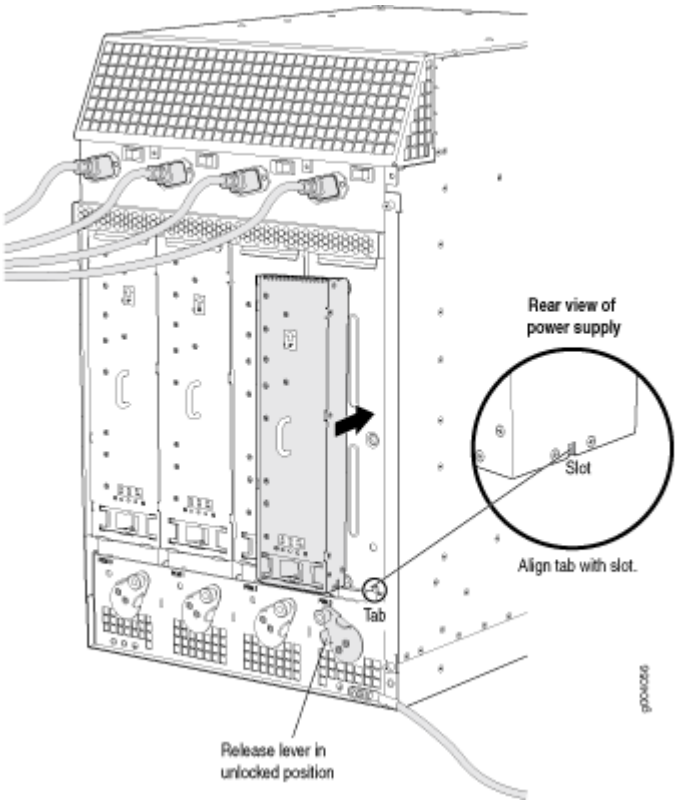
NOTE: Do not use a pencil to set the mode switch, because fragments can break off and cause damage to the power supply.

4. If you are installing a high-capacity, or high-capacity second-generation AC, or high-voltage second-generation universal (HVAC or HVDC) power supply, move the AC input switch on the faceplate of the power supply itself to the off (**O**) position.
5. Ensure that the release lever below the empty power supply slot is locked in the counterclockwise position (see Figure 7).

   If necessary, pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever counterclockwise until it stops. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
6. Using both hands, slide the power supply straight into the chassis until the power supply is fully seated in the chassis slot. The power supply faceplate should be flush with any adjacent power supply faceplates.

   The small tab on the metal housing that is controlled by the release lever must be inside of the corresponding slot at the bottom of the power supply (see Figure 7). This tab is used to pull the power supply down in the chassis slot, prior to removing the power supply.

Figure 144: Installing an AC Power Supply (Standard-Capacity Shown, High-Capacity Similar)



7. While firmly pushing the handle on the power supply faceplate with one hand, use your other hand to pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever clockwise until it stops.

Figure 145: Installing a High-Capacity Second-Generation AC Power Supply

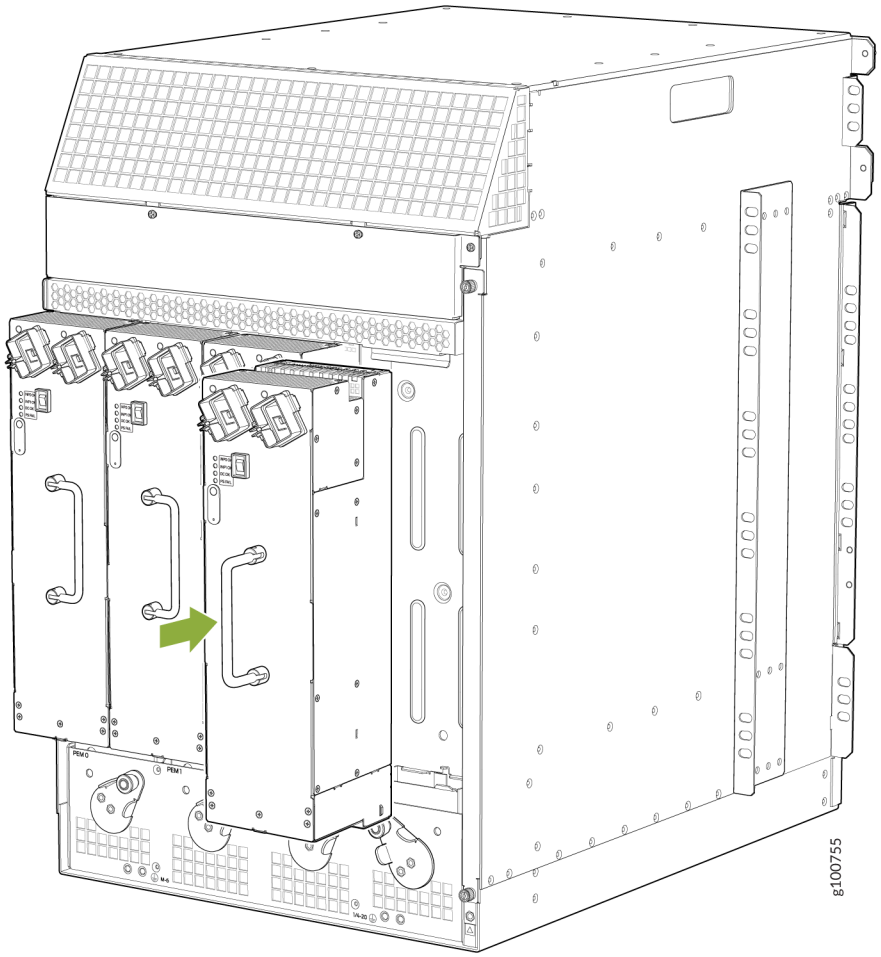
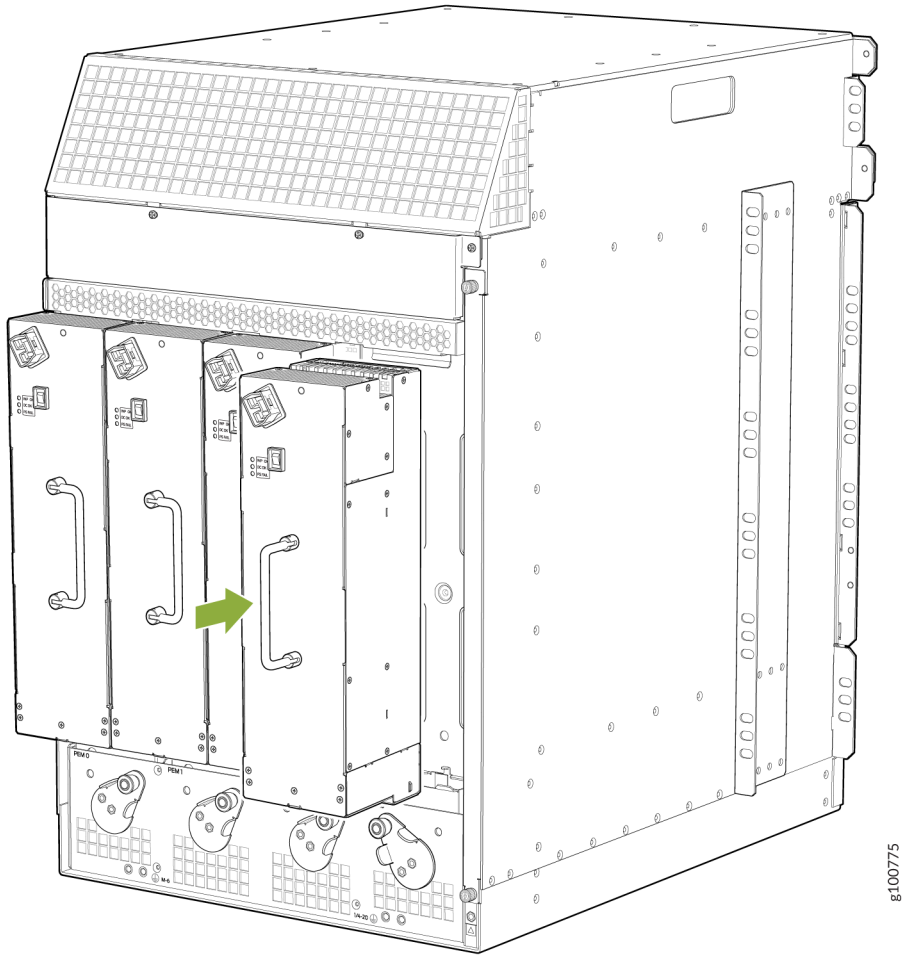


Figure 146: Installing a High-Voltage Second-Generation Universal (HVAC or HVDC) Power Supply



8. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
9. If you are installing a high-capacity power supply, connect a power cord to the appliance inlet at the top edge of the power supply. For more information, see "Connecting an SRX5800 Firewall AC Power Supply Cord" on page 314.
10. Move the AC input switch in the chassis above the power supply to the on (—) position.
11. If you are installing a high-capacity, or high-capacity second-generation AC, or high-voltage second-generation universal (HVAC or HVDC) power supply, move the AC input switch on the faceplate of the power supply itself to the on (**1**) position.
12. Verify the following LED indications for each installed power supply:
    - For standard-capacity AC power supplies, verify that the **AC OK** and **DC OK** LEDs light steadily and the **PS FAIL** LED is not lit.

- For high-capacity AC power supplies, verify that the **DC OK** LED lights steadily and the **PS FAIL** LED is not lit. In addition, the **AC-1 OK** LED should light green steadily if the upper AC feed (on the chassis above the power supply) is connected and receiving power, and the **AC-2 OK** LED should light green steadily if the lower AC feed (on the power supply itself) is connected and receiving power.
- For high-capacity second-generation AC power supplies, verify that the **DC OK** LED lights steadily and the **PS FAIL** LED is not lit. In addition, the **IN-1 OK** LED should light green steadily if the upper AC feed (on the chassis above the power supply) is connected and receiving power, and the **IN-2 OK** LED should light green steadily if the lower AC feed (on the power supply itself) is connected and receiving power.
- For high-voltage second-generation universal (HVAC/HVDC) AC power supplies, verify that the **INP OK** and **DC OK** LEDs light steadily and the **PS FAIL** LED is not lit.

> **NOTE**: After a power supply is powered on, it can take up to 60 seconds for status indicators—such as the status LEDs on the power supply and the **show chassis** command display—to indicate that the power supply is functioning normally. Ignore error indicators that appear during the first 60 seconds.

If any of the status LEDs indicates that the power supply is not functioning normally, repeat the installation and cabling procedures.

Replacing an SRX5800 Firewall AC Power Supply Cord

IN THIS SECTION

To replace an SRX5800 Firewall AC power supply cord, perform the following procedures:

Disconnecting an SRX5800 Firewall AC Power Supply Cord

Before you begin to disconnect an AC power supply cord:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap

To disconnect an AC power cord:

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Move the AC input switch nearest to the appliance inlet for the power cord you are replacing to the off (**O**) position:
   - For standard-capacity AC power supplies, there is only one AC input switch for each power supply; it is located next to the appliance inlet on the chassis above the power supply.
   - For high-capacity AC power supplies, there is one AC input switch for each of the two appliance inlets. One is located next to the AC inlet on the chassis above the power supply, and the other is located next to the appliance inlet on the power supply itself.
3. Unplug the power cord from the power source receptacle.
4. Unplug the power cord from the appliance inlet on the chassis or power supply.

Connecting an SRX5800 Firewall AC Power Supply Cord

Before you begin to connect an AC power supply cord:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap

NOTE: Power cords are not supplied with the firewall. You must order the power cords separately.

To connect an AC power cord:

1. Locate a replacement power cord with the type of plug appropriate for your geographical location.
2. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
3. Verify that the AC input switch nearest to the appliance inlet for the power cord you are replacing is in the off (**O**) position:

- For standard-capacity AC power supplies, there is only one AC input switch for each power supply; it is located next to the appliance inlet on the chassis above the power supply.
- For high-capacity AC power supplies, there is one AC input switch for each of the two appliance inlets. One switch is located next to the AC inlet on the chassis above the power supply, and the other is located next to the appliance inlet on the power supply itself.

4. Plug the replacement power cord into the corresponding appliance inlet.
5. Insert the power cord plug into an external AC power source receptacle.

> **NOTE**: Each power supply must be connected to a dedicated AC power feed and a dedicated customer site circuit breaker. We recommend that you use a 15 A (250 VAC) minimum, or as required by local code.

6. Dress the power cord appropriately. Verify that the power cord does not block the air exhaust and access to firewall components, or drape where people could trip on it.
7. Move the AC input switch nearest to the appliance inlet for the power cord you are replacing to the on (|) position:
   - For standard-capacity AC power supplies, there is only one AC input switch for each power supply; it is located next to the appliance inlet on the chassis above the power supply.
   - For high-capacity AC power supplies, there is one AC input switch for each of the two appliance inlets. One is located next to the AC inlet on the chassis above the power supply, and the other is located next to the appliance inlet on the power supply itself.
8. Verify the following LED indications for the power supply for which you replaced the power cord:
   - For standard-capacity AC power supplies, verify that the **AC OK** and **DC OK** LEDs light steadily and the **PS FAIL** LED is not lit.
   - For high-capacity AC power supplies, verify that the **DC OK** LED lights steadily and the **PS FAIL** LED is not lit. In addition, the **AC-1 OK** LED should light green steadily if the upper AC feed (on the chassis above the power supply) is connected and receiving power, and the **AC-2 OK** LED should light green steadily if the lower AC feed (on the power supply itself) is connected and receiving power.

   If any of the status LEDs indicates that the power supply is not functioning normally, repeat the installation and cabling procedures.

Replacing an SRX5800 Firewall DC Power Supply

IN THIS SECTION

To replace a DC power supply, perform the following procedures:

Removing an SRX5800 Firewall DC Power Supply

Before you remove a power supply, be aware of the following:

NOTE: The minimum number of power supplies must be present in the firewall at all times.

WARNING: Before you perform DC power procedures, ensure there is no power to the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the off position, and tape the switch handle of the circuit breaker in the off position.

CAUTION: To maintain proper cooling and prevent thermal shutdown of the operating power supply unit, each power supply slot must contain either a power supply or a blank panel. If you remove a power supply, you must install a replacement power supply or a blank panel shortly after the removal.

NOTE: After powering off a power supply, wait at least 60 seconds before turning it back on.

Before you begin to remove a DC power supply:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

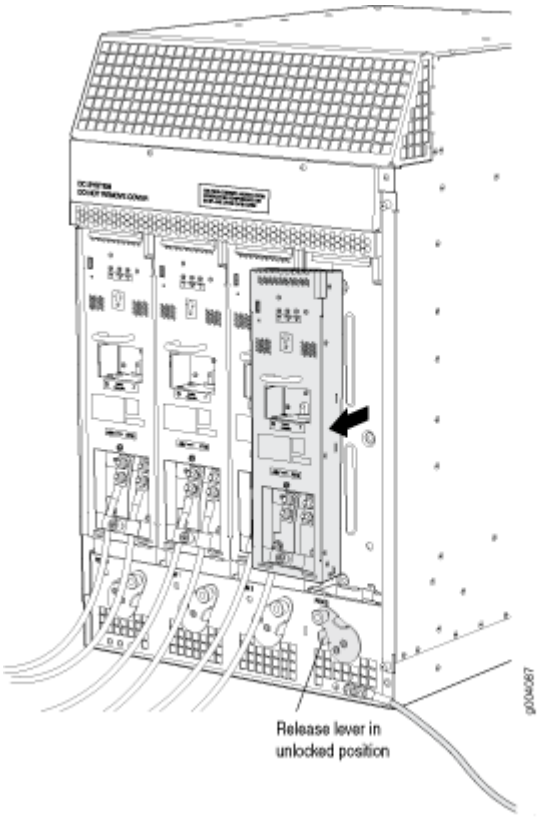
- ESD grounding strap

- 7/16–in. nut driver or socket wrench

To remove a DC power supply (see Figure 10):

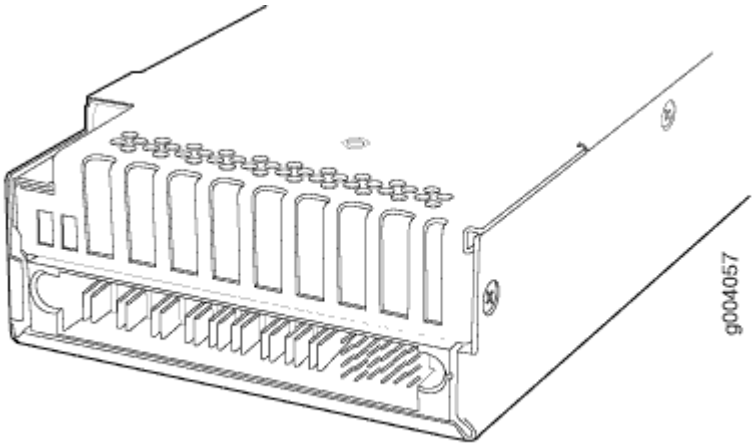
1. Switch off the dedicated customer site circuit breaker for the power supply being removed. Follow your site's procedures for ESD.
2. Make sure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cables might become active during the removal process. If the firewall is equipped with high-capacity DC power supplies, check both pairs of DC leads to make sure that the voltage is 0 V.
3. Verify that the **INPUT OK** LEDs on the power supply to be removed are not lit.
4. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
5. Move the DC circuit breaker on the power supply faceplate to the off (**O**) position.
6. Remove the clear plastic cover protecting the terminal studs on the faceplate.
7. Remove the nuts and washers from the terminal studs. (Use a 7/16-in. nut driver or socket wrench.)
8. Remove the cable lugs from the terminal studs.
9. Loosen the captive screw on the cable restraint on the lower edge of the power supply faceplate.
10. Carefully move the power cables out of the way.
11. While grasping the handle on the power supply faceplate with one hand, use your other hand to pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever counterclockwise until it stops.
12. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
13. Pull the power supply straight out of the chassis. The power supply can weigh up to 12 lb (5.5 kg). Be prepared to accept its full weight.

Figure 147: Removing a DC Power Supply from the Firewall (Standard-Capacity Shown, High-Capacity Similar)



WARNING: Do not touch the power connector on the top of the power supply (see Figure 11). It can contain dangerous voltages.

Figure 148: Top of the Power Supply Showing Midplane Connector



Installing an SRX5800 Firewall DC Power Supply

Before you begin to install a DC power supply:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- 7/16–in. nut driver or socket wrench

WARNING: Before you perform DC power procedures, ensure there is no power to the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the off position, and tape the switch handle of the circuit breaker in the off position.

To install a DC power supply (see Figure 12):

1. Verify that the power switch on the power supply is in the off (**O**) position.
2. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
3. Move the switch or circuit breaker on the power supply faceplate to the off (**O**) position.
4. For a high-capacity DC power supply, configure the power supply for the number of DC feeds:
   a. Rotate the metal cover away from the input mode switch to expose the switch.
   b. Move the input mode switch to position **0** for one feed or position **1** for two feeds.

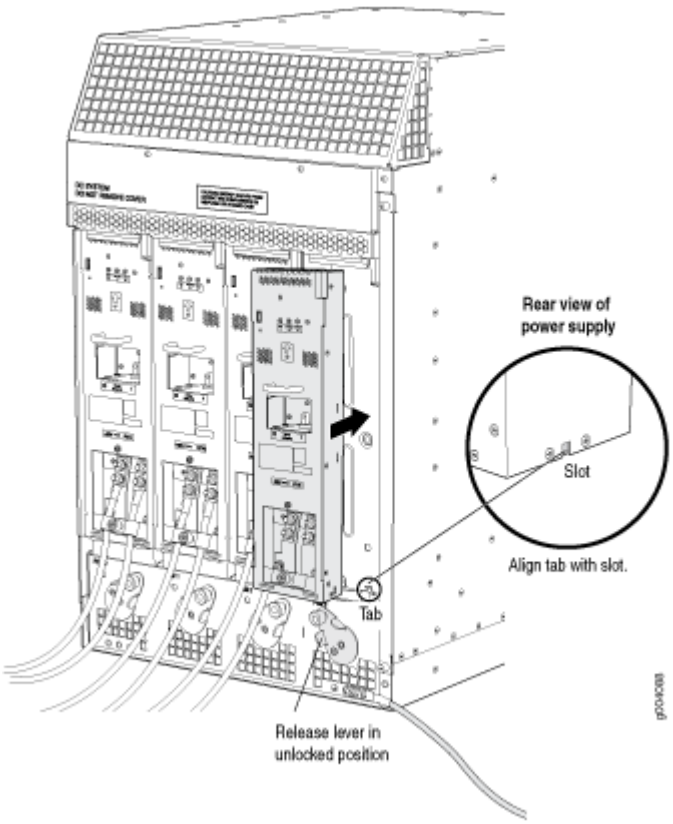
NOTE: The high-capacity DC power supply will operate with only one of its two DC inputs connected to a power feed. However, its DC output will be limited to a maximum of 1700 W. We recommend that you connect two DC power feeds to each high-capacity DC power supply.

5. Ensure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cable leads might become active during installation.
6. Ensure that the release lever below the empty power supply slot is locked in the counterclockwise position (see Figure 12).

   If necessary, pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever counterclockwise until it stops. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
7. Using both hands, slide the power supply straight into the chassis until the power supply is fully seated in the chassis slot.

   The small tab on the metal housing that is controlled by the release lever must be inside of the corresponding slot at the bottom of the power supply (see Figure 12). This tab is used to pull the power supply down in the chassis slot, prior to removing the power supply.

Figure 149: Installing a DC Power Supply (Standard Capacity Shown, High-Capacity Similar)



8. While firmly pushing the handle on the power supply faceplate with one hand, use your other hand to pull the spring-loaded locking pin in the release lever away from the chassis and turn the release lever clockwise until it stops.
9. Let go of the locking pin in the release lever. Ensure that the pin is seated inside the corresponding hole in the chassis.
10. Remove the clear plastic cover protecting the terminal studs on the faceplate.
11. Remove the nuts and washers from the terminal studs.
12. Secure each power cable lug to the terminal studs, first with the split washer, then with the nut.

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

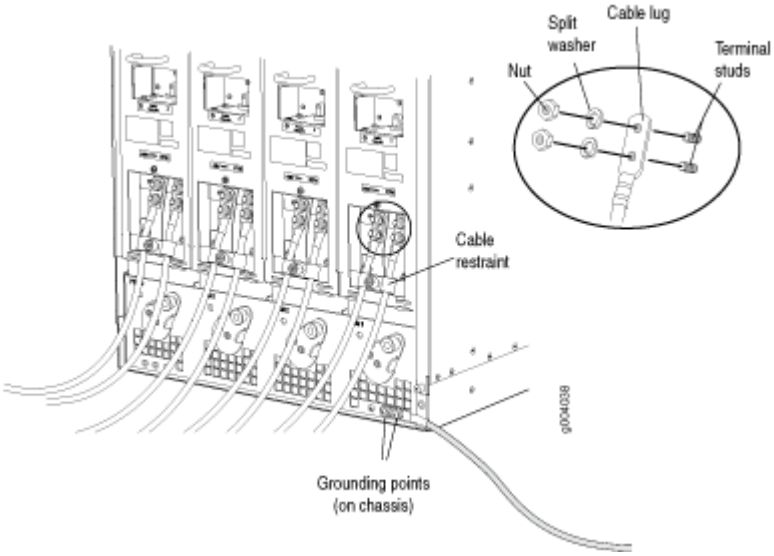
For a standard-capacity power supply:

a. Attach the positive (+) DC source power cable lug to the **RTN** (return) terminal.

b. Attach the negative (–) DC source power cable lug to the **–48V** (input) terminal.

c. Apply between 23 lb-in. (2.6 Nm) and 25 lb-in. (2.8 Nm) of torque to each nut (see Figure 13).

Figure 150: Connecting DC Power to a Standard-Capacity DC Power Supply



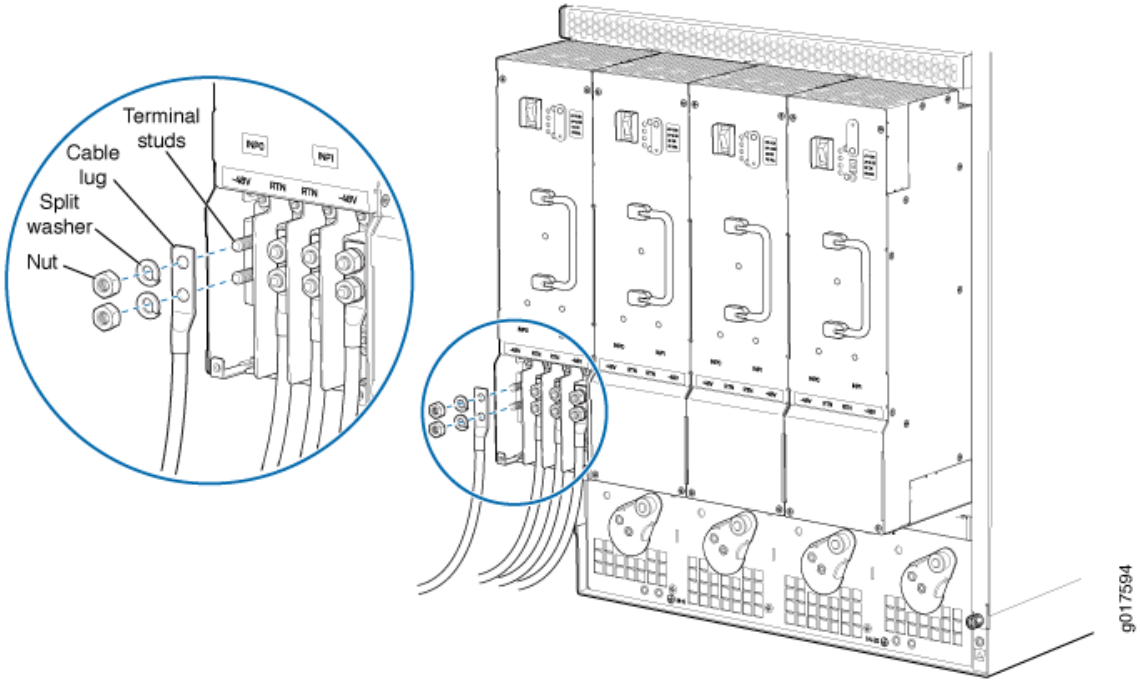
For a high-capacity power supply:

a. On **INP0**, attach the positive (+) DC source power cable lug to the **RTN** (return) terminal. Repeat this step for **INP1** if using two feeds.

b. On **INP0** attach the negative (–) DC source power cable lug to the –48V (input) terminal. Repeat this step for **INP1** if using two feeds.

c. Apply between 23 lb-in. (2.6 Nm) and 25 lb-in. (2.8 Nm) of torque to each nut (see Figure 14).

Figure 151: Connecting DC Power to a High-Capacity DC Power Supply



CAUTION: Ensure that each power cable lug seats flush against the surface of the terminal block as you are tightening the nuts. Ensure that each nut is properly threaded onto the terminal stud. The nut should be able to spin freely with your fingers when it is first placed onto the terminal stud. Applying installation torque to the nut when improperly threaded may result in damage to the terminal stud.

CAUTION: The maximum torque rating of the terminal studs on the DC power supply is 36 in-lb. (4.0 Nm). The terminal studs may be damaged if excessive torque is applied. Use only a torque-controlled driver or socket wrench to tighten nuts on the DC power supply terminal studs.

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 **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.

13. For standard-capacity DC power supplies, secure each DC power cable to its strain relief bracket as follows:

    a. Loosen the captive screw on the cable restraint on the lower edge of the power supply faceplate.

    b. Route the positive and negative DC power cables through the left and right sides of the cable restraint.

    c. Tighten the cable restraint captive screw to hold the power cables in place.

14. Replace the clear plastic cover over the terminal studs on the faceplate.
15. Verify that the power cabling is correct, that the cables are not touching, and that they do not block access to firewall components or drape where people could trip on them.
16. Switch on the dedicated customer site circuit breaker.
17. Verify that the input LEDs on the power supply indicate that the DC power is connected properly:

    - For a standard-capacity power supply, verify that the **INPUT OK** LED on the power supply is lit steadily.

    - For a high-capacity power supply, verify that the **INP0 OK** or **INP1 OK** LEDs on the power supply are lit green steadily. If using two feeds, verify that both **INP0 OK** and **INP1 OK** LEDs on the power supply are lit steadily

    NOTE: An input LED will be lit amber if that input's voltage is in reverse polarity. Check the polarity of the power cables to fix the condition

18. Move the switch or circuit breaker on the DC power supply to the on (|) position .
19. Verify that the output LEDs on the power supply indicate that it is operating properly:

    - For a standard-capacity power supply, verify that the **BREAKER ON** and **PWR OK** LEDs are lit steadily.

    - For a high-capacity power supply, verify that the **DC OK** LED is lit, and that the **PS FAIL** LED is not lit.

Replacing an SRX5800 Firewall DC Power Supply Cable

IN THIS SECTION

To replace an SRX5800 Firewall DC power supply cable, perform the following procedures:

Disconnecting an SRX5800 Firewall DC Power Supply Cable

Before you begin to disconnect a DC power supply cable:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- 7/16–in. nut driver or socket wrench

WARNING: Before you perform DC power procedures, ensure there is no power to the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the off position, and tape the switch handle of the circuit breaker in the off position.

To disconnect a power cable for a DC power supply:

1. Switch off the dedicated customer site circuit breaker for the power supply being removed. Follow your site's procedures for ESD.
2. Make sure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cables might become active during the removal process.
3. Verify that the input LEDs on the power supply are not lit (**INPUT OK** for a standard-capacity power supply, **INP0 OK** and **INP1 OK** for a high-capacity power supply).
4. Remove the power cable from the external DC power source.
5. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
6. Move the DC circuit breaker on the power supply faceplate to the off (**O**) position.
7. Remove the clear plastic cover protecting the terminal studs on the faceplate.
8. Remove the nut and washer from the terminal studs. (Use a 7/16–in. nut driver or socket wrench.)
9. Remove the cable lug from the terminal studs.
10. For a standard-capacity power supply, loosen the captive screw on the cable restraint on the lower edge of the power supply faceplate.

11. Carefully move the power cable out of the way.

Connecting an SRX5800 Firewall DC Power Supply Cable

Before you begin to connect a DC power supply cable:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- 7/16–in. nut driver or socket wrench

WARNING: Before you perform DC power procedures, ensure there is no power to the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the off position, and tape the switch handle of the circuit breaker in the off position.

To connect a power cable for a DC power supply:

1. Locate a replacement power cable that meets the specifications defined in "DC Power Cable Specifications for the SRX5800 Firewall" on page 64.
2. Verify that a licensed electrician has attached a cable lug to the replacement power cable.
3. Verify that the input LEDs on the power supply are not lit (**INPUT OK** for a standard-capacity power supply, **INP0 OK** and **INP1 OK** for a high-capacity power supply).
4. Secure the power cable lug to the terminal studs, first with the split washer, then with the nut. Apply between 23 lb-in. (2.6 Nm) and 25 lb-in. (2.8 Nm) of torque to each nut (see Figure 15 and Figure 16).

Figure 152: Connecting Power Cables to a Standard Capacity DC Power Supply

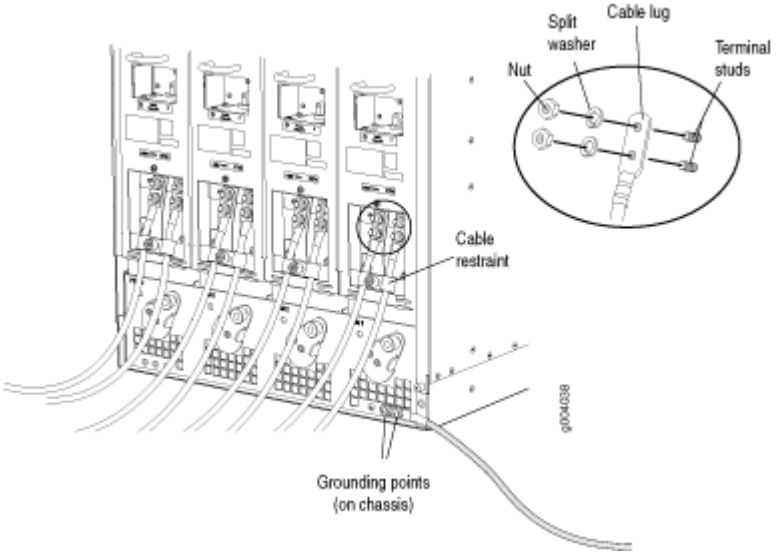
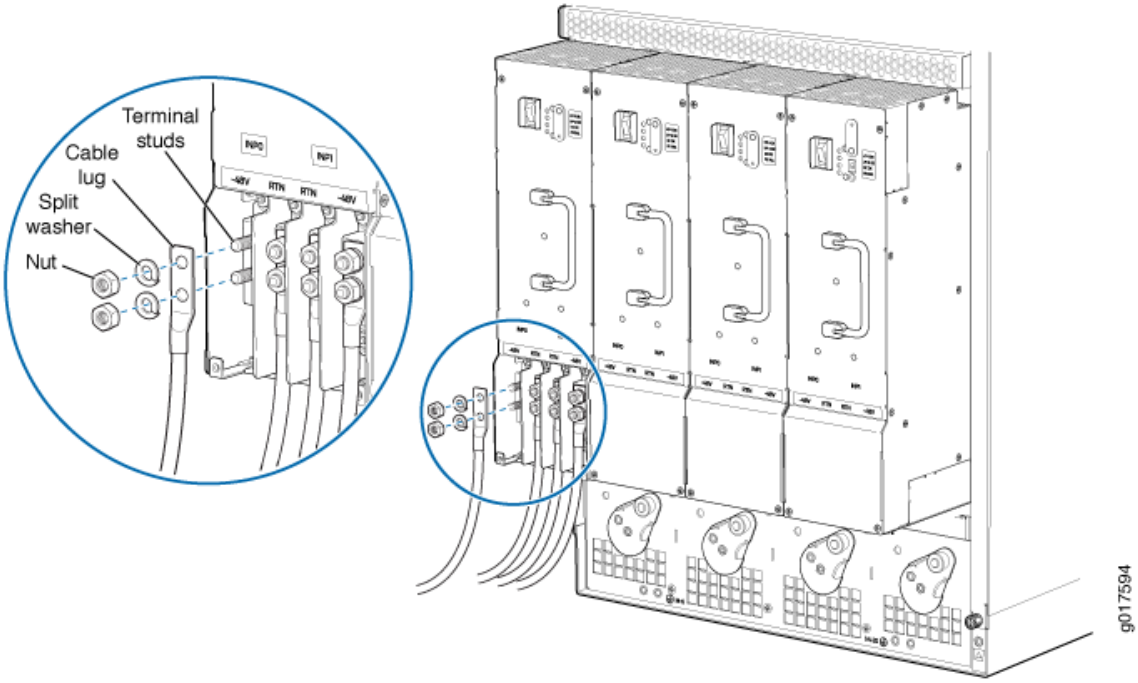


Figure 153: Connecting DC Power Cables to a High-Capacity DC Power Supply



5. For standard-capacity DC power supplies, secure each DC power cable to its strain relief bracket as follows:

   a. Loosen the captive screw on the cable restraint on the lower edge of the power supply faceplate.

b. Route the positive and negative DC power cables through the left and right sides of the cable restraint.

c. Tighten the cable restraint captive screw to hold the power cables in place.

6. Verify that the DC power cable is connected correctly, that it does not touch or block access to firewall components, and that it does not drape where people could trip on it.
7. Replace the clear plastic cover over the terminal studs on the faceplate.
8. Attach the power cable to the DC power source.
9. Turn on the dedicated customer site circuit breaker to the power supply.
10. Verify that the input LEDs on the power supply are lit (**INPUT OK** for a standard-capacity power supply, **INP0 OK** and **INP1 OK** for a high-capacity power supply).
11. Move the DC circuit breaker on the power supply to the on (|) position and verify that the output LEDs on the power supply indicate that it is operating properly:
    - For a standard-capacity power supply, verify that the **BREAKER ON** and **PWR OK** LEDs are lit steadily.
    - For a high-capacity power supply, verify that the **DC OK** LED is lit, and that the **PS FAIL** LED is not lit.

Upgrading an SRX5800 Firewall from Standard-Capacity to High-Capacity Power Supplies

You can replace the standard-capacity power supplies in the SRX5800 Firewall with either two or four high-capacity power supplies of the same input type (AC or DC). Two high-capacity power supplies provide adequate power for a fully loaded chassis; installing four high-capacity power supplies provides redundancy in case one power supply in either zone fails. You do not need to power off the device to upgrade to high-capacity power supplies.

NOTE: The firewall cannot be powered from standard-capacity and high-capacity power supplies simultaneously. The one exception is during the process of replacing standard-capacity power supplies with high-capacity power supplies, when it is permissible to have both types installed briefly.

CAUTION: The firewall cannot be powered from AC and DC power supplies simultaneously. The first type of power supply detected by the firewall when initially powered on determines the type of power supply allowed by the firewall. All installed

power supplies of the other type are disabled by the firewall. If you install a power supply of the other type while the firewall is operating, the firewall disables the power supply and generates an alarm.

The following procedures describe how to upgrade from standard-capacity power supplies to high-capacity power supplies of the same input type (AC or DC) without interrupting power to the firewall components. Choose the procedure that matches your firewall configuration:

To upgrade a firewall that has three or four standard-capacity AC power supplies to two or four high-capacity AC power supplies:

CAUTION: Limit to five minutes or less the time during which standard-capacity AC power supplies and high-capacity AC power supplies are installed in the firewall at the same time.

1. Ensure that the firewall is running Junos OS Release 10.4 or later. Earlier Junos OS releases do not support high-capacity AC power supplies.
2. If you have not already done so, replace both standard-capacity fan trays with high-capacity fan trays. Also replace the standard-capacity air filter with a high-capacity air filter. For more information, see "Replacing an SRX5800 Firewall Fan Tray" on page 292 and "Replacing the SRX5800 Firewall Air Filter" on page 299.
3. Check the LEDs on all of the installed power supply faceplates to ensure that they are operating properly.
4. If there are four standard-capacity AC power supplies installed, remove the standard-capacity AC power supply installed in the **PEM0** slot. See "Removing an SRX5800 Firewall AC Power Supply" on page 304 for instructions on removing AC power supplies. If there are only three standard-capacity AC power supplies installed in the firewall, proceed to the next step.
5. Install a high-capacity AC power supply in the vacant slot in the back of the chassis. See "Installing an SRX5800 Firewall AC Power Supply" on page 304 for instructions on installing AC power supplies.
6. Check the LEDs on the high-capacity AC power supply faceplate to ensure that it is operating properly.
7. Identify the slot for the next high-capacity AC power supply:
   - If the slot you installed the power supply into in 5 is **PEM0** or **PEM2**, install the next high-capacity AC power supply in either slot **PEM1** or **PEM3**
   - If the slot you installed the power supply into in 5 is **PEM1** or **PEM3**, install the next high-capacity AC power supply in either slot **PEM0** or **PEM2**

8. Remove the standard-capacity AC power supply from the slot you identified in step7. See "Removing an SRX5800 Firewall AC Power Supply" on page 304 for instructions on removing AC power supplies.
9. Install a high-capacity AC power supply in the slot you identified in Step 7. See "Installing an SRX5800 Firewall AC Power Supply" on page 304 for instructions on installing AC power supplies.
10. Check the LEDs on both high-capacity AC power supply faceplates to ensure that they are operating properly.
11. Remove the remaining two standard-capacity AC power supply from the firewall. See "Removing an SRX5800 Firewall AC Power Supply" on page 304 for instructions on removing AC power supplies.
12. If you are upgrading to four high-capacity AC power supplies to achieve 2+2 redundancy, install high-capacity AC power supplies in the slots you vacated in Step 11. See "Installing an SRX5800 Firewall AC Power Supply" on page 304 for instructions on installing AC power supplies.
13. Check the LEDs on all installed high-capacity AC power supply faceplates to ensure that they are operating properly.

To upgrade a firewall that has two standard-capacity DC power supplies to two or four high-capacity DC power supplies:

1. Ensure that the Firewall is running Junos OS Release 12.1X44-D10 or later. Earlier Junos OS releases do not support high-capacity DC power supplies.
2. If you have not already done so, replace both standard-capacity fan trays with high-capacity fan trays. Also replace the standard-capacity air filter with a high-capacity air filter. For more information, see "Replacing an SRX5800 Firewall Fan Tray" on page 292 and "Replacing the SRX5800 Firewall Air Filter" on page 299.
3. Install high-capacity DC power supplies in the two empty PEM slots in the back of the chassis. See "Installing an SRX5800 Firewall DC Power Supply" on page 317 for instructions on installing DC power supplies.
4. Check the LEDs on the faceplate of each of the new power supplies to confirm that they are operating properly.
5. Remove both of the standard-capacity power supplies from the firewall. See "Removing an SRX5800 Firewall DC Power Supply" on page 317 for instructions on removing DC power supplies.
6. If you are installing four high-capacity DC power supply to achieve 2+2 redundancy, install high-capacity DC power supplies in the slots vacated in Step "5" on page 331.
7. Check the LEDs on the faceplate of each of the new power supplies to confirm that they are operating properly.

To upgrade a firewall that has four standard-capacity DC power supplies to two or four high-capacity DC power supplies:

1. Ensure that the firewall is running Junos OS Release 12.1X44-D10 or later. Earlier Junos OS releases do not support high-capacity DC power supplies.
2. If you have not already done so, replace both standard-capacity fan trays with high-capacity fan trays. Also replace the standard-capacity air filter with a high-capacity air filter. For more information, see "Replacing an SRX5800 Firewall Fan Tray" on page 292 and "Replacing the SRX5800 Firewall Air Filter" on page 299.
3. Check the LEDs on all four power supply faceplates to ensure that they are operating properly.
4. Remove the standard-capacity power supply from slot **PEM0**. See "Removing an SRX5800 Firewall DC Power Supply" on page 317 for instructions on removing DC power supplies.
5. Install a high-capacity DC power supply in the **PEM0** slot in the back of the chassis. See "Installing an SRX5800 Firewall DC Power Supply" on page 317 for instructions on installing DC power supplies.
6. Repeat Step "4" on page 332 and Step "5" on page 332 to replace the standard-capacity DC power supply in the **PEM1** slot with a high-capacity DC power supply.
7. Check the LEDs on the faceplate of each of the new power supplies to confirm that they are operating properly.
8. Remove the two standard-capacity power supplies from the **PEM2** and **PEM3** slots. See "Removing an SRX5800 Firewall DC Power Supply" on page 317 for instructions on removing DC power supplies.
9. If you are upgrading to four high-capacity DC power supplies to achieve 2+2 redundancy, install high-capacity DC power supplies in the **PEM2** and **PEM3** slots. See "Installing an SRX5800 Firewall DC Power Supply" on page 317 for instructions on installing DC power supplies.
10. Check the LEDs on the faceplate of each of the new power supplies to confirm that they are operating properly.

Maintaining the SRX5800 Host Subsystem

IN THIS SECTION

Maintaining the SRX5800 Firewall Host Subsystem and SCBs

IN THIS SECTION

Purpose

For optimum Firewall performance, verify the condition of the host subsystem and any additional SCBs. The host subsystem comprises an SCB and a Routing Engine installed into a slot in the SCB.

Action

On a regular basis:

- Check the LEDs on the craft interface to view information about the status of the Routing Engines.
- Check the LEDs on the SCB faceplate.
- Check the LEDs on the Routing Engine faceplate.
- To check the status of the Routing Engine, issue the `show chassis routing-engine` command. The output is similar to the following:

```
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             33 degrees C / 91 degrees F
    DRAM                      2048 MB
    Memory utilization          12 percent
    CPU utilization:
      User                       1 percent
      Background                 0 percent
      Kernel                     4 percent
      Interrupt                  0 percent
      Idle                      94 percent
    Model                        RE-S-1300
    Serial ID                    1000697084
    Start time                   2008-07-11 08:31:44 PDT
    Uptime                       3 hours, 27 minutes, 27 seconds
    Load averages:               1 minute   5 minute  15 minute
                                     0.44       0.16       0.06
```

- To check the status of the SCB, issue the `show chassis environment cb` command. The output is similar to the following:

```
user@host> show chassis environment cb

CB 0 status:
  State                      Online Master
  Temperature                40 degrees C / 104 degrees F
  Power 1
    1.2 V                     1208 mV
    1.5 V                     1521 mV
    1.8 V                     1807 mV
    2.5 V                     2507 mV
    3.3 V                     3319 mV
    5.0 V                     5033 mV
    12.0 V                   12142 mV
    1.25 V                    1243 mV
    3.3 V SM3                 3312 mV
    5 V RE                    5059 mV
    12 V RE                  11968 mV
  Power 2
```

```
    11.3 V bias PEM          11253 mV
    4.6 V bias MidPlane       4814 mV
    11.3 V bias FPD          11234 mV
    11.3 V bias POE 0        11176 mV
    11.3 V bias POE 1        11292 mV
  Bus Revision               42
  FPGA Revision              1
```

To check the status of a specific SCB, issue the `show chassis environment cb node slot` command, for example, `show chassis environment cb node 0`.

For more information about using the CLI, see the CLI Explorer.

Taking the SRX5800 Firewall Host Subsystem Offline

The host subsystem is composed of an SCB with a Routing Engine installed in it. You take the host subsystem offline and bring it online as a unit. Before you replace an SCB or a Routing Engine, you must take the host subsystem offline. Taking the host subsystem offline causes the device to shut down.

To take the host subsystem offline:

1. On the console or other management device connected to the Routing Engine that is paired with the SCB 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
   ```

2. Wait until a message appears on the console confirming that the operating system has halted.

   For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

   NOTE: The SCB might continue forwarding traffic for approximately 5 minutes after the `request system halt` command has been issued.

Operating and Positioning the SRX5800 Firewall SCB Ejectors

- When removing or inserting an SCB, ensure that the SCBs or blank panels in adjacent slots are fully inserted to avoid hitting them with the ejector handles. The ejector handles require that all adjacent components be completely inserted so the ejector handles do not hit them, which could result in damage.
- The ejector handles have a center of rotation and need to be stored toward the center of the board. Ensure the long ends of the ejectors located at both the top and the bottom of the board are vertical and pressed as far as possible toward the center of the board. Once you have installed an SCB, place the ejector handles in their proper position, vertically and toward the center of the board. To avoid blocking the visibility of the LEDs,position the ejectors over the PARK icon.
- To insert or remove the SCB card, slide the ejector across the SCB horizontally, rotate it, and slide it again another quarter of a turn. Turn the ejector again and repeat as necessary. Use the indexing feature to maximize leverage and to avoid hitting any adjacent components.
- Operate both ejector handles simultaneously. The insertion force on an SCB is too great for one ejector.

Replacing an SRX5800 Firewall SCB

IN THIS SECTION

Before replacing an SCB, read the guidelines in "Operating and Positioning the SRX5800 Firewall SCB Ejectors" on page 336. To replace an SCB, perform the following procedures:

NOTE: The procedure to replace an SCB applies to the SRX5K-SCB, SRX5K-SCBE, SRX5K-SCB3, and SRX5K-SCB4.

Removing an SRX5800 Firewall SCB

Before you begin to remove a SCB:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Replacement SCB or blank panel
- Antistatic mat

To remove an SCB (see Figure 1):

NOTE: The SCB and Routing Engine are removed as a unit. You can also remove the Routing Engine separately.

CAUTION: Before removing an SCB, ensure that you know how to operate the ejector handles properly to avoid damage to the equipment.

1. If you are removing an SCB from a chassis cluster, deactivate the fabric interfaces from any of the nodes.

   NOTE: The fabric interfaces should be deactivated to avoid failures in the chassis cluster.

   ```
   user@host# deactivate interfaces fab0
   user@host# deactivate interfaces fab1
   user@host# commit
   ```

2. Power off the Firewall using the command **request system power-off**.

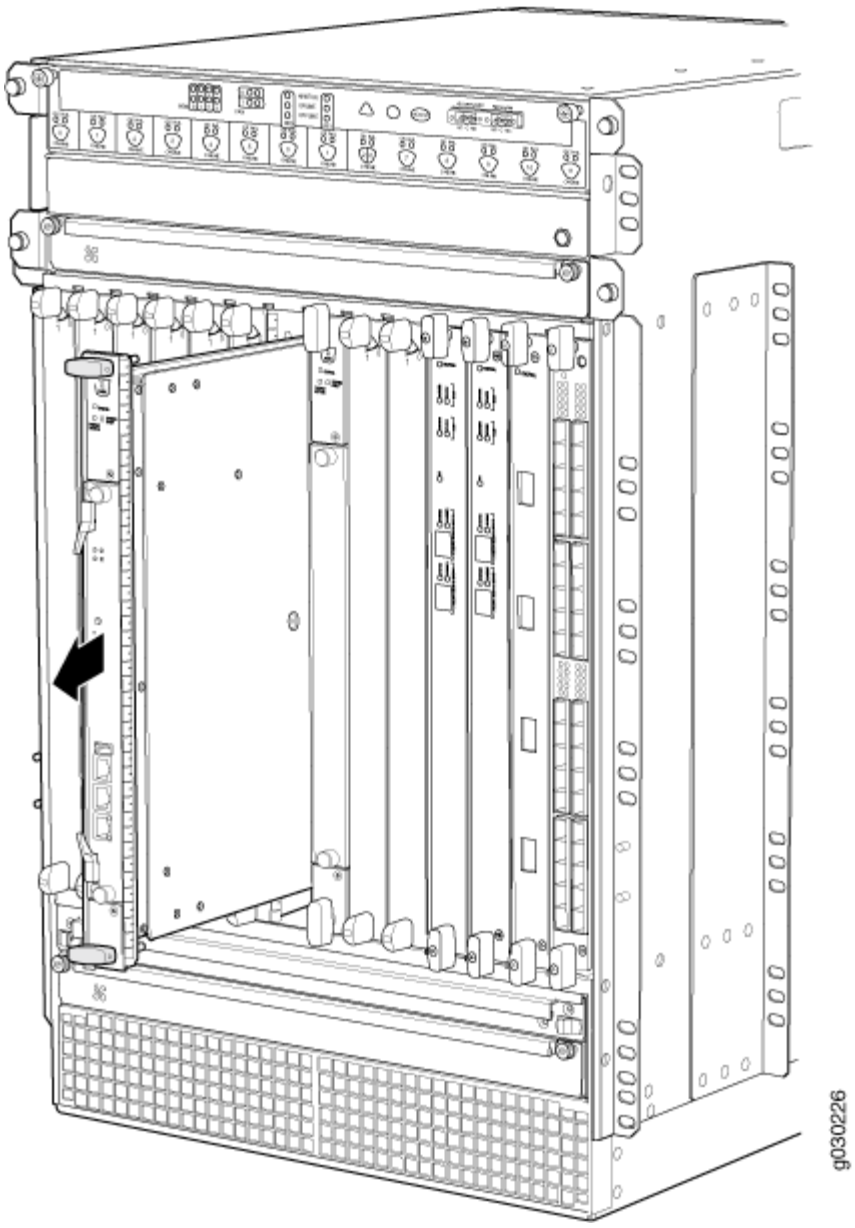
   ```
   user@host# request system power-off
   ```

   NOTE: Wait until a message appears on the console confirming that the services stopped.

3. Physically turn off the power and remove the power cables from the chassis.
4. Place an electrostatic bag or antistatic mat on a flat, stable surface.

5. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
6. Rotate the ejector handles simultaneously counterclockwise to unseat the SCB.
7. Grasp the ejector handles and slide the SCB about halfway out of the chassis.
8. Place one hand underneath the SCB to support it and slide it completely out of the chassis.
9. Place the SCB on the antistatic mat.
10. If you are not replacing the SCB now, install a blank panel over the empty slot.

Figure 154: Removing an SCB



Installing an SRX5800 Firewall SCB

Before you begin to install a SCB:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap

To install an SCB (see Figure 2):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Power off the Firewall using the command **request system power-off**.

```
user@host# request system power-off
```

> **NOTE**: Wait until a message appears on the console confirming that the services stopped.

3. Physically turn off the power and remove the power cables from the chassis.
4. Carefully align the sides of the SCB with the guides inside the chassis.
5. Slide the SCB into the chassis until you feel resistance, carefully ensuring that it is correctly aligned.
6. Grasp both ejector handles and rotate them simultaneously clockwise until the SCB is fully seated.
7. Place the ejector handles in the proper position, vertically and toward the center of the board.
8. Connect the power cables to the chassis and power on the Firewall.
9. To verify that the SCB is functioning normally, check the LEDs on its faceplate. The green **OK/FAIL** LED should light steadily a few minutes after the SCB is installed. If the **OK/FAIL** LED is red, remove and install the SCB again. If the **OK/FAIL** LED still lights steadily, the SCB is not functioning properly. Contact your customer support representative.

   To check the status of the SCB:

```
user@host> show chassis environment cb
```

10. If you installed an SCB into a chassis cluster, through the console of the newly installed SCB put the node back into cluster and reboot.

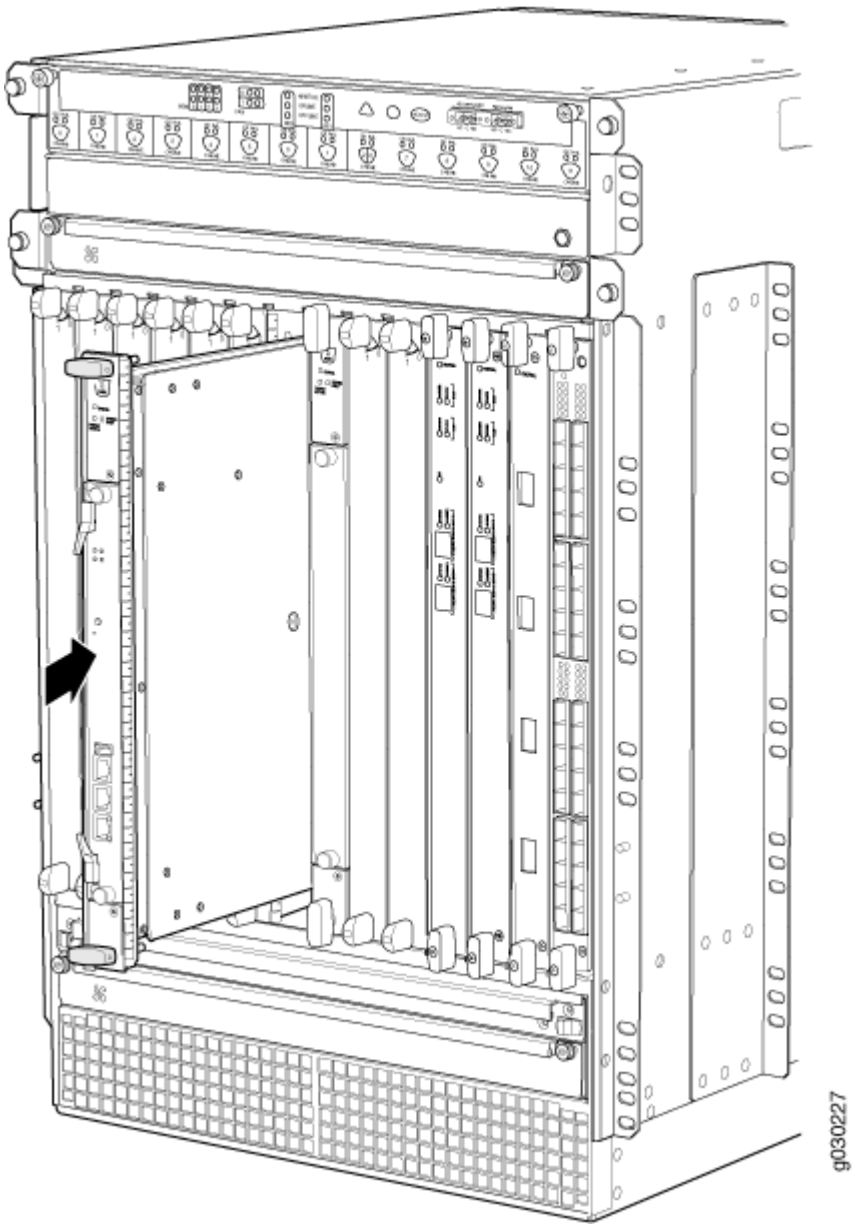
```
user@host> set chassis cluster cluster-id X node Y reboot
```

where *x* is the cluster ID and *Y* is the node ID

11. Activate the disabled fabric interfaces.

```
user@host# activate interfaces fab0
user@host# activate interfaces fab1
user@host# commit
```

Figure 155: Installing an SCB



Replacing the SRX5800 Firewall Routing Engine

IN THIS SECTION

To replace the Routing Engine, perform the following procedures:

NOTE: The procedure to replace a Routing Engine applies to SRX5K-RE-13-20, SRX5K-RE-1800X4, and SRX5K-RE-128G.

Removing the SRX5800 Firewall Routing Engine

Before you begin to remove a routing engine:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Replacement routing engine or blank panel
- Antistatic mat
- Phillips (+) number 2 screwdriver

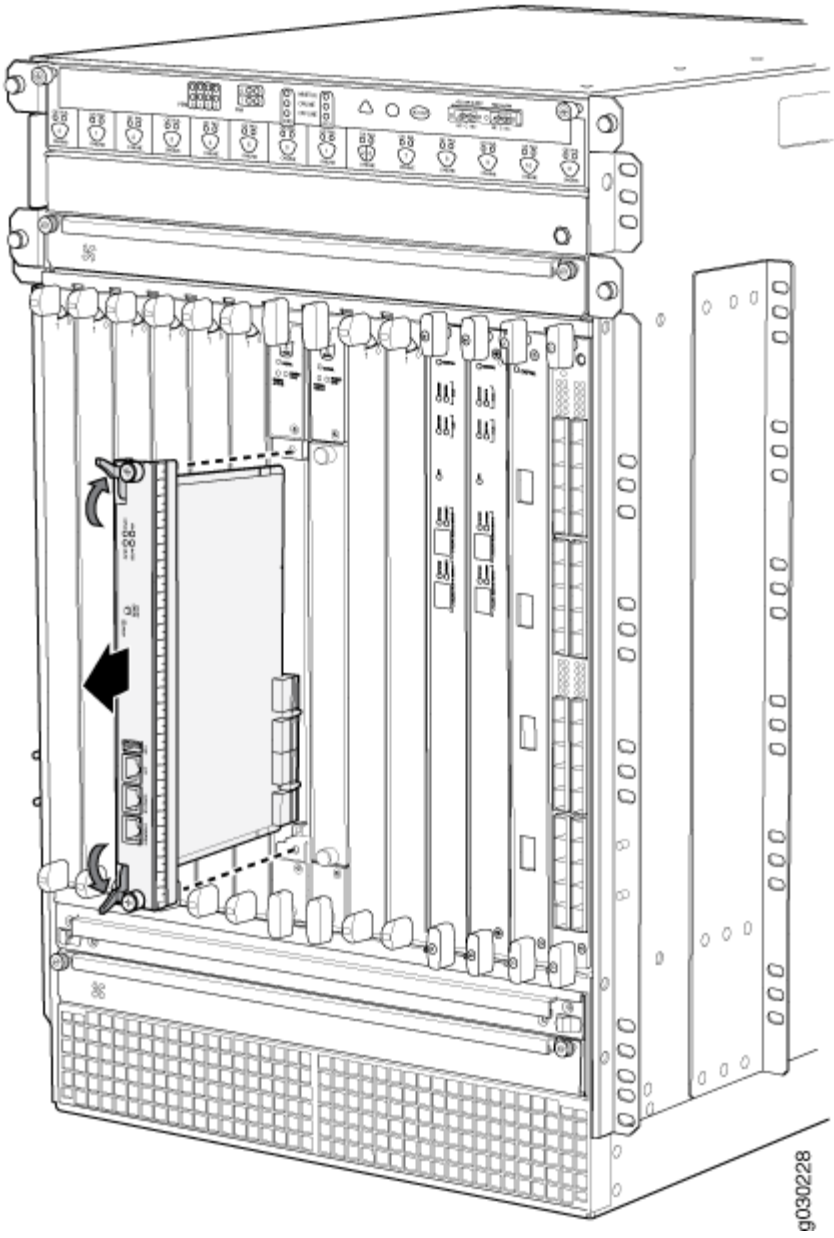
CAUTION: Before you replace a Routing Engine, you must take the host subsystem offline.

To remove the Routing Engine (see Figure 3):

1. Take the host subsystem offline as described in "Taking the SRX5800 Firewall Host Subsystem Offline" on page 335.
2. Place an electrostatic bag or antistatic mat on a flat, stable surface.
3. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.

4. Using the Phillips (+) number 2 screwdriver loosen the captive screws at each end of the Routing Engine faceplate.
5. Flip the ejector handles outward to unseat the Routing Engine.
6. Grasp the Routing Engine by the ejector handles and slide it about halfway out of the chassis.
7. Place one hand underneath the Routing Engine to support it and slide it completely out of the chassis.
8. Place the Routing Engine on the antistatic mat.

Figure 156: Removing the Routing Engine



Installing the SRX5800 Firewall Routing Engine

Before you begin to install a routing engine:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Phillips (+) number 2 screwdriver

To install a Routing Engine into an SCB (see Figure 4):

> **NOTE**: If you install only one Routing Engine in the firewall, you must install it in SCB slot 0 of firewall chassis.

1. If you have not already done so, take the host subsystem offline. See "Taking the SRX5800 Firewall Host Subsystem Offline" on page 335.
2. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
3. Ensure that the ejector handles are not in the locked position. If necessary, flip the ejector handles outward.
4. Place one hand underneath the Routing Engine to support it.
5. Carefully align the sides of the Routing Engine with the guides inside the opening on the SCB.
6. Slide the Routing Engine into the SCB until you feel resistance, and then press the Routing Engine's faceplate until it engages the connectors.
7. Press both of the ejector handles inward to seat the Routing Engine.
8. Using the Phillips (+) number 2 screwdriver tighten the captive screws on the top and bottom of the Routing Engine faceplate.
9. Power on the firewall.

   The Routing Engine might require several minutes to boot.

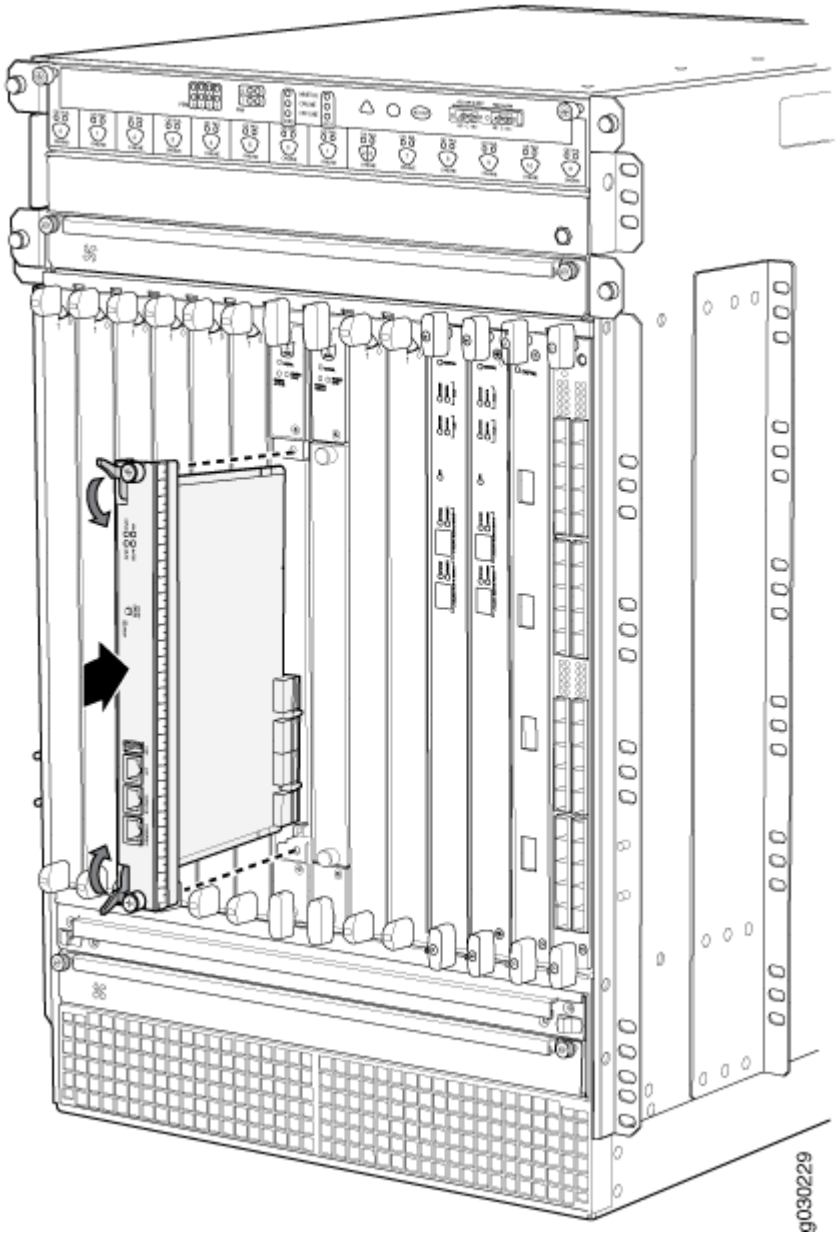
   After the Routing Engine boots, verify that it is installed correctly by checking the **RE0** and **RE1** LEDs on the craft interface. If the firewall is operational and the Routing Engine is functioning properly, the green **ONLINE** LED lights steadily. If the red **FAIL** LED lights steadily instead, remove and install the Routing Engine again. If the red **FAIL** LED still lights steadily, the Routing Engine is not functioning properly. Contact your customer support representative.

To check the status of the Routing Engine, use the CLI command:

```
user@host> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Master ...
```

For more information about using the CLI, see the CLI Explorer.

Figure 157: Installing the Routing Engine



10. If the Routing Engine was replaced on one of the nodes in a chassis cluster, then you need to copy certificates and key pairs from the other node in the cluster:

    a. Start the shell interface as a root user on both nodes of the cluster.

    b. Verify files in the **/var/db/certs/common/key-pair** folder of the source node (other node in the cluster) and destination node (node on which the Routing Engine was replaced) by using the following command:

    ```
    ls -la /var/db/certs/common/key-pair/
    ```

c. If the same files exist on both nodes, back up the files on the destination node to a different location. For example:

```
root@SRX-B% pwd /var/db/certs/common/key-pair root@SRX-B% ls -la total 8 drwx------ 2 root wheel 512 Jan 22 15:09 drwx------ 7 root wheel 512 Mar 26 2009 -rw-r--r-- 1 root wheel 0 Jan 22 15:09 test root@SRX-B% mv test test.old root@SRX-B% ls -la total 8 drwx------ 2 root wheel 512 Jan 22 15:10 drwx------ 7 root wheel 512 Mar 26 2009 -rw-r--r-- 1 root wheel 0 Jan 22 15:09 test.old root@SRX-B%
```

d. Copy the files from the **/var/db/certs/common/key-pair** folder of the source node to the same folder on the destination node.

> **NOTE**: Ensure that you use the correct node number for the destination node.

e. In the destination node, use the `ls -la` command to verify that all files from the **/var/db/certs/common/key-pair** folder of the source node are copied.

f. Repeat Step b through Step e for the **/var/db/certs/common/local** and **/var/db/certs/common/certification-authority** folders.

Low Impact Hardware Upgrade for SCB3 and IOC3

Before you begin the LICU procedure, verify that both firewalls in the cluster are running the same Junos OS release.

> **NOTE**: You can perform the hardware upgrade using the LICU process only.
>
> You must perform the hardware upgrade at the same time as the software upgrade from Junos OS Release 12.3X48-D10 to 15.1X49-D10.

If your device is part of a chassis cluster, you can upgrade SRX5K-SCBE (SCB2) to SRX5K-SCB3 (SCB3) and SRX5K-MPC (IOC2) to IOC3 (SRX5K-MPC3-100G10G or SRX5K-MPC3-40G10G) using the low-impact hardware upgrade (LICU) procedure, with minimum downtime. You can also follow this procedure to upgrade SCB1 to SCB2, and RE1 to RE2.

In the chassis cluster, the primary device is depicted as node 0 and the secondary device as node 1.

Follow these steps to perform the *LICU*.

1. Ensure that the secondary node does not have an impact on network traffic by isolating it from the network when LICU is in progress. For this, disable the physical interfaces (RETH child interfaces) on the secondary node.

```
For SRX5400 Services Gateways
admin@cluster#set interfaces xe-5/0/0 disable
admin@cluster#set interfaces xe-5/1/0 disable
For SRX5600 Services Gateways
admin@cluster#set interfaces xe-9/0/0 disable
admin@cluster#set interfaces xe-9/0/4 disable
For SRX5800 Services Gateways
admin@cluster#set interfaces xe-13/0/0 disable
admin@cluster#set interfaces xe-13/1/0 disable
```

2. Disable SYN bit and TCP sequence number checking for the secondary node to take over.

```
admin@cluster#set security flow tcp-session no-syn-check
admin@cluster#set security flow tcp-session no-sequence-check
```

3. Commit the configuration.

```
root@#commit
```

4. Disconnect control and fabric links between the devices in the chassis cluster so that nodes running different Junos OS releases are disconnected. For this, change the control port and fabric port to erroneous values. Fabric ports must be set to any FPC number and control ports to any non-IOC port. Issue the following commands:

```
admin@cluster#delete chassis cluster control-ports
admin@cluster#set chassis cluster control-ports fpc 10 port 0 <<<<<<< non-SPC port
admin@cluster#set chassis cluster control-ports fpc 22 port 0 <<<<<<< non-SPC port
admin@cluster#delete interfaces fab0
admin@cluster#delete interfaces fab1
admin@cluster#set interfaces fab0 fabric-options member-interfaces xe-4/0/5 <<<<<<< non-IOC
port
admin@cluster#set interfaces fab1 fabric-options member-interfaces xe-10/0/5<<<<<<< non-IOC
port
```

5. Commit the configuration.

```
root@#commit
```

> **NOTE**: After you commit the configuration, the following error message appears: *Connection to node1 has been broken error:remote unlock-configuration failed on node1 due to control plane communication break*.

Ignore the error message.

6. Upgrade the Junos OS release on the secondary node from 12.3X48-D10 to 15.1X49-D10.

```
admin@cluster#request system software add <location of package/junos filename> no-validate
no-copy
```

7. Power on the secondary node.

```
admin@cluster#request system reboot
```

See:

- *Powering On an AC-Powered SRX5400 Firewall*
- *Powering On a DC-Powered SRX5400 Firewall*
- *Powering On an AC-Powered SRX5600 Firewall*
- *Powering On a DC-Powered SRX5600 Firewall*
- "Powering On an AC-Powered SRX5800 Firewall" on page 263
- "Powering On a DC-Powered SRX5800 Firewall " on page 271

8. Perform the hardware upgrade on the secondary node by replacing SCB2 with SCB3, IOC2 with IOC3, and the existing midplane with the enhanced midplane.

   Following these steps while upgrading the SCB:

   To upgrade the Routing Engine on the secondary node:

   a. Before powering off the secondary node, copy the configuration information to a USB device.

   b. Replace RE1 with RE2 and upgrade the Junos OS on RE2.

   c. Upload the configuration to RE2 from the USB device.

For more information about mounting the USB drive on the device, refer to KB articles *KB12880* and *KB12022* from the *Knowledge Base*.

Perform this step when you upgrade the MPC.

a. Configure the control port, fabric port, and RETH child ports on the secondary node.

```
[edit]
```

```
root@clustert# show | display set | grep delete
```

```
delete groups global interfaces fab1
```

```
delete groups global interfaces fab0
```

```
delete interfaces reth0
```

```
delete interfaces reth1
```

```
delete interfaces xe-3/0/5 gigether-options redundant-parent
reth0
```

```
delete interfaces xe-9/0/5 gigether-options redundant-parent
reth0
```

```
delete interfaces xe-3/0/9 gigether-options redundant-parent
reth
```

```
delete interfaces xe-9/0/9 gigether-options redundant-parent
reth0
```

```
[edit]
root@clustert# show | display set | grep fab
set groups global interfaces fab1 fabric-options member-interfaces
```

```
xe-9/0/2
set groups global interfaces fab0 fabric-options member-interfaces
xe-3/0/2
```

```
[edit]
root@clustert# show | display set | grep reth0
set chassis cluster redundancy-group 1 ip-monitoring family
inet 44.44.44.2 interface reth0.0 secondary-ip-address 44.44.44.3
set interfaces xe-3/0/0 gigether-options redundant-parent
reth0
set interfaces xe-9/0/0 gigether-options redundant-parent
reth0
set interfaces reth0 vlan-tagging
set interfaces reth0 redundant-ether-options redundancy-group
1
set interfaces reth0 unit 0 vlan-id 20
set interfaces reth0 unit 0 family inet address 44.44.44.1/8
```

```
[edit]
root@clustert# show | display set | grep reth1
set interfaces xe-3/0/4 gigether-options redundant-parent
reth1
set interfaces xe-9/0/4 gigether-options redundant-parent
reth1
set interfaces reth1 vlan-tagging
set interfaces reth1 redundant-ether-options redundancy-group
1
 set interfaces reth1 unit 0 vlan-id 30
set interfaces reth1 unit 0 family inet address 55.55.55.1/8
```

9. Verify that the secondary node is running the upgraded Junos OS release.

```
root@cluster> show version  node1

Hostname: <displays the hostname>
Model: <displays the model number>
```

```
Junos: 15.1X49-D10
JUNOS Software Release [15.1X49-D10]
```

```
root@cluster> show chassis cluster status

Monitor Failure codes:
    CS  Cold Sync monitoring        FL  Fabric Connection monitoring
    GR  GRES monitoring             HW  Hardware monitoring
    IF  Interface monitoring        IP  IP monitoring
    LB  Loopback monitoring         MB  Mbuf monitoring
    NH  Nexthop monitoring          NP  NPC monitoring
    SP  SPU monitoring              SM  Schedule monitoring
    CF  Config Sync monitoring


Cluster ID: 1
Node   Priority Status         Preempt Manual   Monitor-failures

Redundancy group: 0 , Failover count: 1
node0  0        lost           n/a     n/a      n/a
node1  100      primary        no      no       None

Redundancy group: 1 , Failover count: 3
node0  0        lost           n/a     n/a      n/a
node1  150      primary        no      no       None
```

```
root@cluster>show chassis fpc pic-status  node1
Slot 1   Online       SRX5k IOC II
  PIC 0  Online       1x 100GE CFP
  PIC 2  Online       2x 40GE QSFP+
Slot 2   Online       SRX5k SPC II
  PIC 0  Online       SPU Cp
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 3   Online       SRX5k IOC II
  PIC 0  Online       10x 10GE SFP+
  PIC 2  Online       2x 40GE QSFP+
Slot 4   Online       SRX5k SPC II
  PIC 0  Online       SPU Flow
```

```
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 5   Online       SRX5k IOC II
  PIC 0  Online       10x 10GE SFP+
  PIC 2  Online       2x 40GE QSFP+
```

10. Verify configuration changes by disabling interfaces on the primary node and enabling interfaces on the secondary.

```
For SRX5400 Services Gateways
admin@cluster#set interfaces xe-2/0/0 disable
admin@cluster#set interfaces xe-2/1/0 disable
admin@cluster#delete interfaces xe-5/0/0 disable
admin@cluster#delete interfaces xe-5/1/0 disable
For SRX5600 Services Gateways
admin@cluster#set interfaces xe-2/0/0 disable
admin@cluster#set interfaces xe-2/0/4 disable
admin@cluster#delete interfaces xe-9/0/0 disable
admin@cluster#delete interfaces xe-9/0/4 disable
For SRX5800 Services Gateways
admin@cluster#set interfaces xe-1/0/0 disable
admin@cluster#set interfaces xe-1/1/0 disable
admin@cluster#delete interfaces xe-13/0/0 disable
admin@cluster#delete interfaces xe-13/1/0 disable
```

11. Check the configuration changes.

```
root@#commit check
```

12. After verifying, commit the configuration.

```
root@#commit
```

Network traffic fails over to the secondary node.

13. Verify that the failover was successful by checking the session tables and network traffic on the secondary node.

```
admin@cluster#show security flow session summary
admin@cluster#monitor interface traffic
```

14. Upgrade the Junos OS release on the primary node from 12.3X48-D10 to 15.1X49-D10.

```
admin@cluster#request system software add <location of package/junos filename> no-validate
no-copy
```

Ignore error messages pertaining to the disconnected cluster.

15. Power on the primary node.

```
admin@cluster#request system reboot
```

See:

- *Powering On an AC-Powered SRX5400 Firewall*
- *Powering On a DC-Powered SRX5400 Firewall*
- *Powering On an AC-Powered SRX5600 Firewall*
- *Powering On a DC-Powered SRX5600 Firewall*
- "Powering On an AC-Powered SRX5800 Firewall" on page 263
- "Powering On a DC-Powered SRX5800 Firewall " on page 271

16. Perform the hardware upgrade on the primary node by replacing SCB2 with SCB3, IOC2 with IOC3, and the existing midplane with the enhanced midplane.

Perform the following steps while upgrading the SCB.

To upgrade the Routing Engine on the primary node:

a. Before powering off the secondary node, copy the configuration information to a USB device.

b. Replace RE1 with RE2 and upgrade the Junos OS on RE2.

c. Upload the configuration to RE2 from the USB device.

For more information about mounting the USB drive on the device, refer to KB articles *KB12880* and *KB12022* from the *Knowledge Base*.

Perform this step when you upgrade the MPC.

a. Configure the control port, fabric port, and RETH child ports on the primary node.

```
[edit]
root@clustert# show | display set | grep delete
delete groups global interfaces fab1
delete groups global interfaces fab0
delete interfaces reth0
delete interfaces reth1
delete interfaces xe-3/0/5 gigether-options redundant-parent
reth0
delete interfaces xe-9/0/5 gigether-options redundant-parent
reth0
delete interfaces xe-3/0/9 gigether-options redundant-parent
reth0
delete interfaces xe-9/0/9 gigether-options redundant-parent
reth0
```

```
[edit]
root@clustert# show | display set | grep fab
set groups global interfaces fab1 fabric-options member-interfaces
xe-9/0/2
set groups global interfaces fab0 fabric-options member-interfaces
xe-3/0/2
```

```
[edit]
root@clustert# show | display set | grep reth0
set chassis cluster redundancy-group 1 ip-monitoring family
inet 44.44.44.2 interface reth0.0 secondary-ip-address 44.44.44.3
set interfaces xe-3/0/0 gigether-options redundant-parent
reth0
set interfaces xe-9/0/0 gigether-options redundant-parent
reth0
set interfaces reth0 vlan-tagging
set interfaces reth0 redundant-ether-options redundancy-group
1
set interfaces reth0 unit 0 vlan-id 20
set interfaces reth0 unit 0 family inet address 44.44.44.1/8
```

```
[edit]
root@clustert# show | display set | grep reth1
set interfaces xe-3/0/4 gigether-options redundant-parent
reth1
set interfaces xe-9/0/4 gigether-options redundant-parent
reth1
set interfaces reth1 vlan-tagging
set interfaces reth1 redundant-ether-options redundancy-group
1
 set interfaces reth1 unit 0 vlan-id 30
set interfaces reth1 unit 0 family inet address 55.55.55.1/8
```

17. Verify that the primary node is running the upgraded Junos OS release, and that the primary node is available to take over network traffic.

```
root@cluster> show version  node1

Hostname: <displays the hostname>
Model: <displays the model number>
Junos: 15.1X49-D10
JUNOS Software Release [15.1X49-D10]
```

```
root@cluster> show chassis cluster status

Monitor Failure codes:
    CS  Cold Sync monitoring        FL  Fabric Connection monitoring
    GR  GRES monitoring             HW  Hardware monitoring
    IF  Interface monitoring        IP  IP monitoring
    LB  Loopback monitoring         MB  Mbuf monitoring
    NH  Nexthop monitoring          NP  NPC monitoring
    SP  SPU monitoring              SM  Schedule monitoring
    CF  Config Sync monitoring


Cluster ID: 1
Node   Priority Status         Preempt Manual   Monitor-failures

Redundancy group: 0 , Failover count: 1
```

```
node0  0        lost           n/a     n/a      n/a
node1  100      primary        no      no       None

Redundancy group: 1 , Failover count: 3
node0  0        lost           n/a     n/a      n/a
node1  150      primary        no      no       None
```

```
root@cluster>show chassis fpc pic-status  node1
Slot 1   Online       SRX5k IOC II
  PIC 0  Online       1x 100GE CFP
  PIC 2  Online       2x 40GE QSFP+
Slot 2   Online       SRX5k SPC II
  PIC 0  Online       SPU Cp
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 3   Online       SRX5k IOC II
  PIC 0  Online       10x 10GE SFP+
  PIC 2  Online       2x 40GE QSFP+
Slot 4   Online       SRX5k SPC II
  PIC 0  Online       SPU Flow
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 5   Online       SRX5k IOC II
  PIC 0  Online       10x 10GE SFP+
  PIC 2  Online       2x 40GE QSFP+
```

18. Check the configuration changes.

```
root@#commit check
```

19. After verifying, commit the configuration.

```
root@#commit
```

20. Verify configuration changes by disabling interfaces on the secondary node and enabling interfaces on the primary.

```
For SRX5400 Services Gateways
admin@cluster#set interfaces xe-5/0/0 disable
admin@cluster#set interfaces xe-5/1/0 disable
admin@cluster#delete interfaces xe-2/0/0 disable
admin@cluster#delete interfaces xe-2/1/0 disable
For SRX5600 Services Gateways
admin@cluster#set interfaces xe-9/0/0 disable
admin@cluster#set interfaces xe-9/0/4 disable
admin@cluster#delete interfaces xe-2/0/0 disable
admin@cluster#delete interfaces xe-2/0/4 disable
For SRX5800 Services Gateways
admin@cluster#set interfaces xe-13/0/0 disable
admin@cluster#set interfaces xe-13/1/0 disable
admin@cluster#delete interfaces xe-1/0/0 disable
admin@cluster#delete interfaces xe-1/1/0 disable
```

Network traffic fails over to the primary node.

21. To synchronize the devices within the cluster, reconfigure the control ports and fabric ports with the correct port values on the secondary node.

```
admin@cluster#delete chassis cluster control-ports
admin@cluster#set chassis cluster control-ports fpc 1 port 0
admin@cluster#set chassis cluster control-ports fpc 13 port 0
admin@cluster#delete interfaces fab0
admin@cluster#delete interfaces fab1
admin@cluster#set interfaces fab0 fabric-options member-interfaces xe-3/0/2
admin@cluster#set interfaces fab1 fabric-options member-interfaces xe-9/0/2
```

22. Commit the configuration.

```
root@#commit
```

23. Power on the secondary node.

```
admin@cluster#request system reboot
```

See:

- *Powering On an AC-Powered SRX5400 Firewall*
- *Powering On a DC-Powered SRX5400 Firewall*
- *Powering On an AC-Powered SRX5600 Firewall*
- *Powering On a DC-Powered SRX5600 Firewall*
- "Powering On an AC-Powered SRX5800 Firewall" on page 263
- "Powering On a DC-Powered SRX5800 Firewall " on page 271

a. When you power on the secondary node, enable the control ports and fabric ports on the primary node, and reconfigure them with the correct port values.

```
admin@cluster#delete chassis cluster control-ports
admin@cluster#set chassis cluster control-ports fpc 1 port 0
admin@cluster#set chassis cluster control-ports fpc 13 port 0
admin@cluster#delete interfaces fab0
admin@cluster#delete interfaces fab1
admin@cluster#set interfaces fab0 fabric-options member-interfaces xe-3/0/2
admin@cluster#set interfaces fab1 fabric-options member-interfaces xe-9/0/2
```

24. Commit the configuration.

```
root@#commit
```

25. After the secondary node is up, verify that it synchronizes with the primary node.

```
admin@cluster#delete interfaces xe-4/0/5 disable
admin@cluster#delete interfaces xe-10/0/5 disable
```

26. Enable SYN bit and TCP sequence number checking for the secondary node.

```
admin@cluster#delete security flow tcp-session no-syn-check
admin@cluster#delete security flow tcp-session no-sequence-check
```

27. Commit the configuration.

```
root@#commit
```

28. Verify the Redundancy Group (RG) states and their priority.

```
root@cluster>show version
node0:
--------------------------------------------------------------------------
Hostname: <displays the hostname>
Model: <displays the model number>
Junos: 15.1X49-D10
JUNOS Software Release [15.1X49-D10]

node1:
--------------------------------------------------------------------------
Hostname: <displays the hostname>
Model: <displays the model>
Junos: 15.1X49-D10
JUNOS Software Release [15.1X49-D10]
```

After the secondary node is powered on, issue the following command:

```
root@cluster>show chassis fpc pic-status
node0:
--------------------------------------------------------------------------
Slot 1   Online       SRX5k IOC II
  PIC 0  Online       1x 100GE CFP
  PIC 2  Online       2x 40GE QSFP+
Slot 2   Online       SRX5k SPC II
  PIC 0  Online       SPU Cp
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 3   Online       SRX5k IOC3 24XGE+6XLG
  PIC 0  Online       12x 10GE SFP+
  PIC 1  Online       12x 10GE SFP+
  PIC 2  Offline      3x 40GE QSFP+
  PIC 3  Offline      3x 40GE QSFP+
Slot 4   Online       SRX5k SPC II
  PIC 0  Online       SPU Flow
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 5   Online       SRX5k IOC II
```

```
  PIC 0  Online       10x 10GE SFP+
  PIC 2  Online       10x 10GE SFP+

node1:
--------------------------------------------------------------------------
Slot 1   Online       SRX5k IOC II
  PIC 0  Online       1x 100GE CFP
  PIC 2  Online       2x 40GE QSFP+
Slot 2   Online       SRX5k SPC II
  PIC 0  Online       SPU Cp
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 3   Online       SRX5k IOC3 24XGE+6XLG
  PIC 0  Online       12x 10GE SFP+
  PIC 1  Online       12x 10GE SFP+
  PIC 2  Offline      3x 40GE QSFP+
  PIC 3  Offline      3x 40GE QSFP+
Slot 4   Online       SRX5k SPC II
  PIC 0  Online       SPU Flow
  PIC 1  Online       SPU Flow
  PIC 2  Online       SPU Flow
  PIC 3  Online       SPU Flow
Slot 5   Online       SRX5k IOC II
  PIC 0  Online       10x 10GE SFP+
  PIC 2  Online       2x 40GE QSFP+
```

```
root@cluster> show chassis cluster status
    CS  Cold Sync monitoring        FL  Fabric Connection monitoring
    GR  GRES monitoring             HW  Hardware monitoring
    IF  Interface monitoring        IP  IP monitoring
    LB  Loopback monitoring         MB  Mbuf monitoring
    NH  Nexthop monitoring          NP  NPC monitoring
    SP  SPU monitoring              SM  Schedule monitoring
    CF  Config Sync monitoring

Cluster ID: 1
Node   Priority Status         Preempt Manual   Monitor-failures

Redundancy group: 0 , Failover count: 0
```

```
node0  250      primary        no      no       None
node1  100      secondary      no      no       None

Redundancy group: 1 , Failover count: 0
node0  254      primary        no      no       None
node1  150      secondary      no      no       None
```

```
root@cluster>show security monitoring
node0:
--------------------------------------------------------------------------
                  Flow session   Flow session     CP session     CP session
FPC PIC CPU Mem        current        maximum        current        maximum
--------------------------------------------------------------------------
  2   0   0  11              0              0        1999999      104857600
  2   1   2   5         289065        4194304              0              0
  2   2   2   5         289062        4194304              0              0
  2   3   2   5         289060        4194304              0              0
  4   0   2   5         289061        4194304              0              0
  4   1   2   5         281249        4194304              0              0
  4   2   2   5         281251        4194304              0              0
  4   3   2   5         281251        4194304              0              0

node1:
--------------------------------------------------------------------------
                  Flow session   Flow session     CP session     CP session
FPC PIC CPU Mem        current        maximum        current        maximum
--------------------------------------------------------------------------
  2   0   0  11              0              0        1999999      104857600
  2   1   0   5         289065        4194304              0              0
  2   2   0   5         289062        4194304              0              0
  2   3   0   5         289060        4194304              0              0
  4   0   0   5         289061        4194304              0              0
  4   1   0   5         281249        4194304              0              0
  4   2   0   5         281251        4194304              0              0
  4   3   0   5         281251        4194304              0              0
```

Enable the traffic interfaces on the secondary node.

```
root@cluster> show interfaces terse | grep reth0
xe-3/0/0.0              up    up   aenet    --> reth0.0
xe-3/0/0.32767          up    up   aenet    --> reth0.32767
xe-9/0/0.0              up    up   aenet    --> reth0.0
 xe-9/0/0.32767          up    up   aenet    --> reth0.32767
reth0                   up    up
reth0.0                 up    up   inet     44.44.44.1/8

reth0.32767             up    up   multiservice
```

```
root@cluster> show interfaces terse | grep reth1
xe-3/0/4.0              up    up   aenet    --> reth1.0
xe-3/0/4.32767          up    up   aenet    --> reth1.32767
xe-9/0/4.0              up    up   aenet    --> reth1.0
 xe-9/0/4.32767          up    up   aenet    --> reth1.32767
reth1                  up    up
reth1.0                 up    up   inet     55.55.55.1/8

reth1.32767             up    up   multiservice
```

For more information about LICU, refer to KB article *KB17947* from the *Knowledge Base*.

In-Service Hardware Upgrade for SRX5K-RE-1800X4 and SRX5K-SCBE or SRX5K-RE-1800X4 and SRX5K-SCB3 in a Chassis Cluster

Ensure that the following prerequisites are completed before you begin the *ISHU* procedure:

- Replace all interface cards such as IOCs and Flex IOCs as specified in Table 71 on page 363.

  Table 71: List of Interface Cards for Upgrade

Cards to Replace	Replacement Cards for Upgrade
SRX5K-40GE-SFP	SRX5K-MPC and MICs

Table 71: List of Interface Cards for Upgrade *(Continued)*

Cards to Replace	Replacement Cards for Upgrade
SRX5K-4XGE-XFP	SRX5K-MPC and MICs
SRX5K-FPC-IOC	SRX5K-MPC and MICs
SRX5K-RE-13-20	SRX5K-RE-1800X4
SRX5K-SCB	SRX5K-SCBE
SRX5K-SCBE	SRX5K-SCB3

- Verify that both firewalls in the cluster are running the same Junos OS versions; release 12.1X47-D15 or later for SRX5K-SCBE with SRX5K-RE-1800X4 and 15.1X49-D10 or later for SRX5K-SCB3 with SRX5K-RE-1800X4. For more information on cards supported on the firewalls see "Cards Supported on SRX5400, SRX5600, and SRX5800 Firewalls" on page 107.

  For more information about unified in-service software upgrade (*unified ISSU*), see Upgrading Both Devices in a Chassis Cluster Using an ISSU.

If your device is part of a chassis cluster, using the in-service hardware upgrade (ISHU) procedure you can upgrade:

- SRX5K-SCB with SRX5K-RE-13-20 to SRX5K-SCBE with SRX5K-RE-1800X4

  NOTE: Both the firewalls must have the same Junos OS version 12.3X48.

- SRX5K-SCBE with SRX5K-RE-1800X4 to SRX5K-SCB3 with SRX5K-RE-1800X4

  NOTE: You cannot upgrade SRX5K-SCB with SRX5K-RE-13-20 directly to SRX5K-SCB3 with SRX5K-RE-1800X4.

NOTE: We strongly recommend that you perform the *ISHU* during a maintenance window, or during the lowest possible traffic as the secondary node is not available at this time.

Ensure to upgrade the SCB and Routing Engine at the same time as the following configurations are only supported:

- SRX5K-RE-13-20 and SRX5K-SCB
- SRX5K-RE-1800X4 and SRX5K-SCBE
- SRX5K-RE-1800X4 and SRX5K-SCB3

NOTE: While performing the ISHU, in the SRX5800 firewall, the second SCB can contain a Routing Engine but the third SCB must not contain a Routing Engine. In the SRX5600 Firewall, the second SCB can contain a Routing Engine.

To perform an *ISHU*:

1. Export the configuration information from the secondary node to a USB or an external storage device.

   For more information about mounting the USB on the device, refer to KB articles *KB12880* and *KB12022* from the *Knowledge Base*.
2. Power off the secondary node.

   See, *Powering Off the SRX5400 Firewall*, *Powering Off the SRX5600 Firewall*, or "Powering Off the SRX5800 Firewall" on page 272.
3. Disconnect all the interface cards from the chassis backplane by pulling them out of the backplane by 6” to 8” (leaving cables in place).
4. Replace the SRX5K-SCBs with SRX5K-SCBEs, or SRX5K-SCBEs with SRX5K-SCB3s and SRX5K-RE-13-20s with SRX5K-RE-1800X4s based on the chassis specifications.
5. Power on the secondary node.

   See:

   - *Powering On an AC-Powered SRX5400 Firewall*
   - *Powering On a DC-Powered SRX5400 Firewall*
   - *Powering On an AC-Powered SRX5600 Firewall*
   - *Powering On a DC-Powered SRX5600 Firewall*
   - "Powering On an AC-Powered SRX5800 Firewall" on page 263
   - "Powering On a DC-Powered SRX5800 Firewall " on page 271

6. After the secondary node reboots as a standalone node, configure the same cluster ID as in the primary node.

```
root@>set chassis cluster cluster-id 1 node 1
```

7. Install the same Junos OS software image on the secondary node as on the primary node and reboot.

> **NOTE**: Ensure that the Junos OS version installed is release 12.1X47-D15 or later for SRX5K-RE-1800X4 & SRX5K-SCBE and 15.1X49-D10 or later for SRX5K-RE-1800X4 & SRX5K-SCB3.

8. After the secondary node reboots, import all the configuration settings from the USB to the node.

   For more information about mounting the USB on the device, refer to KB articles *KB12880* and *KB12022* from the *Knowledge Base*.

9. Power off the secondary node.

   See *Powering Off the SRX5400 Firewall*, *Powering Off the SRX5600 Firewall*, or "Powering Off the SRX5800 Firewall" on page 272.

10. Re-insert all the interface cards into the chassis backplane.

> **NOTE**: Ensure the cards are inserted in the same order as in the primary node, and maintain connectivity between the control link and fabric link.

11. Power on the node and issue this command to ensure all the cards are online:

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

After the node boots, it must join the cluster as a secondary node. To verify, issue the following command

```
admin@cluster> show chassis cluster status
```

> **NOTE**: The command output must indicate that the node priority is set to a non-zero value, and that the cluster contains a primary node and a secondary node.

12. Initiate Redundancy Group (RG) failover to the upgraded node, manually, so that it is assigned to all RGs as a primary node.

For RG0, issue the following command:

```
admin@cluster> request chassis cluster failover
redundancy-group 0 node 1
```

For RG1, issue the following command:

```
admin@cluster> request chassis cluster failover
redundancy-group 1 node 1
```

Verify that all RGs are failed over by issuing the following command:

```
admin@cluster> show chassis cluster status
```

13. Verify the operations of the upgraded secondary node by performing the following:

    - To ensure all FPC's are online, issue the following command:

      ```
      admin@cluster> show chassis fpc pic-status
      ```

    - To ensure all RG's are upgraded and the node priority is set to a non-zero value, issue the following command:

      ```
      admin@cluster> show chassis cluster status
      ```

    - To ensure that the upgraded primary node receives and transmits data, issue the following command:

      ```
      admin@cluster> monitor interface traffic
      ```

    - To ensure sessions are created and deleted on the upgraded node, issue the following command:

      ```
      admin@cluster> show security monitoring
      ```

14. Repeat Step 1 through 12 for the primary node.

15. To ensure that the ISHU process is completed successfully, check the status of the cluster by issuing the following command:

```
admin@cluster> show chassis cluster status
```

For detailed information about chassis cluster, see the *Chassis Cluster User Guide for SRX Series Devices* at www.juniper.net/documentation/.

Maintaining the SRX5800 Line Cards and Modules

IN THIS SECTION

Maintaining Interface Cards and SPCs on the SRX5800 Firewall

IN THIS SECTION

Purpose

For optimum firewall performance, verify the condition of the Services Processing Cards (SPCs) and interface cards (IOCs, Flex IOCs and MPCs). The firewall can have up to 11 SPCs and interface cards. To maintain SPCs and interface cards, perform the following procedures regularly.

Action

On a regular basis:

- Check the LEDs on the craft interface corresponding to the slot for each SPC and interface card. The green LED labeled **OK** lights steadily when a card is functioning normally.
- Check the **OK/FAIL** LED on the faceplate of each SPC and interface card. If the card detects a failure, it sends an alarm message to the Routing Engine.
- Issue the CLI `show chassis fpc` command to check the status of installed cards. As shown in the sample output, the value *Online* in the column labeled *State* indicates that the card is functioning normally:

```
user@host> show chassis fpc
        Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State       (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online       41      9          0       1024       15         57
  1  Online       43      5          0       1024       16         57
  2  Online       43     11          0       1024       16         57
  3  Empty
  4  Empty
  5  Online       42      6          0       1024       16         57
```

For more detailed output, add the `detail` option. The following example does not specify a slot number, which is optional:

```
user@host> show chassis fpc detail

Slot 0 information:
  State                                 Online
  Temperature                           41 degrees C / 105 degrees F
  Total CPU DRAM                      1024 MB
  Total RLDRAM                         256 MB
  Total DDR DRAM                      4096 MB
  Start time:                              2007-07-10 12:28:33 PDT
```

```
  Uptime:                              1 hour, 33 minutes, 52 seconds
Slot 1 information:
  State                                Online
  Temperature                       43 degrees C / 109 degrees F
  Total CPU DRAM                   1024 MB
  Total RLDRAM                      256 MB
  Total DDR DRAM                   4096 MB
  Start time:                          2007-07-10 12:28:38 PDT
  Uptime:                              1 hour, 33 minutes, 47 seconds
Slot 2 information:
  State                                Online
  Temperature                       43 degrees C / 109 degrees F
  Total CPU DRAM                   1024 MB
  Total RLDRAM                      256 MB
  Total DDR DRAM                   4096 MB
  Start time:                          2007-07-10 12:28:40 PDT
  Uptime:                              1 hour, 33 minutes, 45 seconds
Slot 5 information:
  State                                Online
  Temperature                       42 degrees C / 107 degrees F
  Total CPU DRAM                   1024 MB
  Total RLDRAM                      256 MB
  Total DDR DRAM                   4096 MB
  Start time:                          2007-07-10 12:28:42 PDT
  Uptime:                              1 hour, 33 minutes, 43 seconds
```

- Issue the CLI `show chassis fpc pic-status` command. The slots are numbered **0** through **5**, bottom to top:

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

Slot 0   Online       SRX5k DPC 40x 1GE
  PIC 0  Online       10x 1GE RichQ
  PIC 1  Online       10x 1GE RichQ
  PIC 2  Online       10x 1GE RichQ
  PIC 3  Online       10x 1GE RichQ
Slot 1   Online       SRX5k DPC 40x 1GE
  PIC 0  Online       10x 1GE RichQ
  PIC 1  Online       10x 1GE RichQ
  PIC 2  Online       10x 1GE RichQ
  PIC 3  Online       10x 1GE RichQ
Slot 2   Online       SRX5k DPC 40x 1GE
```

```
  PIC 0  Online       10x 1GE RichQ
  PIC 1  Online       10x 1GE RichQ
  PIC 2  Online       10x 1GE RichQ
  PIC 3  Online       10x 1GE RichQ
Slot 3   Online       SRX5k SPC
  PIC 0  Offline
  PIC 1  Offline
Slot 4   Online       SRX5k SPC
  PIC 0  Offline
  PIC 1  Offline
```

For further description of the output from the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

Replacing SRX5800 Firewall IOCs

IN THIS SECTION

To replace an IOC, perform the following procedures:

Removing an SRX5800 Firewall IOC

Before you begin to remove an IOC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Replacement IOC or IOC blank panel
- Antistatic mat for the IOC

- Rubber safety caps for the transceivers
- Dust covers to cover the ports

An IOC weighs up to 13.1 lb (5.9 kg). Be prepared to accept its full weight.

To remove an IOC (see Figure 1):

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. Label the cables connected to each port on the IOC so that you can later reconnect the cables to the correct ports.
3. Use one of the following methods to take the IOC offline:
   - Press and hold the corresponding IOC online button on the craft interface. The green **OK** LED next to the button begins to blink. Hold the button down until the LED goes off.
   - Issue the following CLI command:

     ```
     user@host>request chassis fpc slot slot-number offline
     ```

     For more information about the command, see *Junos OS System Basics and Services Command Reference* at https://www.juniper.net/documentation/.
4. Power off the firewall using the command **request system power-off**.

   ```
   user@host# request system power-off
   ```

   NOTE: Wait until a message appears on the console confirming that the services stopped.
5. Physically turn off the power and remove the power cables from the chassis.
6. Remove the cables from the IOC.

   LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

CAUTION: Do not leave a fiber-optic transceiver uncovered, except when you are inserting or removing cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

7. Immediately cover each optical transceiver and the end of each fiber-optic cable with a rubber safety cap.
8. Cover the ports on the IOC with dust covers if you remove the optical transceivers from the IOC.
9. Arrange the disconnected cables in the cable manager to prevent the cables from developing stress points.
10. Simultaneously turn both of the ejector handles counterclockwise to unseat the IOC.
11. Grasp the handles and slide the IOC straight out of the card cage halfway.
12. Place one hand around the front of the IOC and the other hand under it to support it. Slide the IOC completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

CAUTION: The weight of the IOC is concentrated in the back end. Be prepared to accept the full weight—up to 13.1 lb (5.9 kg)—as you slide the IOC out of the chassis.

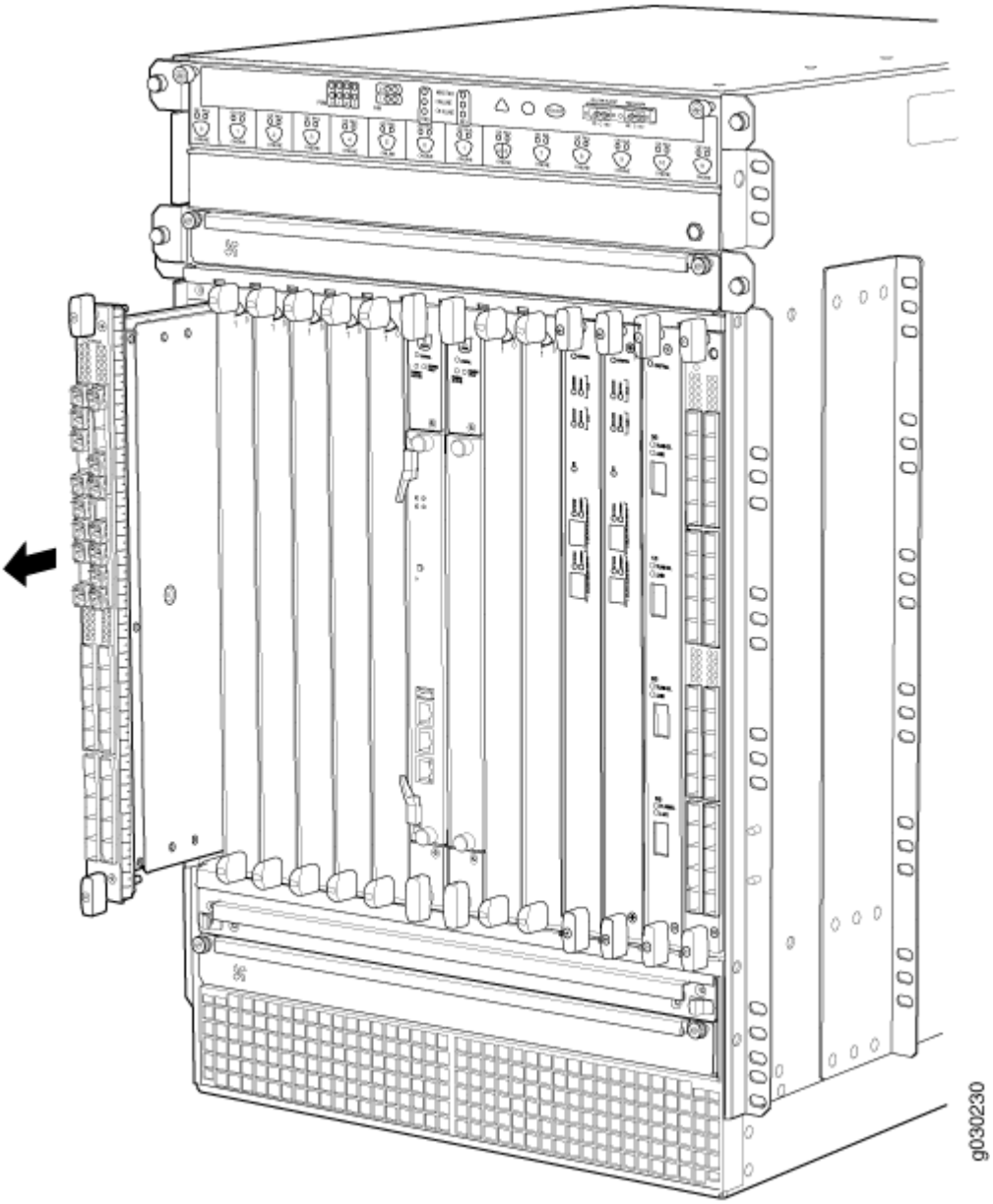
When the IOC is out of the chassis, do not hold it by the ejector handles, bus bars, or edge connectors. They cannot support its weight.

Do not stack IOC on top of one another after removal. Place each one individually in an electrostatic bag or on its own antistatic mat on a flat, stable surface.

13. If you are not reinstalling an IOC into the empy slot within a short time, install a blank IOC panel over the slot to maintain proper airflow in the card cage.

CAUTION: After removing an IOC from the chassis, wait at least 30 seconds before reinserting it, removing an IOC from a different slot, or inserting an IOC into a different slot.

Figure 158: Removing an IOC



Installing an SRX5800 Firewall IOC

Before you begin to install an IOC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap

- Antistatic mat for the IOC
- Rubber safety caps for the transceivers

An IOC weighs up to 13.1 lb (5.9 kg). Be prepared to accept its full weight.

To install an IOC (see Figure 2):

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. Power off the firewall using the command **request system power-off**.

```
user@host# request system power-off
```

NOTE: Wait until a message appears on the console confirming that the services stopped.

3. Physically turn off the power and remove the power cables from the chassis.
4. Place the IOC on an antistatic mat or remove it from its electrostatic bag.
5. Identify the slot on the firewall where it will be installed.
6. Verify that each transceiver is covered by a rubber safety cap. If it is not, cover the transceiver with a safety cap.
7. Orient the IOC so that the faceplate faces you.
8. Lift the IOC into place and carefully align the top and bottom edges of the IOC with the guides inside the card cage.
9. Slide the IOC all the way into the card cage until you feel resistance.
10. Grasp both ejector handles and rotate them clockwise simultaneously until the IOC is fully seated.
11. Remove the rubber safety cap from each fiber-optic transceiver and cable.

LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

12. Insert the cables into the cable connector ports on each IOC (see Figure 3).
13. Arrange the cable in the cable manager to prevent it from dislodging or developing stress points. Secure the cable so that it is not supporting its own weight as it hangs to the floor. Place excess cable out of the way in a neatly coiled loop. Placing fasteners on the loop helps to maintain its shape.

CAUTION: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

14. Connect the power cables to the chassis.
15. Power on the firewall.
16. Use one of the following methods to bring the IOC online:

    - Press and hold the corresponding IOC online button on the craft interface until the green **OK** LED next to the button lights steadily, in about 5 seconds.
    - Issue the following CLI command:

```
user@host>request chassis fpc slot slot-number online
```

    For more information about the command, see *Junos OS System Basics and Services Command Reference* at https://www.juniper.net/documentation/.

    CAUTION: After the **OK** LED turns green, wait at least 30 seconds before removing the IOC again, removing an IOC from a different slot, or inserting an IOC in a different slot.

    You can also verify that the IOC is functioning correctly by issuing the `show chassis fpc` and `show chassis fpc pic-status` commands.

Figure 159: Installing an IOC

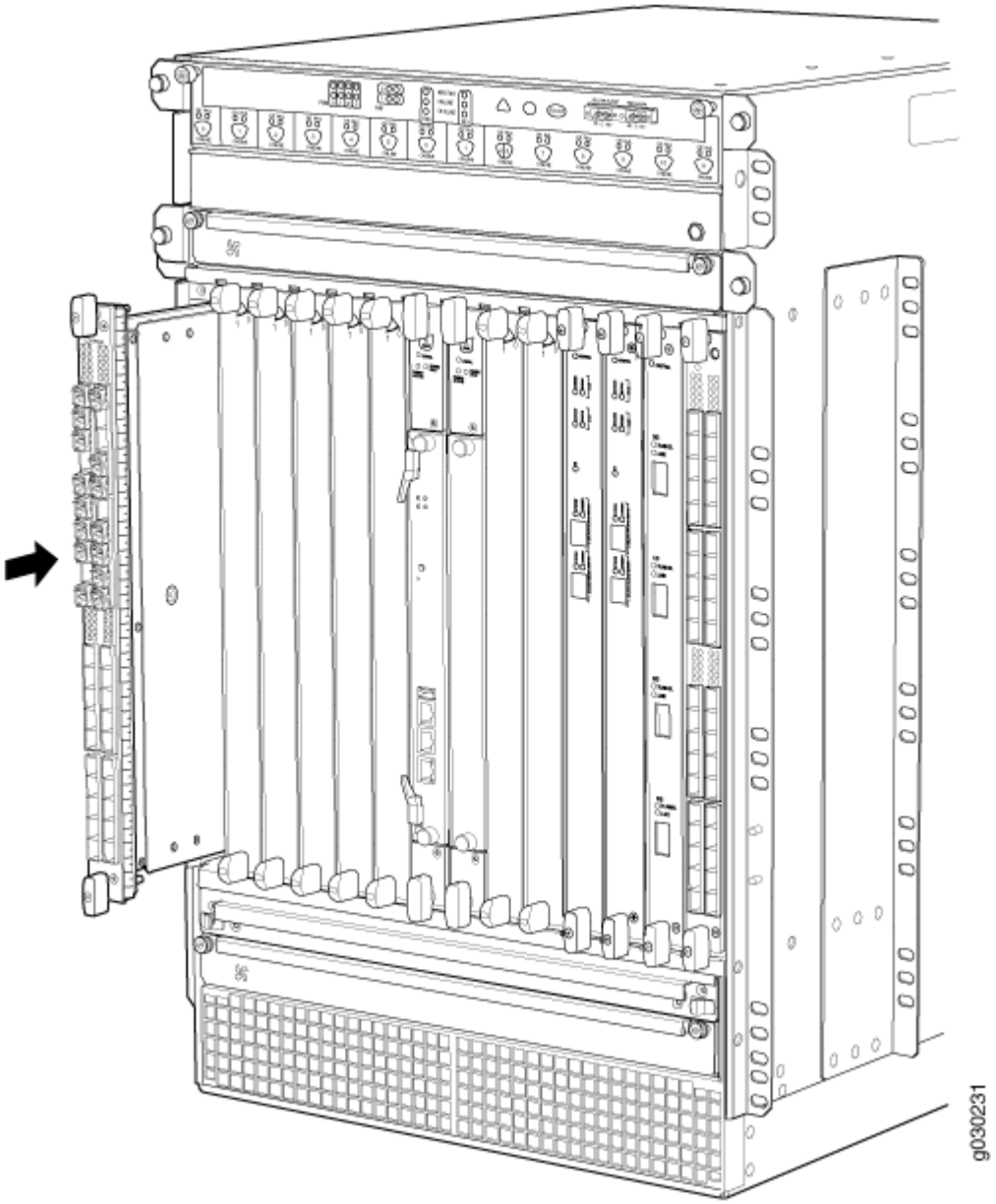
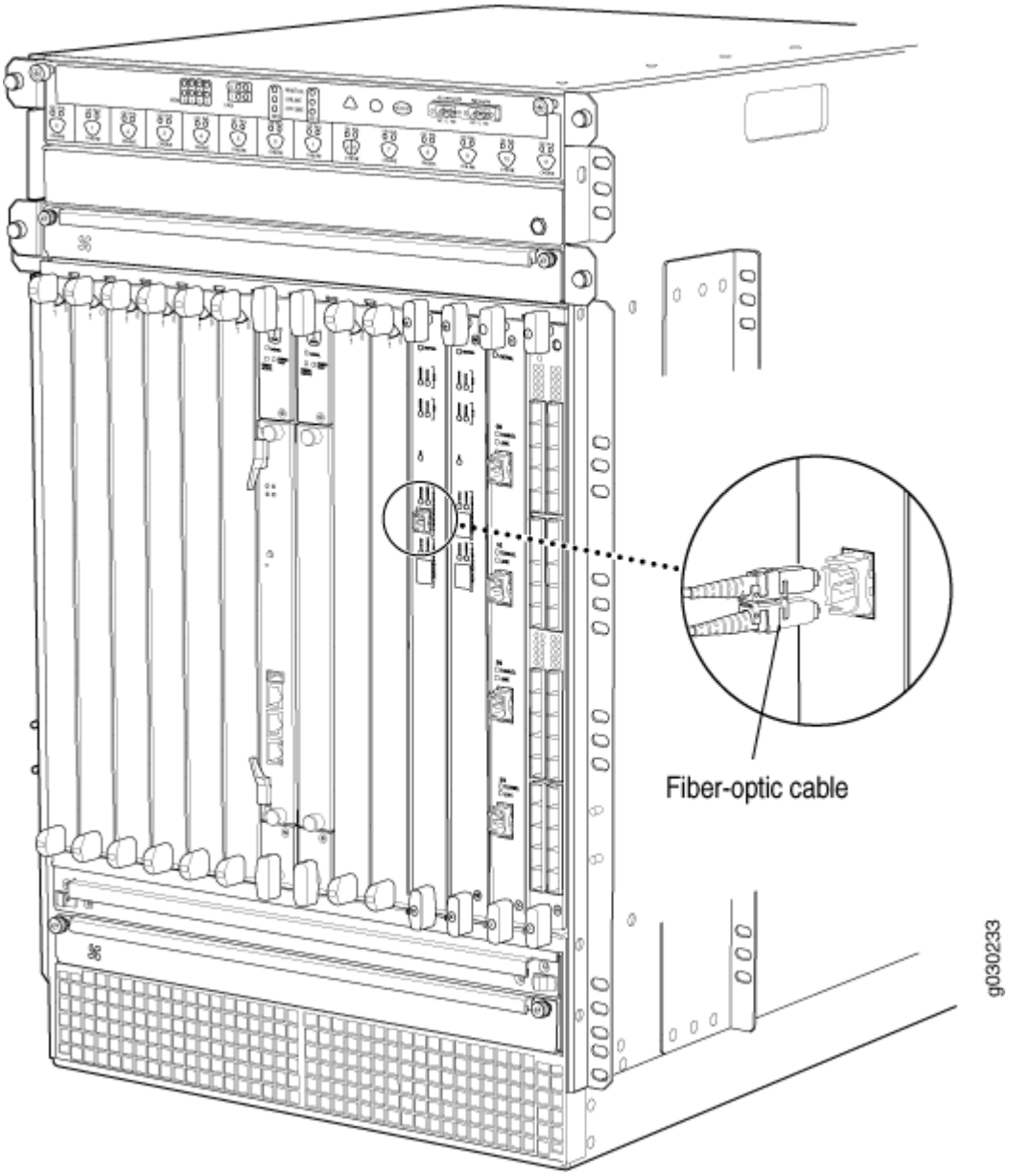


Figure 160: Attaching a Cable to an IOC



Replacing SRX5800 Firewall Flex IOCs

IN THIS SECTION

To replace a Flex IOC, perform the following procedures:

Removing an SRX5800 Firewall Flex IOC

Before you begin to remove a Flex IOC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Replacement Flex IOC or Flex IOC blank panel
- Antistatic mat for the Flex IOC

A Flex IOC weighs up to 13.1 lb (5.9 kg). Be prepared to accept the full weight of the card as you remove it.

To remove a Flex IOC (see Figure 4):

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. Use one of the following methods to take the Flex IOC offline:
   - Press and hold the corresponding online button on the craft interface. The green **OK** LED next to the button begins to blink. Hold the button down until the LED goes off.
   - Issue the following CLI command:

     ```
     user@host>request chassis fpc slot slot-number offline
     ```

     For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

3. Power off the firewall using the command **request system power-off**.

```
user@host# request system power-off
```

NOTE: Wait until a message appears on the console confirming that the services stopped.

4. Physically turn off the power and remove the power cables from the chassis.
5. If you have not already done so, remove the port modules installed in the Flex IOC. See "Removing an SRX5800 Firewall Port Module" on page 384.
6. Simultaneously turn both of the ejector handles counterclockwise to unseat the Flex IOC.
7. Grasp the handles and slide the Flex IOC straight out of the card cage halfway.
8. Place one hand around the front of the Flex IOC and the other hand under it to support it. Slide the Flex IOC completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

CAUTION: The weight of the Flex IOC is concentrated in the back end. Be prepared to accept the full weight—up to 13 lb (5.9 kg)—as you slide the Flex IOC out of the chassis.

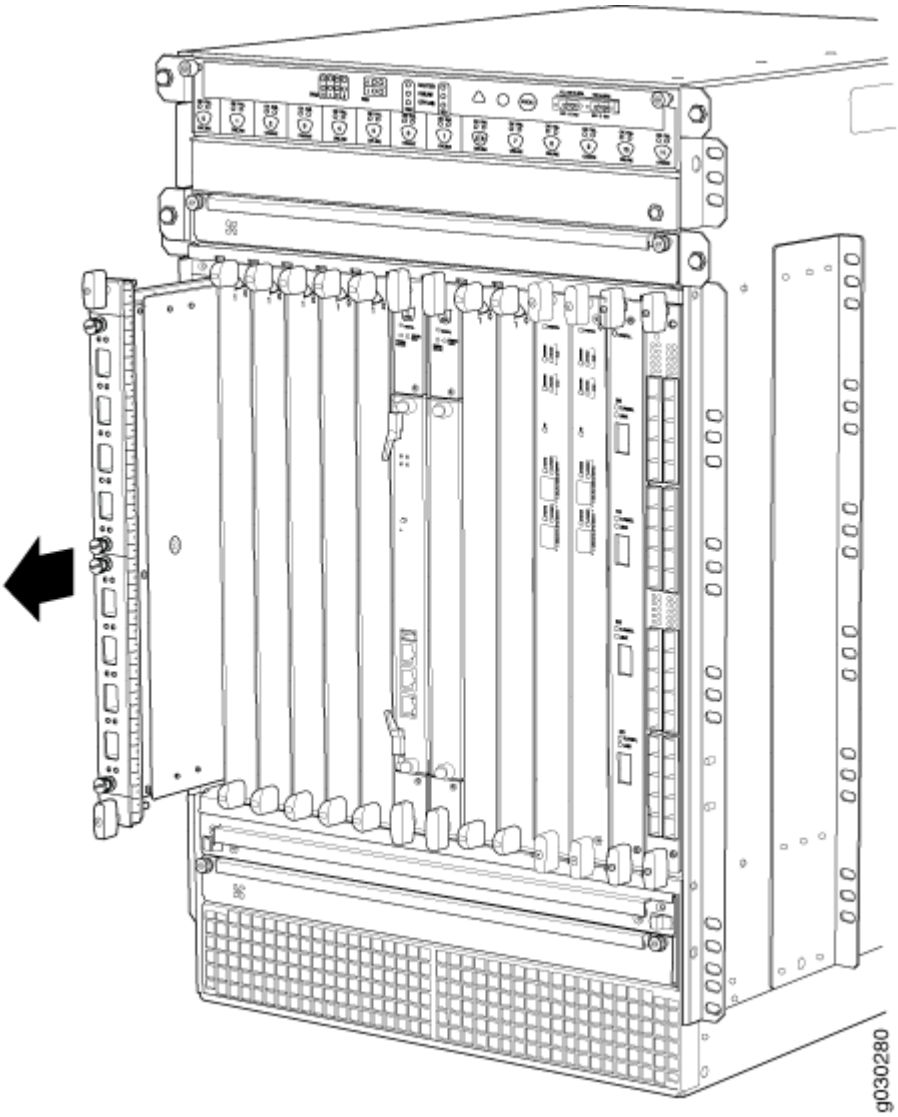
When the Flex IOC is out of the chassis, do not hold it by the ejector handles, bus bars, or edge connectors. They cannot support its weight.

Do not stack Flex IOCs on top of one another after removal. Place each one individually in an electrostatic bag or on its own antistatic mat on a flat, stable surface.

9. If you are not reinstalling a replacement card into the empty slot within a short time, install a blank panel over the slot to maintain proper airflow in the card cage.

CAUTION: After removing an IOC from the chassis, wait at least 30 seconds before reinserting it, removing an IOC from a different slot, or inserting an IOC into a different slot.

Figure 161: Removing a Flex IOC



Installing an SRX5800 Firewall Flex IOC

Before you begin to install a Flex IOC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Antistatic mat for the Flex IOC

NOTE: Your firewall must be running Junos version 9.5R1 or later in order to recognize Flex IOCs and port modules.

To install a Flex IOC (see Figure 5):

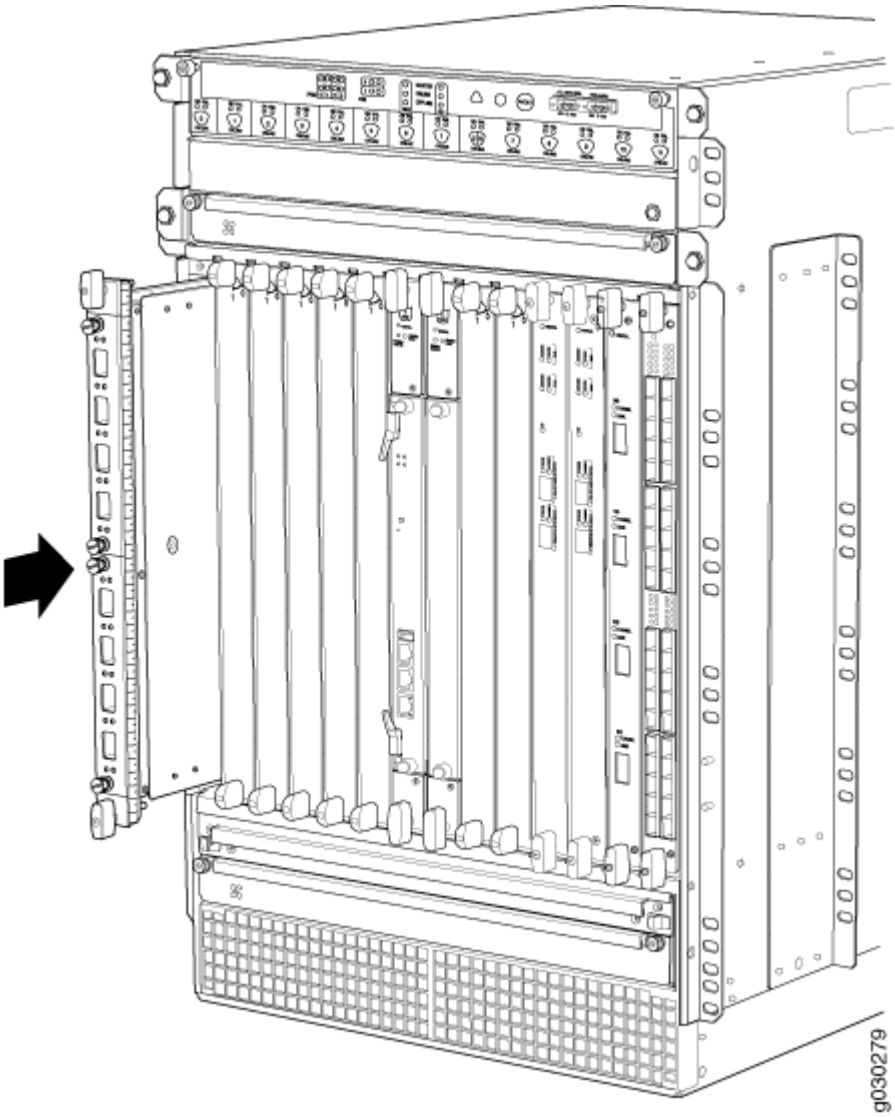
1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. Power off the firewall using the command **request system power-off**.

```
user@host# request system power-off
```

NOTE: Wait until a message appears on the console confirming that the services stopped.

3. Physically turn off the power and remove the power cables from the chassis.
4. Place the Flex IOC on an antistatic mat or remove it from its electrostatic bag.
5. Identify the slot on the firewall where you will install the Flex IOC.
6. If you have not already done so, remove the blank panel from the slot where you are installing the Flex IOC.
7. Orient the Flex IOC so that the faceplate faces you, the text on the card is right-side up, and the EMI strip is on the right-hand side.
8. Lift the Flex IOC into place and carefully align first the bottom and then the top of the card with the guides inside the card cage.
9. Slide the Flex IOC all the way into the card cage until you feel resistance.

Figure 162: Installing a Flex IOC



10. Grasp both ejector handles and rotate them clockwise simultaneously until the Flex IOC is fully seated.
11. Connect the power cables to the chassis.
12. Power on the firewall.
13. Use one of the following methods to bring the Flex IOC online:
    - Press and hold the corresponding online button on the craft interface until the green **OK** LED next to the button lights steadily, in about 5 seconds.

- Issue the following CLI command:

```
user@host>request chassis fpc slot slot-number online
```

For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

CAUTION: After the **OK** LED turns green, wait at least 30 seconds before removing the card again, removing a card from a different slot, or inserting a card in a different slot.

Replacing SRX5800 Firewall Port Modules

IN THIS SECTION

To replace a port module, perform the following procedures:

Removing an SRX5800 Firewall Port Module

Before you begin to remove a port module:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Phillips (+) number 1 screwdriver
- Replacement port module or blank panel
- Antistatic mat for the port module

- Rubber safety caps for the transceivers
- Dust covers to cover the ports

Port modules are installed in Flex IOCs in the firewall card cage. A port module weighs up to 1.6 lb (0.7 kg). Be prepared to accept its full weight when you remove or install a port module.

To remove a port module (see Figure 6):

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. Label the cables connected to each port on the port module so that you can later reconnect the cables to the correct ports.
3. Use one of the following methods to take the port module offline:
   - Insert a pointed tool into the **ONLINE** pinhole on the front panel of the port module to press the button behind it. Hold the button down until the **OK/FAIL** LED goes off.
   - Issue the following CLI command:

     ```
     user@host>request chassis fpc-slot slot-number pic-slot slot-number offline
     ```

     For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.
4. Power off the firewall.
5. Disconnect the cables from the port module. If the port module uses fiber-optic cable, immediately cover each transceiver and the end of each cable with a rubber safety cap. Arrange the disconnected cables in the cable management system to prevent the cables from developing stress points.

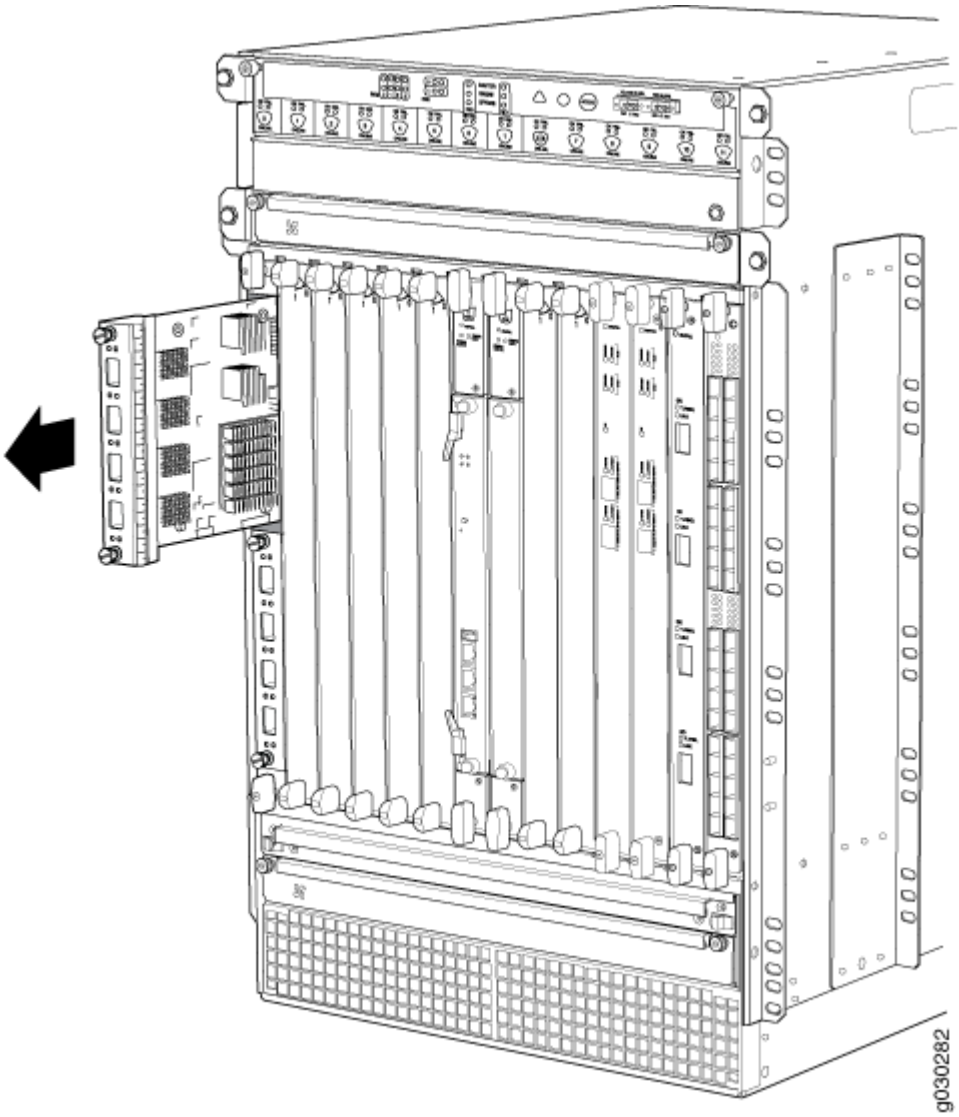
LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

CAUTION: Do not leave a fiber-optic transceiver uncovered, except when you are inserting or removing cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

6. Cover the ports on the port module with dust covers, if you remove the optical transceivers from the IOC.
7. Using the Phillips (+) number 1 screwdriver loosen the captive screws that retain the port module in its slot in the Flex IOC.
8. Grasp the captive screws and slide the port module straight out of the Flex IOC halfway.
9. Place one hand around the front of the port module and the other hand under it to support it. Slide the port module completely out of the Flex IOC, and place it on the antistatic mat or in the electrostatic bag.

Figure 163: Removing a Port Module



10. If you are not reinstalling a port module into the empty slot within a short time, install a blank panel over the slot to maintain proper airflow in the card cage.

> ⚠ **CAUTION**: After removing a port module from the chassis, wait at least 30 seconds before reinserting it, removing a port module from a different slot, or inserting a port module into a different slot.

Installing an SRX5800 Firewall Port Module

Before you begin to install a port module:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

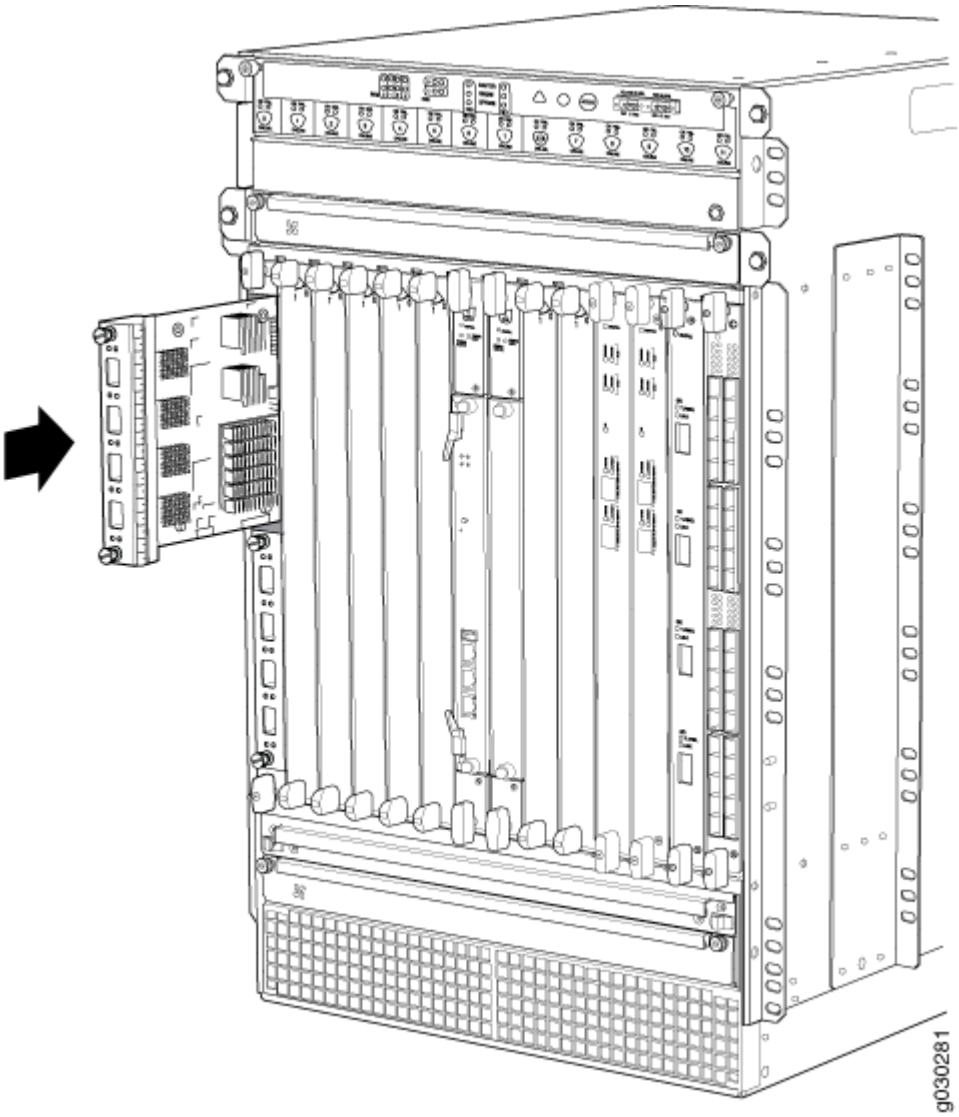
Ensure that you have the following available:

- ESD grounding strap
- Phillips (+) number 1 screwdriver
- Rubber safety caps for transceivers

To install a port module into a Flex IOC (see Figure 7):

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. Power off the firewall.
3. Place the port module on an antistatic mat or remove it from its electrostatic bag.
4. Verify that each fiber-optic transceiver is covered with a rubber safety cap. If it is not, cover the transceiver with a safety cap.
5. If necessary, remove the blank panel covering the slot in the Flex IOC where you are installing the port module.
6. Orient the port module so that the faceplate faces you.
7. Lift the port module into place and carefully align the top and bottom edges of the port module with the guides inside the Flex IOC.
8. Slide the port module all the way into the Flex IOC until it is fully seated.
9. Using the Phillips (+) number 1 screwdriver tighten both captive screws to secure the port module in the Flex IOC.

Figure 164: Installing a Port Module



10. If the port module uses fiber-optic interfaces, remove the rubber safety cap from each transceiver and cable.

> **LASER WARNING**: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

11. Insert the appropriate cables into the cable connector ports on each port module. Secure the cables so that they are not supporting their own weight. Place excess cable out of the way in a neatly coiled loop, using the cable management system. Placing fasteners on a loop helps to maintain its shape.

CAUTION: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

12. Power on the firewall.
13. Use one of the following methods to take the port module online:
    - Insert a pointed tool into the **ONLINE** pinhole on the front panel of the port module to press the button behind it. Hold the button down until the **OK/FAIL** LED at the opposite end of the front panel lights green steadily, in about 5 seconds.
    - Issue the following CLI command:

      ```
      user@host>request chassis fpc-slot slot-number pic-slot slot-number online
      ```

      For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

CAUTION: After the **OK/FAIL** LED turns green, wait at least 30 seconds before removing the port module again, removing a port module from a different slot, or inserting a port module in a different slot.

You can also verify that the port module is functioning correctly by issuing the `show chassis fpc` and `show chassis fpc pic-status` commands.

Replacing SRX5800 Firewall SPCs

IN THIS SECTION

To replace an SPC, perform the following procedures:

Removing an SRX5800 Firewall SPC

Before you begin to remove a SPC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Replacement SPC or blank panel
- Antistatic mat
- Rubber safety caps for transceivers

An SPC weighs up to 18.3 lb (8.3 kg). Be prepared to accept its full weight.

To remove an SPC (see Figure 8):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Power off the firewall using the command **request system power-off**.

```
user@host# request system power-off
```

NOTE: Wait until a message appears on the console confirming that the services stopped.

3. Physically turn off the power and remove the power cables from the chassis.

4. Label the cables connected to each port on the SPC so that you can later reconnect the cables to the correct ports.
5. Disconnect the cables from the SPC. If the SPC uses fiber-optic cable, immediately cover each transceiver and the end of each cable with a rubber safety cap. Arrange the disconnected cables in the cable management system to prevent the cables from developing stress points.

LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

CAUTION: Do not leave a fiber-optic transceiver uncovered, except when you are inserting or removing cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

CAUTION: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

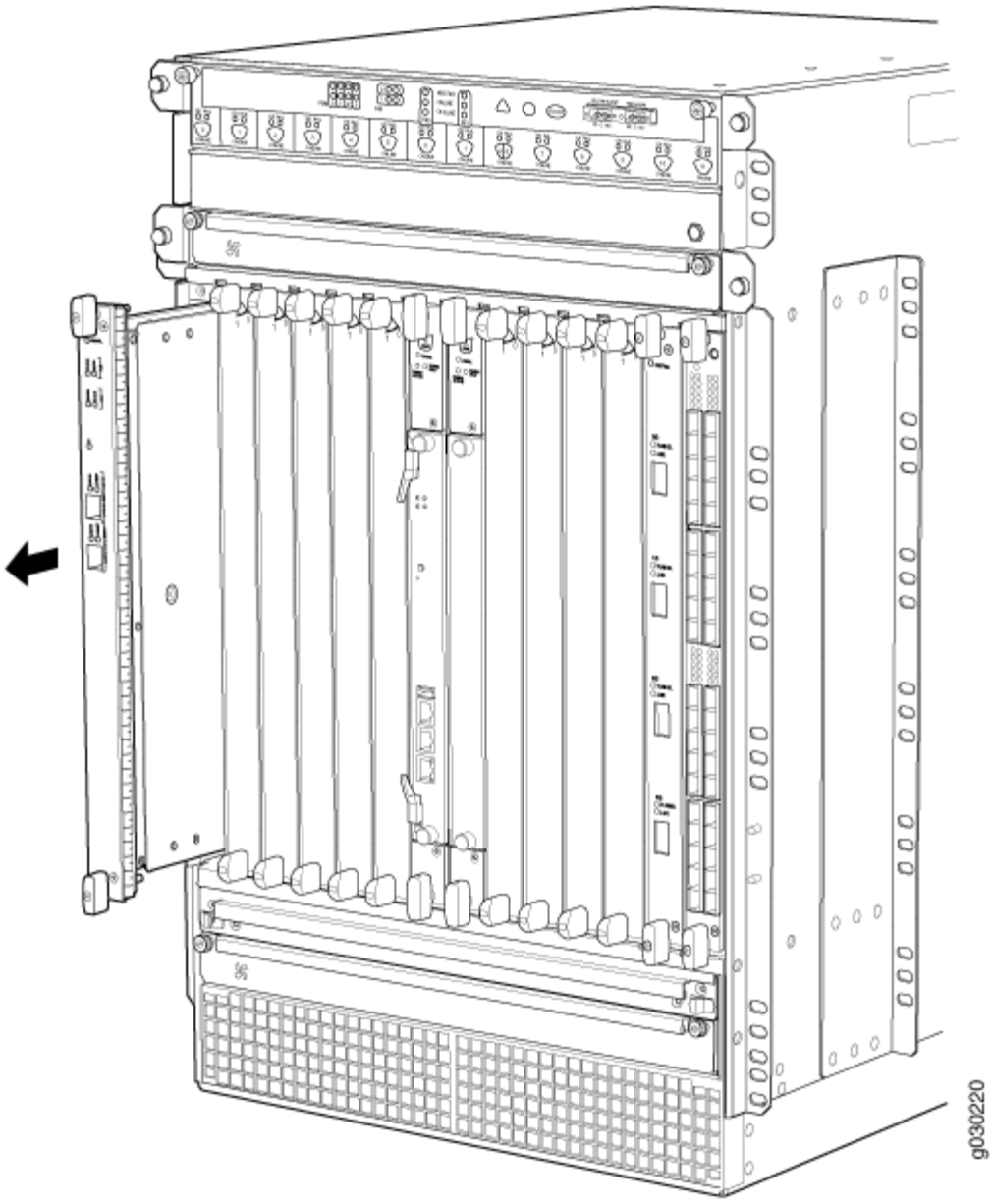
6. Simultaneously turn both of the ejector handles counterclockwise to unseat the SPC.
7. Grasp the handles and slide the SPC straight out of the card cage halfway.
8. Place one hand around the front of the SPC and the other hand under it to support it. Slide the SPC completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

CAUTION: The weight of the SPC is concentrated in the back end. Be prepared to accept the full weight—up to 18.3 lb (8.3 kg)—as you slide the SPC out of the chassis. When the SPC is out of the chassis, do not hold it by the ejector handles, bus bars, or edge connectors. They cannot support its weight.

Do not stack SPCs on top of one another after removal. Place each one individually in an electrostatic bag or on its own antistatic mat on a flat, stable surface.

9. If you are not reinstalling an SPC into the empty slot within a short time, install a blank panel over the slot to maintain proper airflow in the card cage.

Figure 165: Removing an SPC



Installing an SRX5800 Firewall SPC

Before you begin to install a SPC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Antistatic mat
- Rubber safety caps for transceivers

To install an SPC (see Figure 9):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Power off the firewall using the command **request system power-off**.

```
user@host# request system power-off
```

NOTE: Wait until a message appears on the console confirming that the services stopped.

3. Physically turn off the power and remove the power cables from the chassis.
4. Place the SPC on an antistatic mat or remove it from its electrostatic bag.
5. Identify the slot on the firewall where it will be installed.
6. Verify that each fiber-optic transceiver is covered with a rubber safety cap. If it does not, cover the transceiver with a safety cap.
7. Orient the SPC so that the faceplate faces you, the text on the card is right-side up, and the EMI strip is on the right-hand side.
8. Lift the SPC into place and carefully align first the bottom and then the top of the card with the guides inside the card cage.
9. Slide the SPC all the way into the card cage until you feel resistance.
10. Grasp both ejector handles and rotate them clockwise simultaneously until the SPC is fully seated.
11. If the SPC uses fiber-optic cable, remove the rubber safety cap from each transceiver and cable.

LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

12. Insert the appropriate cables into the cable connector ports on each SPC (see Figure 10). Secure the cables so that they are not supporting their own weight. Place excess cable out of the way in a neatly coiled loop, using the cable management system. Placing fasteners on a loop helps to maintain its shape.

> **CAUTION**: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

> **CAUTION**: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

13. Connect the power cables to the chassis.
14. Power on the firewall.
15. Verify that the SPC is functioning correctly by issuing the `show chassis fpc` and `show chassis fpc pic-status` commands.

Figure 166: Installing an SPC

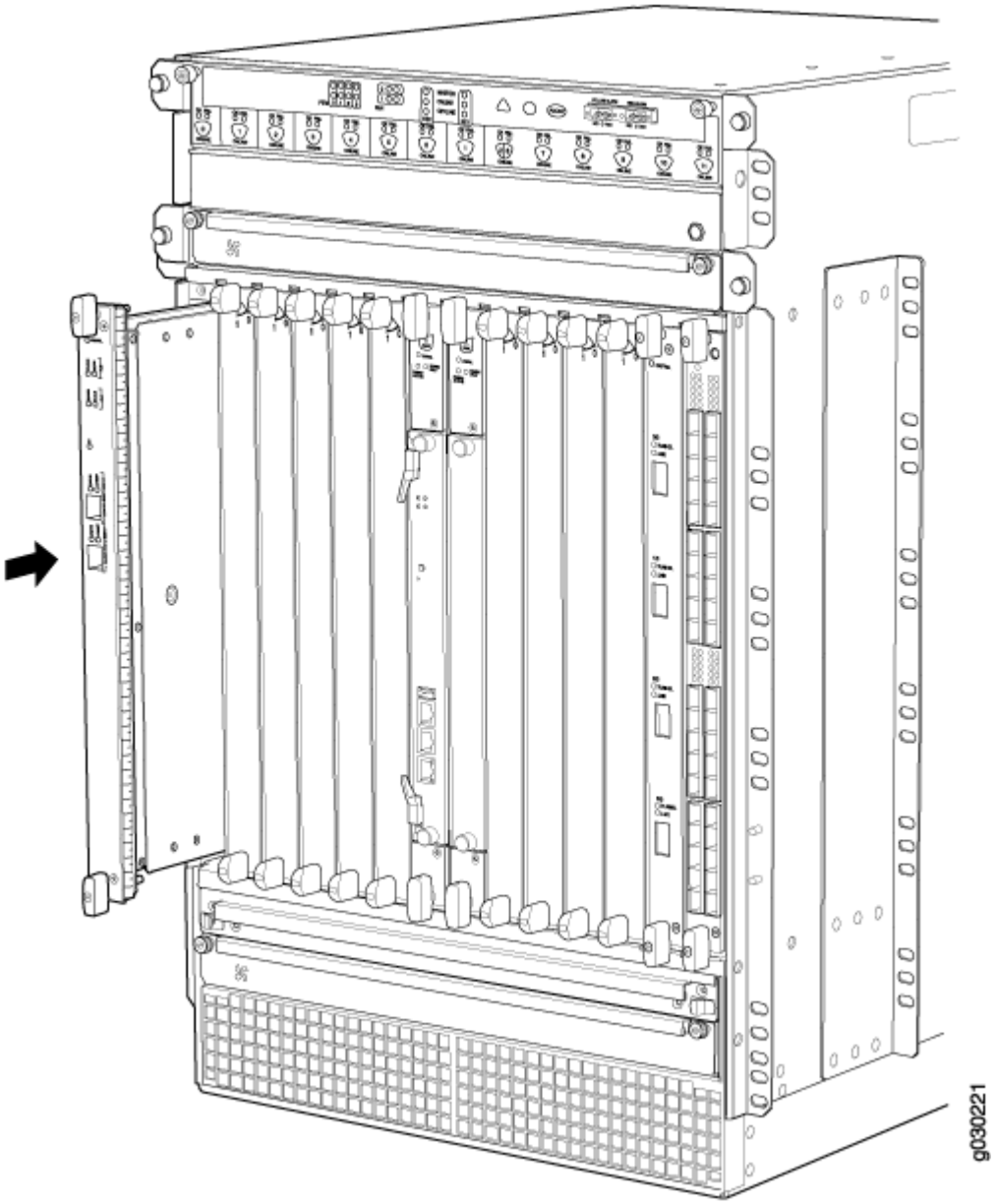
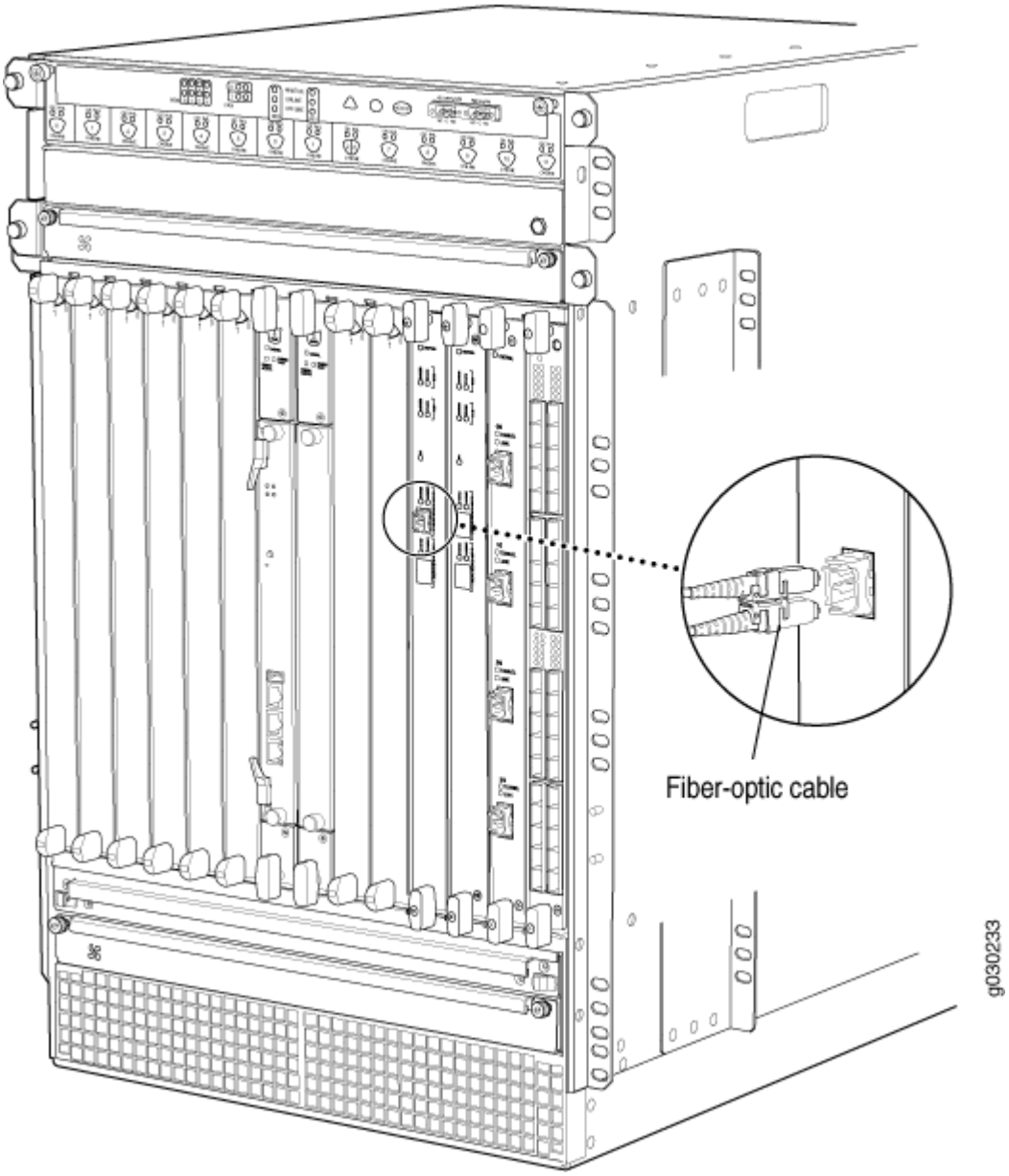


Figure 167: Attaching a Cable to an SPC



NOTE: To install additional SPCs in a firewall that is part of a chassis cluster, it must meet the following conditions.

- Each firewall must already have at least two SPCs installed in it.
- To add first-generation SRX5K-SPC-2-10-40 SPCs, both of the firewalls in the cluster must be running Junos OS Release 11.4R2S1, 12.1R2, or later.

- To add second-generation SRX5K-SPC-4-15-320 SPCs, both of the firewalls in the cluster must be running Junos OS Release 12.1X44-D10, or later.
- To add next-generation SRX5K-SPC3 SPCs, both of the firewalls in the cluster must be running Junos OS Release 18.2R1-S1, or later.
- You must install SPCs of the same type and in the same slots in both of the firewalls in the cluster. Both firewalls in the cluster must end up with the same physical configuration of SPCs.
- If you are only adding first-generation SRX5K-SPC-2-10-40 SPCs to the chassis, you must install them so that the new SPCs are not the SPCs with the lowest-numbered slots in the chassis. For example, if the chassis already has two SPCs with one SPC each in slots 2 and 3, you cannot install additional SPCs in slots 0 or 1 using this procedure.
- If you are adding second-generation SRX5K-SPC-4-15-320 SPCs to the chassis, you must install the new SPCs so that a second-generation SRX5K-SPC-4-15-320 SPC is the SPC in the original lowest-numbered slot. For example, if the chassis already has two first-generation SPCs installed in slots 2 and 3, you must install SRX5K-SPC-4-15-320 SPCs in slots 0 or 1. You will need to make sure that an SRX5K-SPC-4-15-320 SPC is installed in the slot providing central point (CP) functionality so that the CP functionality is performed by an SRX5K-SPC-4-15-320 SPC.
- If you are adding next-generation SRX5K-SPC3 SPCs to the chassis, you must install the new SPCs so that a next-generation SRX5K-SPC3 SPC is the SPC in the original lowest-numbered slot. For example, if the chassis already has two second-generation SPCs installed in slots 2 and 3, you must install SRX5K-SPC3 SPCs in slots 0 or 1. You will need to make sure that an SRX5K-SPC3 SPC is installed in the slot providing central point (CP) functionality so that the CP functionality is performed by an SRX5K-SPC3 SPC.

  NOTE: Your firewall cannot have a mix of SRX5K-SPC-2-10-40 SPCs and SRX5K-SPC3 SPCs, but starting with Junos OS release 18.2R2 and then 18.4R1 but not 18.3R1 you can have a mix of SRX5K-SPC-4-15-320 SPCs and SRX5K-SPC3 SPCs.

- If you are adding the second-generation SRX5K-SPC-4-15-320 SPCs or the next-generation SRX5K-SPC3 SPCs to a firewall, the firewall must already be equipped with high-capacity power supplies and fan trays, and the high-capacity air filters. See "Upgrading an SRX5800 Firewall from Standard-Capacity to High-Capacity Power Supplies" on page 329 for more information.

During this installation procedure, you must shut down both devices, one at a time.

Replacing SPCs in an Operating SRX5400, SRX5600, or SRX5800 Firewalls Chassis Cluster

If your Firewall is part of an operating chassis cluster, you can replace the first-generation SRX5K-SPC-2-10-40 SPCs with the second generation SRX5K-SPC-4-15-320 SPCs or the first and second generation SPCs with the next generation SRX5K-SPC3s by incurring a minimum downtime on your network.

NOTE: SRX5K-SPC-2-10-40 SPC is not supported on SRX5400 Firewall.

To replace SPCs in a firewall that is part of a chassis cluster, it must meet the following conditions:

- Each firewall must have at least one SPC installed. The installation may warrant additional SPCs if the number of sessions encountered is greater than the session limit of one SPC.
- If the chassis cluster is operating in active-active mode, you must transition it to active-passive mode before using this procedure. You transition the cluster to active-passive mode by making one node primary for all redundancy groups.
- To replace first-generation SRX5K-SPC-2-10-40 SPCs, both of the firewalls in the cluster must be running Junos OS Release 11.4R2S1, 12.1R2, or later.
- To replace second-generation SRX5K-SPC-4-15-320 SPCs, both of the firewalls in the cluster must be running Junos OS Release 12.1X44-D10, or later.
- To replace next-generation SRX5K-SPC3 SPCs, both of the firewalls in the cluster must be running Junos OS Release 18.2R1-S1, or later.
- You must install SPCs of the same type and in the same slots in both of the firewalls in the cluster. Both firewalls in the cluster must have the same physical configuration of SPCs.
- If you are replacing an existing SRX5K-SPC-2-10-40 SPC with an SRX5K-SPC-4-15-320 SPC, you must install the new SPC in the lowest-numbered slot. For example, if the chassis already has SPCs installed in slots 2 and 3, then you must replace the SPC in slot 2 first. This ensures that the central point (CP) functionality is performed by an SRX5K-SPC-4-15-320 SPC.
- If you are adding SRX5K-SPC3 SPCs for the first time to the chassis which has a mix of other SPCs, you must install the first SRX5K-SPC3 in the lowest-numbered slot first and the other SPX5K-SPC3s can be installed in any available slot. For example, if the chassis already has two SRX5K-SPC-4-15-320 SPCs installed in slots 2 and 3, you must install SRX5K-SPC3 SPCs in slots 0 or 1. You will need to make sure that an SRX5K-SPC3 SPC is installed in the slot providing central point (CP) functionality so that the CP functionality is performed by an SRX5K-SPC3 SPC.

> **NOTE**: Your firewall cannot have a mix of SRX5K-SPC-2-10-40 SPCs and SRX5K-SPC3 SPCs, but starting with Junos OS release 18.2R2 and then 18.4R1 but not 18.3R1 you can have a mix of SRX5K-SPC-4-15-320 SPCs and SRX5K-SPC3 SPCs.

If you are adding SRX5K-SPC3s to the chassis which has only SRX5K-SPC3s, the new SRX5K-SPC3 can be installed in any available slot.

- If you are adding the SRX5K-SPC-4-15-320 SPCs or the SRX5K-SPC3 SPCs to a firewall, the firewall must already be equipped with high-capacity power supplies and fan trays, and the high-capacity air filters. See *Upgrading an SRX5600 Firewall from Standard-Capacity to High-Capacity Power Supplies* or *Upgrading an SRX5600 Firewall from Standard-Capacity to High-Capacity Power Supplies* for more information.

If your installation does not meet these criteria, use the procedure in *Installing an SRX5400 Firewall SPC*, or *Installing an SRX5600 Firewall SPC*, or "Installing an SRX5800 Firewall SPC" on page 391 to install SPCs in your firewall.

> **NOTE**: During this installation procedure, you must shut down both devices, one at a time. During the period when one device is shut down, the remaining device operates without a backup. If that remaining device fails for any reason, you incur network downtime until you restart at least one of the devices.

To replace SPCs in an Firewall cluster:

1. Use the console port on the Routing Engine to establish a CLI session with one of the devices in the cluster.
2. Use the **show chassis cluster status** command to determine which firewall is currently primary, and which firewall is secondary, within the cluster.
3. If the device with which you established the CLI session in Step 2 is not the secondary node in the cluster, use the console port on the device that is the secondary node to establish a CLI session.
4. Use the **show chassis fpc pic-status** command to check the status of all the cards on both the nodes.
5. Power off the firewall by using one of the following commnads:
   - Use the **request system power-off** command to shut down the firewall if it has the Routing Engine SRX5K-RE-13-20 or the Routing Engine SRX5K-RE-1800X4 installed.
   - Use the **request vmhost power-off** command to shut down the firewall if it has the Routing Engine SRX5K-RE3-128G installed.

NOTE: Wait until a message appears on the console confirming that the services stopped.

6. Wait for the secondary firewall to shut down completely and than remove the power cables from the chassis.
7. Remove the SPC from the powered-off firewall using the procedure in *Removing an SRX5400 Firewall SPC*, or *Removing an SRX5600 Firewall SPC*, or "Removing an SRX5800 Firewall SPC" on page 391.
8. Install the new SPC or SPCs in the powered-off Firewall using the procedure in *Installing an SRX5400 Firewall SPC*, or *Installing an SRX5600 Firewall SPC*, or "Installing an SRX5800 Firewall SPC" on page 391.
9. Insert the power cables to the chassis and power on the secondary firewall and wait for it to finish starting.
10. Reestablish the CLI session with the secondary node device.
11. Use the **show chassis fpc pic-status** command to make sure that all of the cards in the secondary node chassis are back online.
12. Use the **show chassis cluster status** command to make sure that the priority for all redundancy groups is greater than zero.
13. Use the console port on the device that is the primary node to establish a CLI session.
14. In the CLI session for the primary node device, use the **request chassis cluster failover** command to fail over each redundancy group that has an ID number greater than zero.
15. Power off the firewall by using one of the following commnads. This action causes redundancy group 0 to fail over onto the other firewall, making it the active node in the cluster.
    - Use the **request system power-off** command to shut down the firewall if it has the Routing Engine SRX5K-RE-13-20 or the Routing Engine SRX5K-RE-1800X4 installed.
    - Use the **request vmhost power-off** command to shut down the firewall if it has the Routing Engine SRX5K-RE3-128G installed.

NOTE: Wait until a message appears on the console confirming that the services stopped.

16. Repeat Step 7 and Step 8 to replace or install SPCs in the powered-off firewall.
17. Power on the firewall and wait for it to finish starting.
18. Use the **show chassis fpc pic-status** command on each node to confirm that all cards are online and both firewalls are operating correctly.
19. Use the **show chassis cluster status** command to make sure that the priority for all redundancy groups is greater than zero.

In-Service Hardware Upgrade for SRX5K-SPC3 in a Chassis Cluster

If your device is part of a chassis cluster and does not have a mix of SPCs but has only SRX5K-SPC3 SPCs, you can only install additional SRX5K-SPC3 (SPC3) using the In-Service Hardware Upgrade (ISHU) procedure and avoid network downtime.

NOTE: This ISHU procedure will not replace any existing Services Processing Cards (SPC), it will guide you to install an additional SPC3 card in a chassis cluster.

NOTE: We strongly recommend that you perform the ISHU during a maintenance window, or during the lowest possible traffic as the secondary node is not available at this time.

To install SPC3s in a firewall that is part of a chassis cluster using the ISHU procedure, the following conditions have to be met:

- Each firewall must have at least one SPC3 installed.
- Starting in Junos OS Release 19.4R1, ISHU for SRX5K-SPC3 is supported on all SRX5000 line of devices chassis cluster:
  - If the chassis has only one SPC3, you can only install one more SPC3 by using the ISHU procedure.
  - If the chassis already has two SPC3 cards, you cannot install any more SPC3 cards by using the ISHU procedure.
  - If the chassis already has three or more SPC3 cards, you can install additional SPC3 cards by using the ISHU procedure.
- Installing SPC3s to the chassis cluster must not change the central point (CP) functionality mode from Combo CP mode to Full CP mode.

  When there are two or less than two SPC3s in the chassis, the CP mode is Combo CP mode. More than two SPC3s in the chassis, the CP mode is Full CP mode.
- If the chassis cluster is operating in active-active mode, you must transition it to active-passive mode before using this procedure. You transition the cluster to active-passive mode by making one node primary for all redundancy groups.
- When you are adding a new SPC3 to the chassis, it must be installed in the higher numbered slot than the first installed SPC3 in the chassis.

- The firewall must already be equipped with high-capacity power supplies and fan trays, and the high-capacity air filters. See *Upgrading an SRX5600 Firewall from Standard-Capacity to High-Capacity Power Supplies* or *Upgrading an SRX5600 Firewall from Standard-Capacity to High-Capacity Power Supplies* for more information.

During this installation procedure, you must shut down both devices, one at a time. During the period when one device is shut down, the other device operates without a backup. If that other device fails for any reason, you incur network downtime until you restart at least one of the devices.

To add SPC3s in an Firewall cluster without incurring downtime:

1. Use the console port on the Routing Engine to establish a CLI session with one of the devices in the cluster.
2. Use the **show chassis cluster status** command to determine which firewall is currently primary, and which firewall is secondary, within the cluster.
3. If the device with which you established the CLI session in Step 2 is not the secondary node in the cluster, use the console port on the device that is the secondary node to establish a CLI session.
4. In the CLI session of the secondary firewall:
   a. Use the **show chassis fpc pic-status** command to check the status of all the cards on both the nodes.
   b. Use the **request vmhost power-off** command to shut down the firewall if it has the Routing Engine SRX5K-RE3-128G installed else use the **request system power-off** command.
5. Wait for the secondary firewall to shut down completely and than remove the power cables from the chassis.
6. Install the new SPC3 or SPC3s in the powered-off firewall using the procedure in *Installing an SRX5400 Firewall SPC*, or *Installing an SRX5600 Firewall SPC*, or "Installing an SRX5800 Firewall SPC" on page 391.
7. Insert the power cables to the chassis and power on the secondary firewall and wait for it to finish starting.
8. Reestablish the CLI session with the secondary node device.
9. Use the **show chassis fpc pic-status** command to make sure that all of the cards in the secondary node chassis are back online.
10. Use the **show chassis cluster status** command to make sure that the priority for all redundancy groups is greater than zero.
11. Use the console port on the device that is the primary node to establish a CLI session.
12. In the CLI session of the primary node:
    a. Use the **request chassis cluster failover** command to fail over each redundancy group that has an ID number greater than zero.

b. Use the **request vmhost power-off** command to shut down the firewall if it has the Routing Engine SRX5K-RE3-128G installed, else use the **request system power-off** command. This action causes redundancy group 0 to fail over onto the other firewall, making it the active node in the cluster.

13. Repeat Step 6 to install SPC3s in the powered-off firewall.
14. Power on the firewall and wait for it to finish starting.
15. Use the **show chassis fpc pic-status** command on each node to confirm that all cards are online and both firewalls are operating correctly.
16. Use the **show chassis cluster status** command to make sure that the priority for all redundancy groups is greater than zero.

Maintaining MICs and Port Modules on the SRX5800 Firewall

IN THIS SECTION

Purpose

For optimum firewall performance, verify the condition of the MICs installed in MPCs, and port modules installed in Flex IOCs.

Action

On a regular basis:

- Check the LEDs on MIC and port modules faceplates. The meaning of the LED states differs for various port modules. If the Flex IOC that houses the port modules detects a port modules failure, the Flex IOC generates an alarm message to be sent to the Routing Engine.
- Issue the CLI `show chassis fpc pic-status` command. The port module and MIC slots in an FPC are numbered from **0** through **1**, bottom to top:

```
user@host> show chassis fpc pic-status
Slot 0   Online       SRX5k SPC
```

```
  PIC 0  Online       SPU Cp-Flow
  PIC 1  Online       SPU Flow
Slot 3   Online       SRX5k DPC 4X 10GE
  PIC 0  Online       1x 10GE(LAN/WAN) RichQ
  PIC 1  Online       1x 10GE(LAN/WAN) RichQ
  PIC 2  Online       1x 10GE(LAN/WAN) RichQ
  PIC 3  Online       1x 10GE(LAN/WAN) RichQ
Slot 5   Online       SRX5k FIOC
  PIC 0  Online       16x 1GE TX
  PIC 1  Online       4x 10GE XFP
```

For further description of the output from the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

Replacing SRX5800 Firewall MICs

IN THIS SECTION

To replace an MIC, perform the following procedures:

Removing an SRX5800 Firewall MIC

The MICs are located in the MPCs installed in the front of the firewall. A MIC weighs less than 2 lb (0.9 kg).

Before you begin to remove a MIC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Antistatic mat
- Replacement MIC or blank panel

- Rubber safety caps for transceivers

To remove a MIC:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface to receive the MIC.
2. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
3. Power off the firewall.
4. Label the cables connected to the MIC so that you can later reconnect each cable to the correct MIC.
5. Disconnect the cables from the MIC. If the MIC uses fiber-optic cable, immediately cover each transceiver and the end of each cable with a rubber safety cap.

   LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

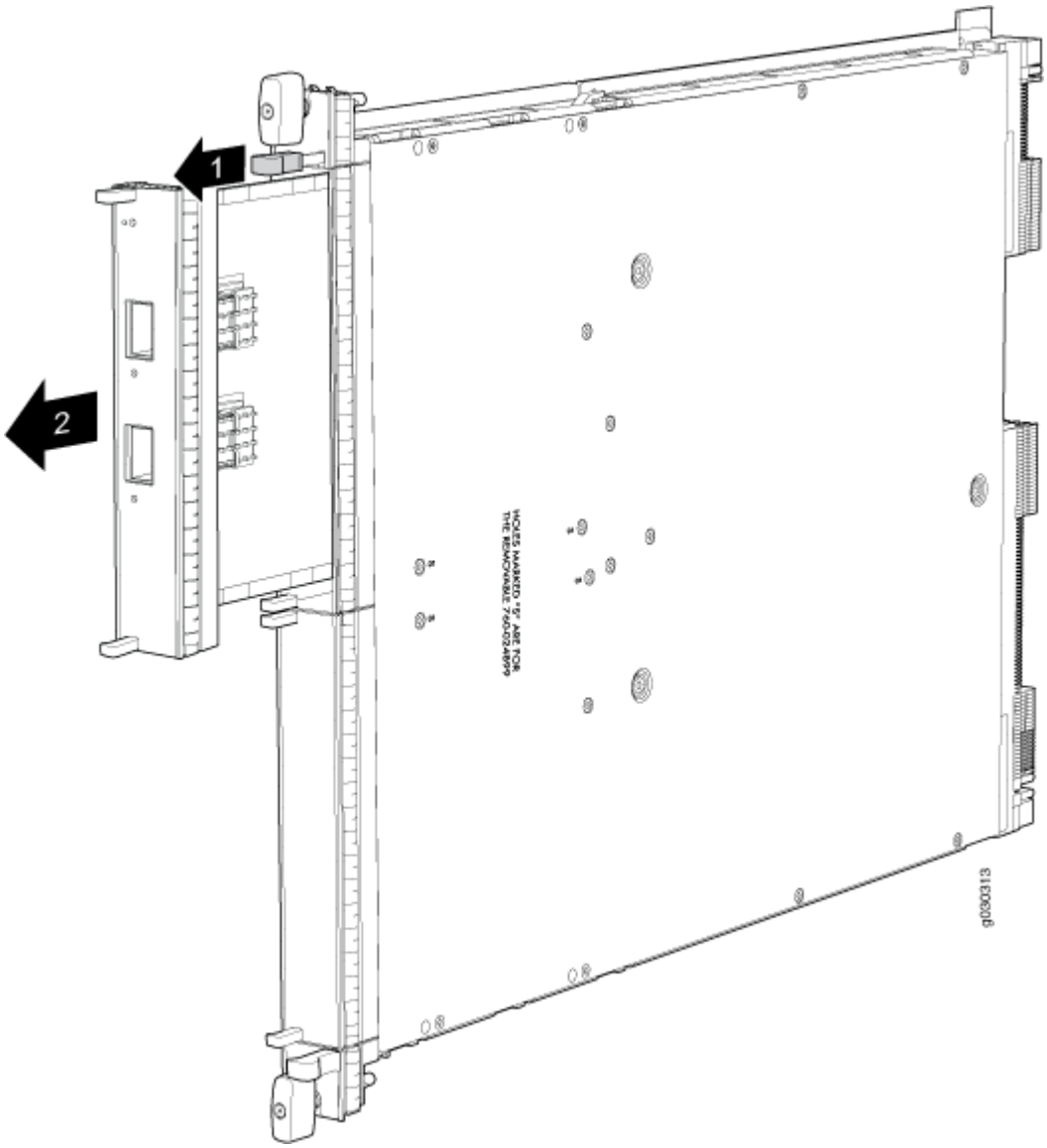
   CAUTION: Do not leave a fiber-optic transceiver uncovered, except when you are inserting or removing cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

6. Arrange the cable to prevent it from dislodging or developing stress points. Secure the cable so that it is not supporting its own weight as it hangs to the floor. Place excess cable out of the way in a neatly coiled loop.

   CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

7. On the MPC, pull the ejector knob that is adjacent to the MIC you are removing away from the MPC faceplate. The ejector knob is located between the MIC and the rotational knob that retains the MPC in the firewall card cage. Pulling the ejector knob unseats the MIC from the MPC and partially ejects it. See Figure 11.

Figure 168: Removing a MIC



8. Grasp the handles on the MIC faceplate, and slide the MIC out of the MPC card carrier. Place it in the electrostatic bag or on the antistatic mat.
9. If you are not reinstalling a MIC into the emptied MIC slot within a short time, install a blank MIC panel over the slot to maintain proper airflow in the MPC card cage.

Installing an SRX5800 Firewall MIC

Before you begin to install a MIC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

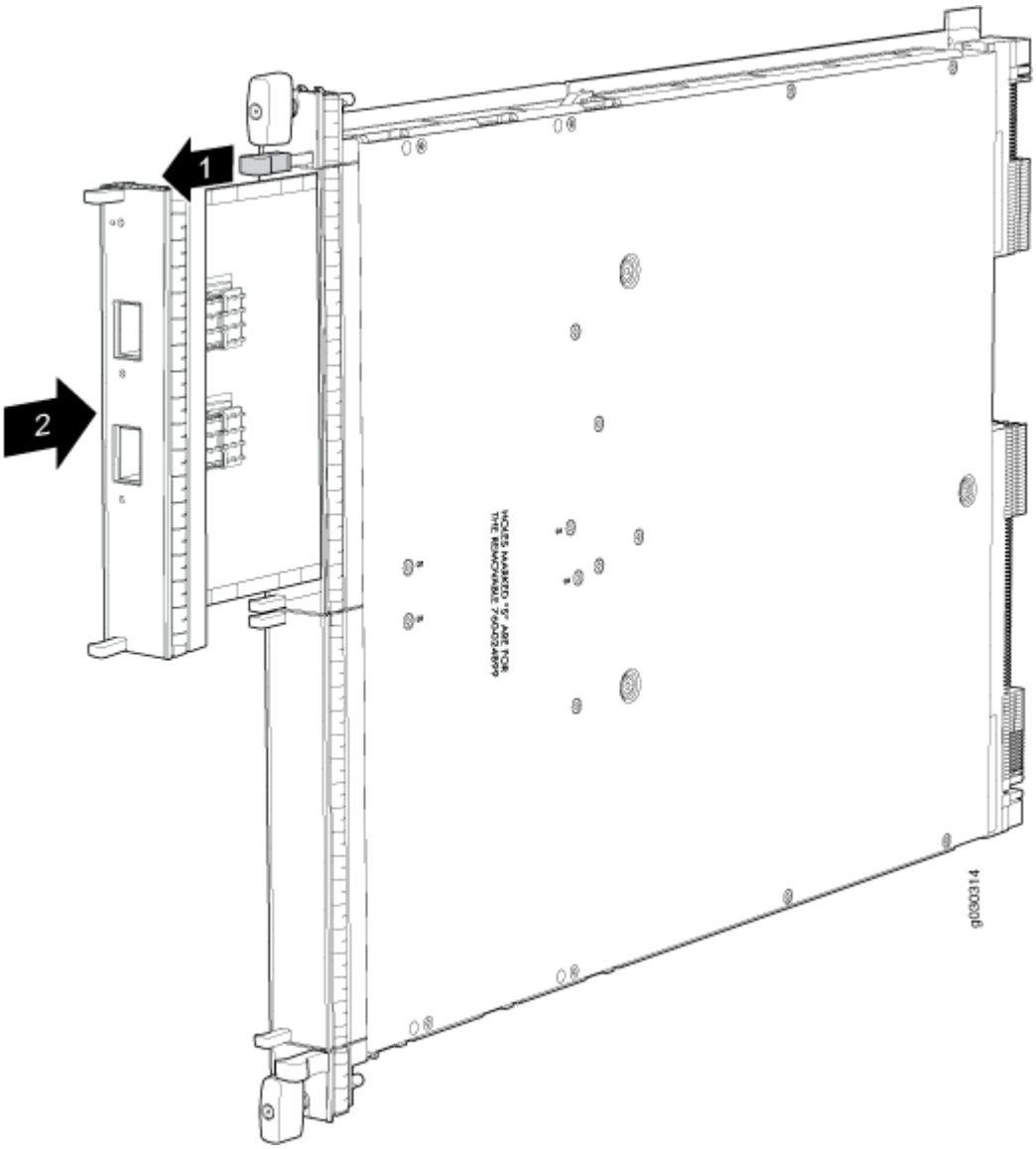
- ESD grounding strap
- Rubber safety caps for transceivers

> **NOTE**: If your firewall is part of a chassis cluster, you may be able to install MICs in the firewalls in the cluster without incurring downtime on your network. See Installing MPCs and MICs in an Operating SRX5800 Firewall Chassis Cluster for more information.

To install a MIC:

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. If you have not already done so, power off the firewall.
3. If the MIC uses fiber-optic cable, verify that a rubber safety cap is over each transceiver on the faceplate. Install a cap if necessary.
4. On the MPC, pull the ejector knob that is adjacent to the MIC you are installing away from the MPC faceplate. The ejector knob is located between the MIC and the rotational knob that retains the MPC in the firewall card cage. See Figure 12.

Figure 169: Installing a MIC



5. Align the rear of the MIC with the guides located at the corners of the MIC slot.
6. Slide the MIC into the MPC until it is firmly seated in the MPC. The ejector knob will automatically move in towards the faceplate to lock the MIC in position as it seats.

   If the MIC does not seat properly in the slot, pull the ejector knob all the way out and try again to seat the MIC. The MIC will not seat properly unless the ejector knob is all the way when you start to insert the MIC.

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

7. After the MIC is seated in its slot, verify that the ejector knob is engaged by pushing it all the way in toward the MPC faceplate.
8. If the MIC uses fiber-optic cable, remove the rubber safety cap from each transceiver and the end of each cable.

LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

CAUTION: Do not leave a fiber-optic transceiver uncovered, except when you are inserting or removing cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

9. Insert the appropriate cables into the cable connectors on the MIC.
10. Arrange each cable to prevent the cable from dislodging or developing stress points. Secure the cable so that it is not supporting its own weight as it hangs to the floor. Place excess cable out of the way in a neatly coiled loop.

CAUTION: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

11. Power on the firewall. The OK LED on the power supply faceplate should blink, then light steadily.
12. Verify that the MPC and MICs are functioning correctly by issuing the `show chassis fpc` and `show chassis fpc pic-status` commands.

Replacing SRX5800 Firewall MPCs

IN THIS SECTION

To replace an MPC, perform the following procedures:

Removing an SRX5800 Firewall MPC

An MPC installs vertically in the front of the firewall. A fully configured MPC can weigh up to 18.35 lb (8.3 kg). Be prepared to accept its full weight.

Before you begin to remove a MPC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Replacement MPC or blank panel
- Antistatic mat
- Rubber safety caps for transceivers

To remove an MPC:

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. Power off the firewall.
3. Label the cables connected to each MIC on the MPC so that you can later reconnect the cables to the correct MICs.
4. Disconnect the cables from the MICs installed in the MPC.

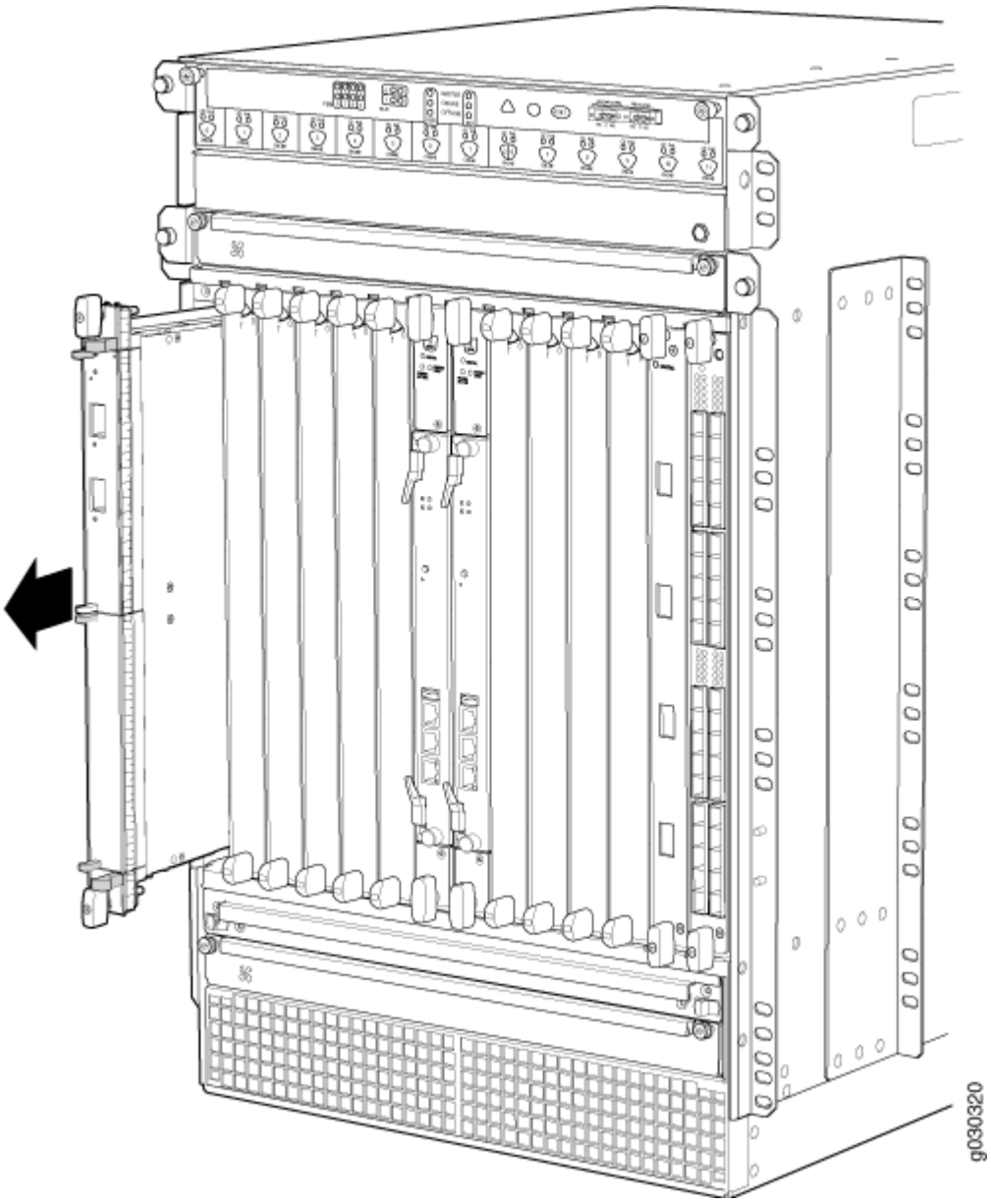
LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

CAUTION: Do not leave a fiber-optic transceiver uncovered, except when inserting or removing a cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

5. If a MIC uses fiber-optic cable, immediately cover each transceiver and the end of each cable with a rubber safety cap.
6. Arrange the disconnected cables in the cable management brackets to prevent the cables from developing stress points.
7. Simultaneously turn both the ejector handles counterclockwise to unseat the MPC.
8. Grasp the handles, and slide the MPC straight out of the card cage halfway. See Figure 13.

Figure 170: Removing an MPC



9. Place one hand around the front of the MPC (the MIC housing) and the other hand under it to support it. Slide the MPC completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

> ⚠ **CAUTION**: The weight of the MPC is concentrated in the back end. Be prepared to accept the full weight—up to 18.35 lb (8.3 kg)—as you slide the MPC out of the chassis.

When the MPC is out of the chassis, do not hold it by the ejector handles, bus bars, or edge connectors. They cannot support its weight.

Do not stack MPCs on top of one another after removal. Place each one individually in an electrostatic bag or on its own antistatic mat on a flat, stable surface.

10. If necessary, remove each installed MIC from the MPC. See "Removing an SRX5800 Firewall MIC" on page 405.
11. After you remove each MIC, immediately place it on an antistatic mat or in an electrostatic bag.
12. If you are not reinstalling an MPC into the emptied line card slots within a short time, install a blank panel over each slot to maintain proper airflow in the card cage.

Installing an SRX5800 Firewall MPC

An MPC installs vertically in the front of the firewall. A fully configured MPC can weigh up to 18.35 lb (8.3 kg). Be prepared to accept its full weight.

NOTE: If your firewall is part of a chassis cluster, you may be able to install MPCs in the firewalls in the cluster without incurring downtime on your network. See Installing MPCs and MICs in an Operating SRX5800 Firewall Chassis Cluster for more information.

Before you begin to install a MPC:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Antistatic mat
- Rubber safety caps for transceivers

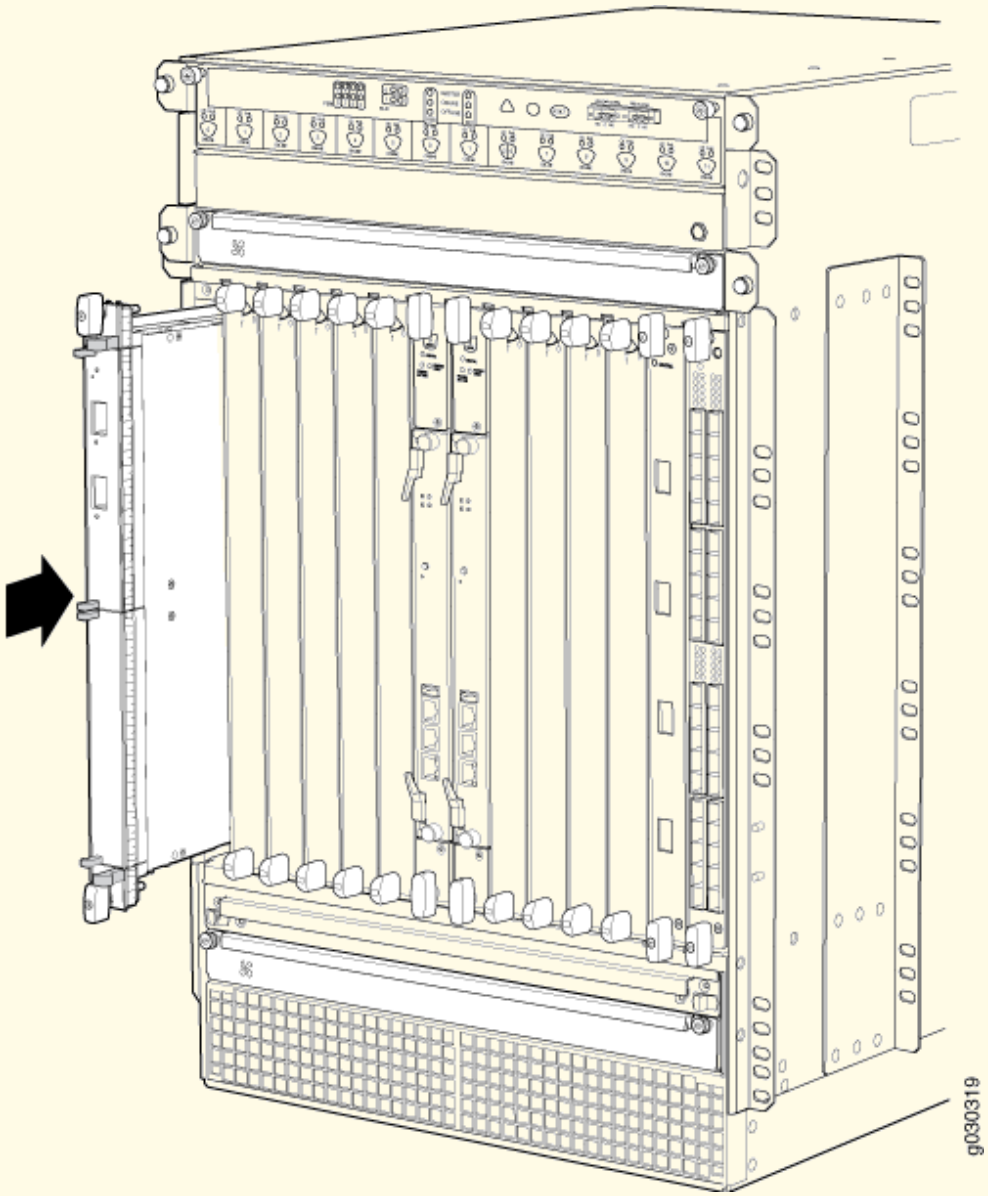
To install an MPC:

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. If you have not already done so, power off the firewall.
3. Place the MPC on an antistatic mat.
4. Take each MIC to be installed in the replacement MPC out of its electrostatic bag, and identify the slot on the MPC where it will be connected.
5. Verify that each fiber-optic MIC has a rubber safety cap covering the MIC transceiver. If it does not, cover the transceiver with a safety cap.

6. Install each MIC into the appropriate slot on the MPC. See "Installing an SRX5800 Firewall MIC" on page 405.
7. Locate the slot in the card cage in which you plan to install the MPC.
8. Orient the MPC so that the faceplate faces you.
9. Lift the MPC into place, and carefully align the sides of the MPC with the guides inside the card cage. See Figure 14.

> **CAUTION**: When the MPC is out of the chassis, do not hold it by the ejector handles, bus bars, or edge connectors. They cannot support its weight.

Figure 171: Installing an MPC



10. Slide the MPC all the way into the card cage until you feel resistance.
11. Grasp both ejector handles, and rotate them clockwise simultaneously until the MPC is fully seated.
12. If any of the MICs on the MPC connect to fiber-optic cable, remove the rubber safety cap from each transceiver and cable.

LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

13. Insert the appropriate cable into the cable connector ports on each MIC on the MPC. Secure the cables so that they are not supporting their own weight. Place excess cable out of the way in a neatly coiled loop, using the cable management system. Placing fasteners on a loop helps to maintain its shape.

    CAUTION: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

    CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

14. Power on the firewall. The OK LED on the power supply faceplate should blink, then light steadily.
15. Verify that the MPC is functioning correctly by issuing the `show chassis fpc` and `show chassis fpc pic-status` commands.

Maintaining the SRX5800 Cables and Connectors

IN THIS SECTION

Maintaining SRX5800 Firewall Network Cables

IN THIS SECTION

Purpose

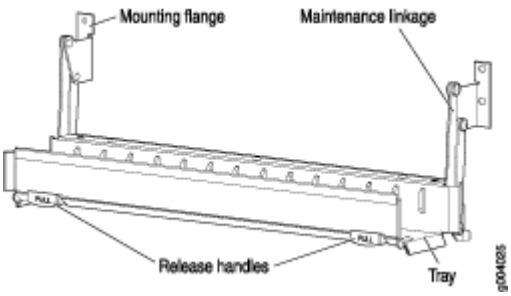
For optimum firewall performance, verify the condition of the network cables.

Action

On a regular basis:

- Use the cable manager to support cables and prevent cables from dislodging or developing stress points (see Figure 172 on page 418).

Figure 172: Cable Manager



- Place excess cable out of the way in the cable manager. Do not allow fastened loops of cable to dangle from the connector or cable manager, because this stresses the cable at the fastening point. Putting fasteners on the loops helps to maintain their shape.
- 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 both ends of the cables to identify them.

The following guidelines apply specifically to fiber-optic cables:

- When you unplug a fiber-optic cable, always place a rubber safety plug over the transceiver on the IOC or port module faceplate and on the end of the cable.
- Anchor fiber-optic cables to avoid stress on the connectors. Be sure to secure fiber-optic cables so that they do not support their own weight as they hang to the floor. Never let fiber-optic cable hang free from the connector.
- 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.
- Frequent plugging and unplugging of fiber-optic cable into and out of optical instruments can cause damage to the instruments that is expensive to repair. Instead, attach 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.
- Keep fiber-optic cable connections clean. Small microdeposits of oil and dust in the canal of the transceiver or cable connector could cause loss of light, reducing signal power and possibly causing intermittent problems with the optical connection.

  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 clean an optical transceiver, 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.

Replacing the Management Ethernet Cable on an SRX5800 Firewall

One Ethernet cable with RJ-45 connectors is provided with the firewall.

Before you begin to replace the management ethernet cable:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap

To replace the cable connected to the **ETHERNET** port:

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.

2. Press the tab on the connector and pull the connector straight out of the port. Figure 173 on page 420 shows the connector.
3. Disconnect the cable from the network device.
4. Plug one end of the replacement cable into the **ETHERNET** port. Figure 174 on page 420 shows the port.
5. Plug the other end of the cable into the network device.

Figure 173: Cable Connector

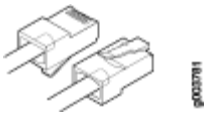
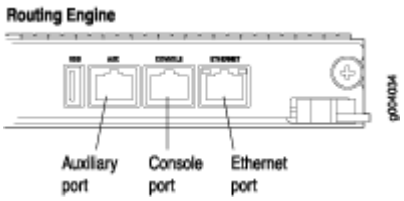


Figure 174: Ethernet Port



Replacing the SRX5800 Firewall Console or Auxiliary Cable

Before you begin to replace the console or auxiliary Cable:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

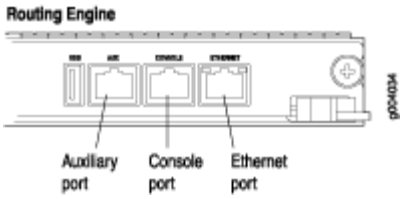
- ESD grounding strap

To use a system console to configure and manage the Routing Engine, connect it to the **CONSOLE** port on the Routing Engine. To use a laptop, modem, or other auxiliary device, connect it to the **AUX** port on the Routing Engine. Both ports accept a cable with an RJ-45 connector. One RJ-45/DB-9 cable is provided with the firewall. If you want to connect a device to both ports, you must supply another cable.

To replace a cable connected to a management console or auxiliary device:

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. Press the tab on the connector and pull the connector straight out of the port.
3. Disconnect the cable from the console or auxiliary device.
4. Plug the RJ-45 end of the replacement serial cable into the **CONSOLE** or **AUX** port. Figure 175 on page 421 shows the external device ports on the Routing Engine.
5. Plug the DB-9 socket end into the console or auxiliary device's serial port.

Figure 175: Auxiliary and Console Ports



Replacing an SRX5800 Firewall Network Interface Cable

IN THIS SECTION

To replace a network interface cable connected to an IOC, port module, or MIC, perform the following procedures:

Removing an SRX5800 Firewall Network Interface Cable

Before you begin removing the network interface cable from the firewall:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap

- Rubber safety caps

Removing and installing network interface cables does not affect firewall function, except that the component does not receive or transmit data while its cable is disconnected.

To remove a fiber-optic cable from a network interface on an IOC, port module, or MIC:

1. If the component connects to fiber-optic cable, have ready a rubber safety cap for each cable and transceiver.
2. If removing all cables connected to the component, use one of the following methods to take the component offline:
   - To take a port module offline :
     - Press the online/offline button on the port module. Use a narrow-ended tool that fits inside the opening that leads to the button. Press and hold the button until the port module LED goes out (about 5 seconds).
     - Issue the following CLI command:

       ```
       user@host> request chassis pic fpc-slot fpc-slot pic-slot port-module-slot offline
       ```

       For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.
   - To take an interface card offline :
     - Press and hold the corresponding online button on the craft interface. The green **OK** LED next to the button begins to blink. Hold the button down until the LED goes off.
     - Issue the following CLI command:

       ```
       user@host>request chassis fpc slot slot-number offline
       ```

       For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.
3. Unplug the cable from the cable connector port. If the network interface uses fiber-optic cable, immediately cover each transceiver and the end of each cable with a rubber safety cap.

LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

CAUTION: Do not leave a fiber-optic transceiver uncovered, except when you are inserting or removing cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

4. Remove the cable from the cable manager and detach it from the destination port.

Installing an SRX5800 Firewall Network Interface Cable

Before you begin installing a network interface cable:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap

To install a fiber-optic cable on a network interface on an IOC, port module, or MIC:

1. Have ready a length of the type of cable used by the component.
2. If the cable connector port is covered by a rubber safety plug, remove the plug.

LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

CAUTION: Do not leave a fiber-optic transceiver uncovered, except when you are inserting or removing cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

3. Insert the cable connector into the cable connector port on the component faceplate.
4. Arrange the cable in the cable manager to prevent it from dislodging or developing stress points. Secure the cable so that it is not supporting its own weight as it hangs to the floor. Place excess cable out of the way in a neatly coiled loop. Placing fasteners on the loop helps to maintain its shape.

CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

CAUTION: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

5. Insert the other end of the cable into the destination port.
6. Repeat the previous steps for any additional cables.
7. If the component is offline (its failure indicator LED is lit), use one of the following methods to bring it online.

   - To bring an IOC or MPC online:

     - Press and hold the corresponding IOC or MPC online button on the craft interface until the green **OK** LED next to the button lights steadily, in about 5 seconds.

     - Issue the following CLI command:

       ```
       user@host>request chassis fpc slot slot-number online
       ```

       For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

   - To bring a port module online:

     - Press the port module online button until the PIC LED lights green. Use a narrow-ended tool that fits inside the opening that leads to the button.

     - Issue the following CLI command:

       ```
       user@host>request chassis pic fpc-slot fpc-slot pic-slot pic-slot online
       ```

       For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

The normal functioning indicator LED confirms that the component is online. You can also verify correct IOC functioning by issuing the `show chassis fpc` command or correct PIC functioning by issuing the `show chassis fpc pic-status` command.

Replacing SRX5800 Firewall XFP and SFP Transceivers

IN THIS SECTION

To replace an XFP or SFP transceiver, perform the following procedures:

Removing an SRX5800 Firewall SFP or XFP Transceiver

Before you begin to remove a SFP or XFP transceiver:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Replacement transceiver or transceiver slot plug
- Antistatic mat
- Rubber safety cap for the transceiver
- Needle-nose pliers

Transceivers are installed in a MIC or SPC. Transceivers are hot-insertable and hot-removable. Removing a transceiver does not interrupt the functioning of the card, but the removed transceiver no longer receives or transmits data.

To remove a transceiver (see Figure 5):

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
2. Label the cables connected to the transceiver so that you can reconnect them correctly later.

LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

WARNING: Do not leave a fiber-optic transceiver uncovered except when inserting or removing a cable. The rubber safety cap keeps the port clean and prevents accidental exposure to laser light.

3. Remove the cable connector from the transceiver. Cover the transceiver and the end of each fiber-optic cable connector with a rubber safety cap immediately after disconnecting the fiber-optic cables.
4. Carefully arrange the disconnected cable in the cable manager to prevent the cable from developing stress points.

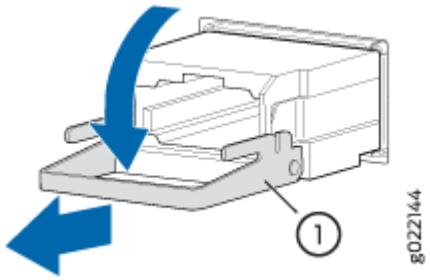
CAUTION: Do not bend a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

5. Using needle-nose pliers, open the ejector lever on the transceiver completely to unlock the transceiver. See Figure 5.

CAUTION: Make sure that you open the ejector lever completely until you hear it click. This prevents damage to the transceiver.

6. Grasp the transceiver ejector lever and pull the transceiver approximately 0.5 in. (1.3 cm) out of the port.
7. Using your fingers, grasp the body of the transceiver and pull it straight out of the port.

Figure 176: Removing a Transceiver



1– Ejector lever

8. Place a rubber safety cap over the transceiver.
9. Place the removed transceiver on an antistatic mat or in an electrostatic bag.
10. If you are not replacing the transceiver, insert transceiver slot plug into the card.

CAUTION: After removing a transceiver from the card, wait at least 30 seconds before reinserting it or inserting a transceiver into a different socket.

Installing an SRX5800 Firewall SFP or XFP Transceiver

Before you begin to install a SFP or XFP transceiver:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

Ensure that you have the following available:

- ESD grounding strap
- Rubber safety cap for the transceiver

Transceivers that are installed in an MIC or SPC. Transceivers are hot-insertable and hot-removable. Removing a transceiver does not interrupt the functioning of the card, but the removed transceiver no longer receives or transmits data.

CAUTION: The Juniper Networks Technical Assistance Center (JTAC) provides complete support for Juniper-supplied optical modules and cables. However, JTAC does not provide support for third-party optical modules and cables that are not qualified or supplied by Juniper Networks. If you face a problem running a Juniper device that uses third-party optical modules or cables, JTAC may help you diagnose host-related issues if the observed issue is not, in the opinion of JTAC, related to the use of the third-party optical modules or cables. Your JTAC engineer will likely request that you check the

third-party optical module or cable and, if required, replace it with an equivalent Juniper-qualified component.

Use of third-party optical modules with high-power consumption (for example, coherent ZR or ZR+) can potentially cause thermal damage to or reduce the lifespan of the host equipment. Any damage to the host equipment due to the use of third-party optical modules or cables is the users' responsibility. Juniper Networks will accept no liability for any damage caused due to such use.

To install a transceiver:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Take each transceiver to be installed out of its electrostatic bag and identify the slot on the component where it will be installed.
3. Verify that each transceiver is covered by a rubber safety cap. If it is not, cover the transceiver with a safety cap.
4. Carefully align the transceiver with the slots in the component. The connectors should face the component.
5. Slide the transceiver until the connector is seated in the component slot. If you are unable to fully insert the transceiver, make sure the connector is facing the right way.
6. Close the ejector handle of the transceiver.
7. Remove the rubber safety cap from the transceiver and insert the cable into the transceiver.
8. Verify that the status LEDs on the component faceplate indicate that the transceiver is functioning correctly.

Replacing the SRX5800 Firewall Cable Manager

IN THIS SECTION

To replace the cable manager, perform the following procedures:

Removing the SRX5800 Firewall Cable Manager

Before you begin to remove cable manager:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

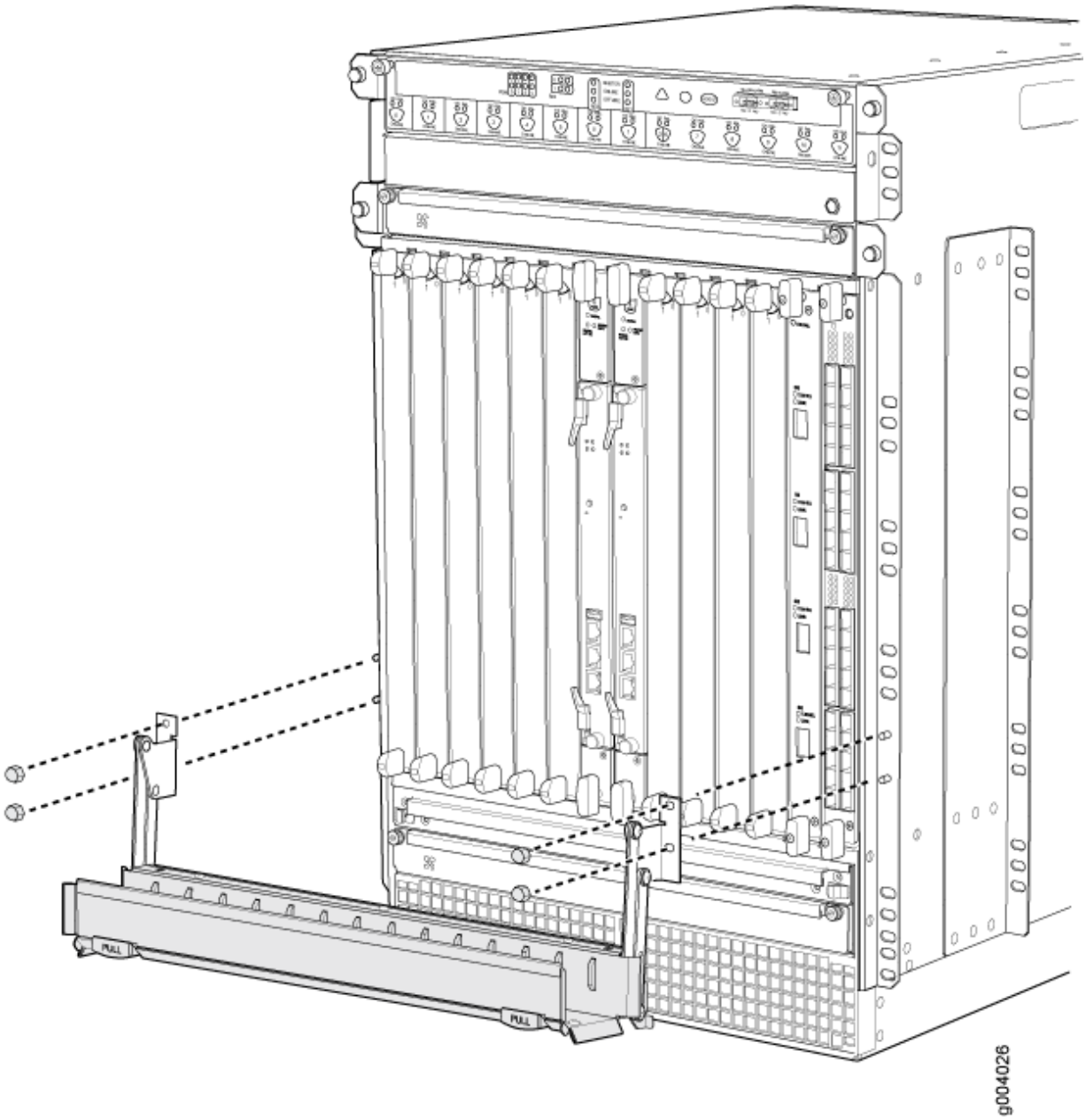
Ensure that you have the following available:

- ESD grounding strap
- 7/16 in. (11 mm) nut driver

To remove the cable manager (see Figure 6):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Using a 7/16-in. nut driver, unscrew the nuts on the corners of the cable manager.
3. Grasp the bottom of the cable manager and pull it straight out from the studs on the front of the chassis.

Figure 177: Removing the Cable Manager



Installing the SRX5800 Firewall Cable Manager

Before you begin installing the standard cable manager:

- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See *Prevention of Electrostatic Discharge Damage*.

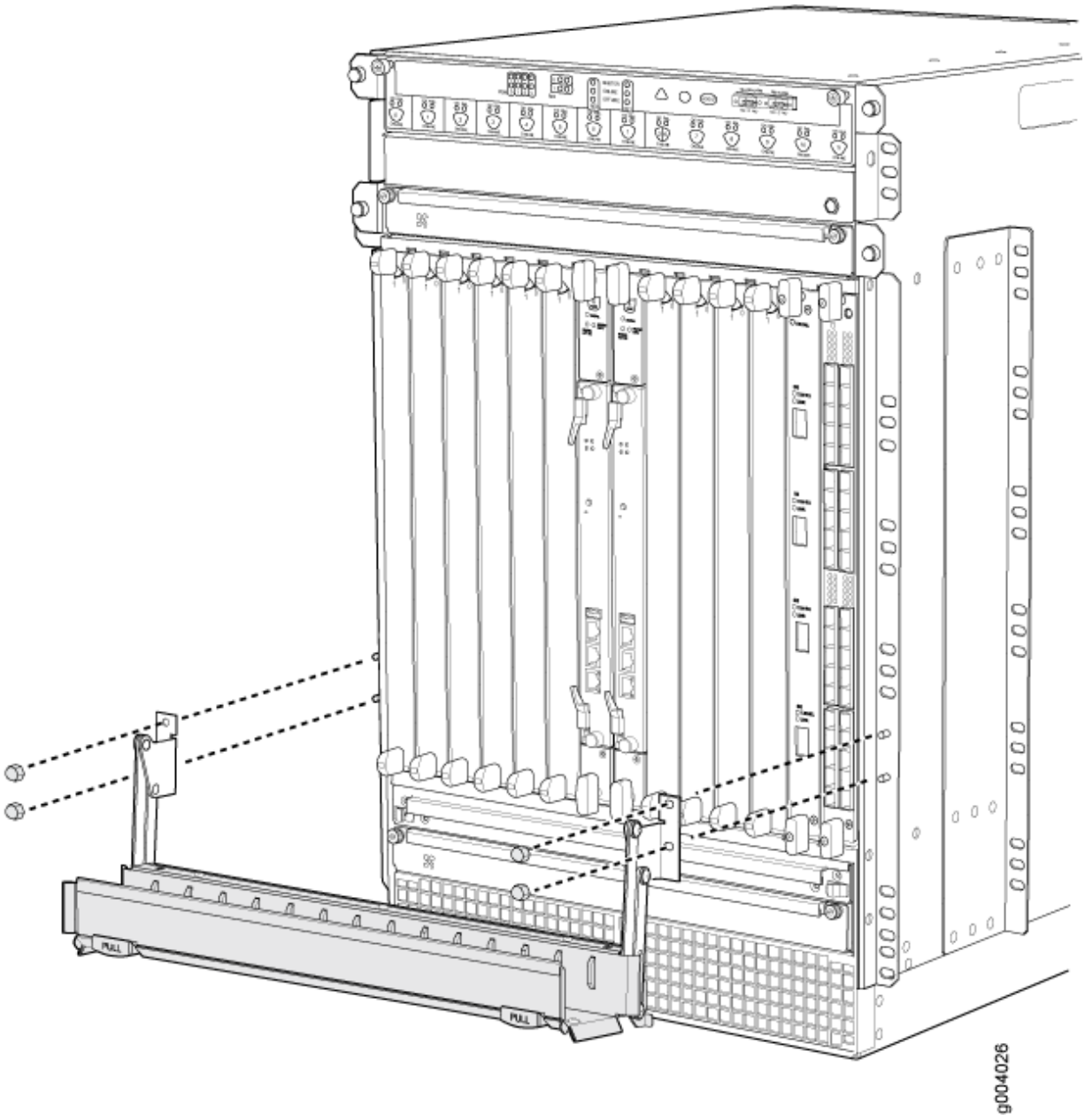
Ensure that you have the following available:

- ESD grounding strap
- 7/16 in. (11 mm) nut driver

To install the cable manager (see Figure 7):

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Position the standard cable manager on the studs on the lower front of the chassis.
3. Insert the nuts on the corners in the standard cable manager onto the studs on the chassis.
4. Using a 7/16 in. (11 mm)nut driver, tighten the nuts securely.

Figure 178: Installing the Cable Manager



5
CHAPTER

Troubleshooting Hardware

Troubleshooting the SRX5800

IN THIS SECTION

Troubleshooting the SRX5800 Firewall with the Junos OS CLI

The Junos OS command-line interface (CLI) is the primary tool for controlling and troubleshooting firewall hardware, Junos OS, routing protocols, and network connectivity. CLI commands display information from routing tables, information specific to routing protocols, and information about network connectivity derived from the ping and traceroute utilities.

You enter CLI commands on one or more external management devices connected to ports on the Routing Engine.

For information about using the CLI to troubleshoot Junos OS, see the appropriate Junos OS configuration guide.

Troubleshooting the SRX5800 Firewall with Chassis and Interface Alarm Messages

When the Routing Engine detects an alarm condition, it lights the major or minor alarm LED on the craft interface as appropriate. To view a more detailed description of the alarm cause, issue the `show chassis alarms` CLI command:

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

There are two classes of alarm messages:

- Chassis alarms—Indicate a problem with a chassis component such as the cooling system or power supplies.
- Interface alarms—Indicate a problem with a specific network interface.

Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls

IN THIS SECTION

Table 72 on page 435 lists the alarms that the chassis components can generate on SRX5400, SRX5600, and SRX5800 Firewalls.

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filters	Change air filter.	Change air filter.	Yellow

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Alternative media	The Firewall boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails.	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Yellow
Craft interface	The craft interface has failed.	Replace failed craft interface.	Red
Interface Cards (MPC/IOC/Flex IOC)	An interface card is offline.	Check the card. Remove and reinsert the card. If this fails, replace failed card.	Yellow
	An interface card has failed.	Replace failed card.	Red
	An interface card has been removed.	Insert card into empty slot.	Red
	Volt Sensor Fail	Reboot the specified card.	Red
Service Processing Card (SPC)	Abnormal exit in the current flow sessions of an SPU.	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Red
	CPU Digital Thermal Sensor (DTS) of the SPC reaches high or over temperature threshold.	Check the status of all fan trays.	Red

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
	FPC airflow temperature sensors in SRX5K-SPC3 reach high or over or crosses fire temperature threshold.	Check the status of all fan trays.	Red
	FPC airflow temperature sensors in SRX5K-SPC3 read/access failure.	If the alarm is present consistently, then it indicates a hardware issue. Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Yellow
	SRX5K-SPC3 checks for missing devices during boot and reports.	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Red

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
	SRX5K-SPC3 LTC Firm Ware Version Mismatch. LEDs on the front panel of the chassis indicate major alarm.	To manually upgrade the LTC Firmware Version: 1. Issue the CLI **show chassis alarm** command to check which FPC slot is raising the `LTC FW Version Mismatch` alarm. 2. Issue the CLI **show system firmware** command to check the current LTC firmware version, if a new verision of LTC firmware is available for the SRX5K-SPC3 card, and the firmware status is `OK`. 3. If there is a new version of LTC firmware, issue the CLI command **request system firmware upgrade pic fpc-slot x pic-slot x tag x** to upgrade the LTC firmware on the SRX5K-SPC3 card. 4. Issue the CLI command **show system firmware** to confirm the status of the SRX5K-SPC3 LTC firmware is `UPGRADED SUCCESSFULLY`. 5. Re-boot the Firewall.	Red
	Memory faults: DIMM failures and ECC errors.	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Red

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
	Real Time Clock battery failure.	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Red
	SSDs on the SRX5K-SPC3 missing or read/write to SSD is failing or SSD file system corrupt.	Replace the SSD. or Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Red
	OPMC Boot FPGA Faults	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Red
	Voltage sensor faults	From the CLI use the command **restart chassis-control** to reboot the firewall. If SPC still doesn't come online, then remove and insert back the SPC.	Red
Fan trays	A fan tray has been removed from the chassis.	Install missing fan tray.	Red

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
	Fan tray not working or failed.	Replace fan tray.	Red
	One fan in the chassis is not spinning or is spinning below required speed.	Replace fan tray.	Red
	A higher-cooling capacity fan tray is required when an MPC or high-density SPCs are installed on the chassis.	Upgrade to a high-capacity fan tray.	Yellow
	Fan tray under voltage.	Reseat the Fan Tray. If problem still continues open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Red
	Wrong fan tray installed.	Check and insert the appropriate fan tray.	Red
	In SRX5800 Firewall, mix of fan trays.	Insert the appropriate fan trays.	Red
	In SRX5800 Firewall, wrong fan tray installed on the top.	Check and insert the appropriate fan tray.	Red
Host subsystem	A host subsystem has been removed.	Insert host subsystem into empty slot.	Yellow
	A host subsystem has failed.	Replace failed host subsystem.	Red

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Power supplies	A power supply has been removed from the chassis.	Insert power supply into empty slot.	Yellow
	A power supply has a high temperature.	Replace failed power supply or power entry module.	Red
	A power supply input has failed.	Check power supply input connection.	Red
	A power supply output has failed.	Check power supply output connection.	Red
	A power supply has failed.	Replace failed power supply.	Red
	Invalid AC power supply configuration.	When two AC power supplies are installed, insert one power supply into an odd-numbered slot and the other power supply into an even-numbered slot.	Red
	Invalid DC power supply configuration.	When two DC power supplies are installed, insert one power supply into an odd-numbered slot and the other power supply into an even-numbered slot.	Red
	Mix of AC and DC power supplies.	Do not mix AC and DC power supplies. For DC power, remove the AC power supply. For AC power, remove the DC power supply.	Red
	Not enough power supplies.	Install an additional power supply.	Red

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Excessive framing errors on console port. An excessive framing error alarm is triggered when the default framing error threshold of 20 errors per second on a serial port is exceeded. This might be caused by a faulty serial console port cable connected to the device.	Replace the serial cable connected to the device. If the cable is replaced and no excessive framing errors are detected within 5 minutes from the last detected framing error, the alarm is cleared automatically.	Yellow
	Error in reading or writing hard disk.	Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	Error in reading or writing CompactFlash card.	Reformat CompactFlash card and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	System booted from default backup Routing Engine. If you manually switched primary role, ignore this alarm condition.	Install bootable image on default primary Routing Engine. If this fails, replace failed Routing Engine.	Yellow
	System booted from hard disk.	Install bootable image on CompactFlash card. If this fails, replace failed Routing Engine.	Yellow
	CompactFlash card missing in boot list.	Replace failed Routing Engine.	Red
	Hard disk missing in boot list.	Replace failed Routing Engine.	Red

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
	Routing Engine failed to boot.	Replace failed Routing Engine.	Red
	The Ethernet management interface (**fxp0** or **em0**) on the Routing Engine is down.	• Check the interface cable connection. • Reboot the system. • If the alarm recurs, open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States)	Red
System Control Board (SCB)	An SCB has been removed.	Insert SCB into empty slot.	Yellow
	An SCB temperature sensor alarm has failed.	Replace failed SCB.	Yellow
	An SCB has failed.	Replace failed SCB.	Red

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
	An SCB throughput decreased.	• Check fabric plane summary if all 4 fabric planes are online. • This alarm could be raised before all fabric planes are brought up. It will be cleared after at least 4 planes are up. • If all planes are up and still seeing alarms, raise a case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States)	Yellow
	An SCB PMBus Device Fail	Ignore the alarm if rasied once or twice. If the alarm is present consistently, then it indicates a hardware issue. Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Yellow

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls ***(Continued)***

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed.	• Check room temperature. • Check air filter and replace it. • Check airflow. • Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed.	• Check room temperature. • Check air filter and replace it. • Check airflow. • Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the Firewall shuts down.	• Check room temperature. • Check air filter and replace it. • Check airflow. • Check fan.	Red
	Chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the Firewall shuts down.	• Check room temperature. • Check air filter and replace it. • Check airflow. • Check fan.	Red

Table 72: Chassis Component Alarm Conditions on SRX5400, SRX5600, and SRX5800 Firewalls *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
	The temperature sensor has failed.	• Check environmental conditions and alarms on other devices. • Ensure that environmental factors (such as hot air blowing around the equipment) are not affecting the temperature sensor. • If the alarm recurs, open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Red

Backup Routing Engine Alarms

For Firewalls with primary and backup Routing Engines, a primary Routing Engine can generate alarms for events that occur on a backup Routing Engine. Table 73 on page 447 lists chassis alarms generated for a backup Routing Engine.

NOTE: Because the failure occurs on the backup Routing Engine, alarm severity for some events (such as Ethernet interface failures) is yellow instead of red.

NOTE: For information about configuring redundant Routing Engines, see the Junos OS High Availability Library for Routing Devices.

Table 73: Backup Routing Engine Alarms

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Alternative media	The backup Routing Engine boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails.	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Yellow
Boot Device	The boot device (CompactFlash or hard disk) is missing in boot list on the backup Routing Engine.	Replace failed backup Routing Engine.	Red
Ethernet	The Ethernet management interface (**fxp0** or **em0**) on the backup Routing Engine is down.	• Check the interface cable connection. • Reboot the system. • If the alarm recurs, open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Yellow
FRU Offline	The backup Routing Engine has stopped communicating with the primary Routing Engine.	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Yellow
Hard Disk	Error in reading or writing hard disk on the backup Routing Engine.	Reformat hard disk and install bootable image. If this fails, replace failed backup Routing Engine.	Yellow

Table 73: Backup Routing Engine Alarms *(Continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Multibit Memory ECC	The backup Routing Engine reports a multibit ECC error.	• Reboot the system with the board reset button on the backup Routing Engine. • If the alarm recurs, open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll free, US & Canada) or 1-408-745-9500 (from outside the United States).	Yellow

Troubleshooting the SRX5800 Firewall with Alarm Relay Contacts

The craft interface has two alarm relay contacts for connecting the firewall to external alarm devices. Whenever a system condition triggers either the major or minor alarm on the craft interface, the alarm relay contacts are also activated. The alarm relay contacts are located on the upper right of the craft interface.

Troubleshooting the SRX5800 Firewall with the Craft Interface LEDs

The craft interface is the panel on the front of the firewall located above the card cage that contains LEDs and buttons that allow you to troubleshoot the device.

LEDs on the craft interface include the following:

- Alarm LEDs—One large red circular LED and one large yellow triangular LED, located on the upper right of the craft interface, indicate two levels of alarm conditions. The circular red LED lights to indicate a critical condition that can result in a system shutdown. The triangular yellow LED lights to indicate a less severe condition that requires monitoring or maintenance. Both LEDs can be lit simultaneously. A condition that causes an alarm LED to light also activates the corresponding alarm relay contact on the craft interface.

- Host subsystem LEDs—Three LEDs, **MASTER**, **ONLINE**, and **OFFLINE**, indicate the status of the host subsystem. A green **MASTER** LED indicates that the host is functioning as primary. The **ONLINE** LED indicates the host is online. The **OFFLINE** LED indicates the host is offline. The host subsystem LEDs are located on the left of the craft interface and are labeled **RE0** and **RE1**.
- Power supply LEDs—Two LEDs (**PEM**) indicate the status of each power supply. Green indicates that the power supply is functioning normally. Red indicates that the power supply is not functioning normally. The power supply LEDs are located in the center of the craft interface, and are labeled **0** through **3**.
- Card OK/Fail LEDs—Two LEDs, **OK** and **FAIL**, indicate the status of the card in each slot in the card cage. Green indicates OK and red indicates a failure. The card OK/Fail LEDs are located along the bottom of the craft interface, and are labeled **0** through **5**, **2/6**, and **7** through **11**.
- SCB LEDs—Two LEDs, **OK** and **FAIL**, indicate the status of each SCB. Green indicates OK and red indicates a failure. The SCB LEDs are located in the center of the craft interface along the bottom, and are labeled **0** and **1**.
- Fan LEDs—Two LEDs indicate the status of each fan tray. Green indicates OK and red indicates a fan failure. The fan LEDs are located on the upper left of the craft interface.

Troubleshooting the SRX5800 Firewall with the Component LEDs

The following LEDs are located on various firewall components and display the status of those components:

- Card LED—One LED labeled **OK/FAIL** on each card in the card cage indicates the card's status.
- MIC and port module LED—One LED labeled **OK/FAIL** on each MIC installed in an MPC, and each port module installed in a Flex IOC indicates the MIC or port module's status.
- SCB LEDs—Three LEDs, labeled **FABRIC ACTIVE**, **FABRIC ONLY**, and **OK/FAIL** , on each SCB faceplate indicate the status of the SCB. If no LEDs are lit, the master Routing Engine might still be booting, or the SCB is not receiving power.
- Routing Engine LEDs—Four LEDs, labeled **MASTER**, **HDD**, **ONLINE**, and **FAIL** on the Routing Engine faceplate indicate the status of the Routing Engine and hard disk drive.
- Power supply LEDs—Three or four LEDs on each power supply faceplate indicate the status of that power supply.

Troubleshooting the SRX5800 Firewall Cooling System

IN THIS SECTION

Problem

Description

The fans in a fan tray are not functioning normally.

Solution

Follow these guidelines to troubleshoot the fans:

- Check the fan LEDs and alarm LEDs on the craft interface.
- If the major alarm LED on the craft interface lights, use the CLI to get information about the source of an alarm condition: `user@host> show chassis alarms`.

  If the CLI output lists only one fan failure, and the other fans are functioning normally, the fan is most likely faulty and you must replace the fan tray.
- Place your hand near the exhaust vents at the side of the chassis to determine whether the fans are pushing air out of the chassis.
- If the fan tray is removed, a minor alarm and a major alarm occur.
- The following conditions automatically cause the fans to run at full speed and also trigger the indicated alarm:
  - A fan fails (major alarm).
  - The firewall temperature exceeds the “temperature warm” threshold (minor alarm).
  - The temperature of the firewall exceeds the maximum (“temperature hot”) threshold (major alarm and automatic shutdown of the power supplies).

Troubleshooting SRX5800 Firewall Interface Cards

IN THIS SECTION

Problem

Description

The interface cards (IOCs, Flex IOCs, or MPCs) are not functioning normally.

Solution

- Monitor the green LED labeled **OK** on the craft interface corresponding to the slot as soon as an interface card is seated in an operating firewall.

  The Routing Engine downloads the interface card's software to it under two conditions: the interface card is present when the Routing Engine boots Junos OS, and the interface card is installed and requested online through the CLI or push button on the front panel. The interface card then runs diagnostics, during which the **OK** LED blinks. When the interface card is online and functioning normally, the **OK** LED lights green steadily.

- Make sure the interface card is properly seated in the midplane. Check that each ejector handle has been turned clockwise and is tight.

- Check the **OK/FAIL** LED on the interface card and **OK** and **FAIL** LEDs for the slot on the craft interface. When the interface card is online and functioning normally, the **OK** LED lights green steadily.

- Issue the CLI `show chassis fpc` command to check the status of installed interface cards. As shown in the sample output, the value *Online* in the column labeled *State* indicates that the interface card is functioning normally:

```
user@host> show chassis fpc
                    Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State           (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online           41      9          0       1024       15         57
```

```
  1  Online           43      5          0       1024       16         57
  2  Online           43     11          0       1024       16         57
  3  Empty
  4  Empty
  5  Online           42      6          0       1024       16         57
```

For more detailed output, add the `detail` option. The following example does not specify a slot number, which is optional:

```
user@host> show chassis fpc detail

Slot 0 information:
  State                               Online
  Temperature                      41 degrees C / 105 degrees F
  Total CPU DRAM                 1024 MB
  Total RLDRAM                    256 MB
  Total DDR DRAM                 4096 MB
  Start time:                         2007-07-10 12:28:33 PDT
  Uptime:                             1 hour, 33 minutes, 52 seconds
Slot 1 information:
  State                               Online
  Temperature                      43 degrees C / 109 degrees F
  Total CPU DRAM                 1024 MB
  Total RLDRAM                    256 MB
  Total DDR DRAM                 4096 MB
  Start time:                         2007-07-10 12:28:38 PDT
  Uptime:                             1 hour, 33 minutes, 47 seconds
Slot 2 information:
  State                               Online
  Temperature                      43 degrees C / 109 degrees F
  Total CPU DRAM                 1024 MB
  Total RLDRAM                    256 MB
  Total DDR DRAM                 4096 MB
  Start time:                         2007-07-10 12:28:40 PDT
  Uptime:                             1 hour, 33 minutes, 45 seconds
Slot 5 information:
  State                               Online
  Temperature                      42 degrees C / 107 degrees F
  Total CPU DRAM                 1024 MB
  Total RLDRAM                    256 MB
  Total DDR DRAM                 4096 MB
```

```
  Start time:                          2007-07-10 12:28:42 PDT
  Uptime:                              1 hour, 33 minutes, 43 seconds
```

For further description of the output from the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

Troubleshooting SRX5800 Firewall MICs and Port Modules

IN THIS SECTION

Problem

Description

The MICs or port modules are not functioning normally.

Solution

- Check the status of each port on a port module by looking at the LED located on the port module faceplate.
- Check the status of a port module by issuing the `show chassis fpc pic-status` CLI command. The port module slots in the Flex IOC are numbered from **0** through **1**:

```
user@host> show chassis fpc pic-status
Slot 0   Online       SRX5k SPC
  PIC 0  Online       SPU Cp-Flow
  PIC 1  Online       SPU Flow
Slot 3   Online       SRX5k DPC 4X 10GE
  PIC 0  Online       1x 10GE(LAN/WAN) RichQ
  PIC 1  Online       1x 10GE(LAN/WAN) RichQ
  PIC 2  Online       1x 10GE(LAN/WAN) RichQ
```

```
  PIC 3  Online       1x 10GE(LAN/WAN) RichQ
Slot 5   Online       SRX5k FIOC
  PIC 0  Online       16x 1GE TX
  PIC 1  Online       4x 10GE XFP
```

For further description of the output from the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

Troubleshooting SRX5800 Firewall SPCs

IN THIS SECTION

Problem

Description

A Services Processing Card (SPC) is not functioning normally.

Solution

- Make sure the SPC is properly seated in the midplane. Check that each ejector handle has been turned clockwise and is tight.
- Issue the CLI `show chassis fpc` command to check the status of installed SPCs. As shown in the sample output, the value *Online* in the column labeled *State* indicates that the SPC is functioning normally:

```
user@host> show chassis fpc

Slot State           (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online           35      4          0       1024       13         25
  1  Online           47      3          0       1024       13         25
```

```
  2  Online            37      8          0       2048       18         14
```

For more detailed output, add the `detail` option. The following example does not specify a slot number, which is optional:

```
user@host> show chassis fpc detail

Slot 0 information:
  State                               Online
  Temperature                          35
  Total CPU DRAM                     1024 MB
  Total RLDRAM                        259 MB
  Total DDR DRAM                     4864 MB
  Start time:                         2013-12-10 02:58:16 PST
  Uptime:                             1 day, 11 hours, 59 minutes, 15 seconds
  Max Power Consumption               585 Watts
Slot 1 information:
  State                               Online
  Temperature                          47
  Total CPU DRAM                     1024 MB
  Total RLDRAM                        259 MB
  Total DDR DRAM                     4864 MB
  Start time:                         2013-12-10 02:55:30 PST
  Uptime:                             1 day, 12 hours, 2 minutes, 1 second
  Max Power Consumption               585 Watts
Slot 2 information:
  State                               Online
  Temperature                          37
  Total CPU DRAM                     2048 MB
  Total RLDRAM                       1036 MB
  Total DDR DRAM                     6656 MB
  Start time:                         2013-12-10 02:58:07 PST
  Uptime:                             1 day, 11 hours, 59 minutes, 24 seconds
  Max Power Consumption               570 Watts
```

For further description of the output from the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.

Troubleshooting the SRX5800 Firewall Power System

IN THIS SECTION

Problem

Description

The power system is not functioning normally.

Solution

- Check the LEDs on each power supply faceplate.
  - If an AC power supply is correctly installed and functioning normally, the **AC OK** and **DC OK** LEDs light steadily, and the **PS FAIL** LED is not lit.
  - If a DC power supply is correctly installed and functioning normally, the **PWR OK**, **BREAKER ON**, and **INPUT OK** LEDs light steadily.
- Issue the CLI `show chassis environment pem` command to check the status of installed power supplies. As shown in the sample output, the value *Online* in the rows labeled *State* indicates that each of the power supply is functioning normally:

```
user@host> show chassis environment pem
PEM 0 status:
  State                     Online
  Temperature               OK
  DC Input:                 OK
  DC Output          Voltage(V) Current(A)  Power(W)  Load(%)
                         57        14           798        19
 PEM 1 status:
  State                     Online
  Temperature               OK
  DC Input:                 OK
```

```
DC Output           Voltage(V) Current(A)  Power(W)  Load(%)
                        57         13           741       18
```

If a power supply is not functioning normally, perform the following steps to diagnose and correct the problem:

- If a major alarm condition occurs, issue the `show chassis alarms` command to determine the source of the problem.
- Check that the AC input switch (—) or DC circuit breaker (|) is in the on position and that the power supply is receiving power.
- Verify that the source circuit breaker has the proper current rating. Each power supply must be connected to a separate source circuit breaker.
- Verify that the AC power cord or DC power cables from the power source to the firewall are not damaged. If the insulation is cracked or broken, immediately replace the cord or cable.
- Connect the power supply to a different power source with a new power cord or power cables. If the power supply status LEDs indicate that the power supply is not operating normally, the power supply is the source of the problem. Replace the power supply with a spare.
- If all power supplies have failed, the system temperature might have exceeded the threshold, causing the system to shut down.

> **NOTE**: If the system temperature exceeds the threshold, Junos OS shuts down all power supplies so that no status is displayed.
>
> Junos OS also can shut down one of the power supplies for other reasons. In this case, the remaining power supplies provide power to the firewall, and you can still view the system status through the CLI or display.

To restart a high-capacity AC power supply after a shut down due to an over-temperature situation:

1. Move the power switch on the power supply to the off (o) position.
2. Turn off power to where the AC line goes into the power distribution module (PDM) area.
3. Wait for the power supply LEDs to fade out and for the fans inside the power supply to shutdown. This can take up to 10 seconds.

> ⚠ **CAUTION**: Do not attempt to power-on the power supply if the LED is still lit and the fan is still running. If you do, the firewall will not reboot.

4. Turn on power to where the AC line goes into the power distribution module (PDM) area.
5. Move the power switch on the power supply to the on (|) position.
6. Verify that the LEDs on the power supply faceplate are properly lit.
7. Issue the CLI `show chassis environment pem` command and verify the State is `ONLINE` and the Temperature is `OK`.

To restart a high-capacity DC power supply after a shut down due to an over-temperature situation:

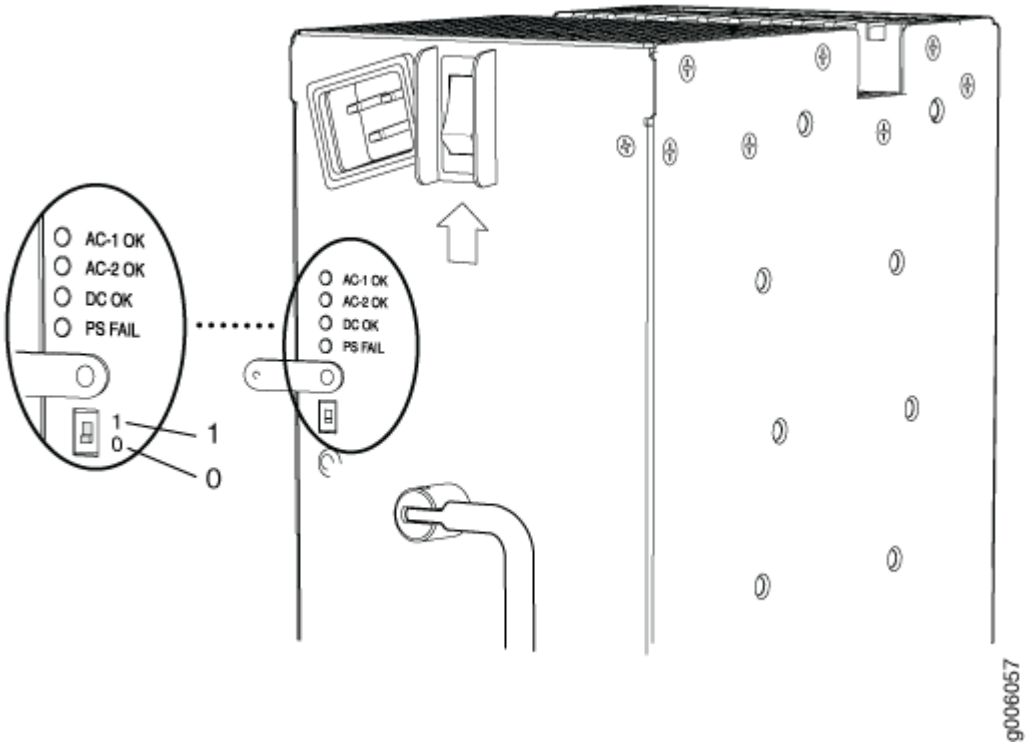
1. Switch off the circuit breaker(s) on the DC distribution panel to remove power to the chassis and power supplies.
2. Switch on the circuit breaker(s) on the distribution panel to power up the chassis and power supplies.

> **NOTE**: The power switch on the power supplies is not part of the outer or inner DC circuits and therefore does not need to be switched off when restarting the chassis.

> **NOTE**: If output power is not load-balancing correctly in the same zone on a firewall with a high-capacity AC or DC power supply module, connect two feeds and change the DIP switch to **1** to boost the voltage on the power supply module.

Each High Capacity AC or DC power supply accepts two AC or DC feeds in two unique AC or DC receptacles. It is possible to operate with one feed, but there is a reduction in the power supply output. The DIP switch must be set according to the number of AC or DC feeds that are present for the power supply.

Figure 179: AC Power Input Mode Switch



- Position – **0** indicates that only one AC or DC feed is provided.
- Position – **1** indicates that two AC or DC feeds are provided.

The following example shows what should be the DIP switch position based on the number of AC or DC input feeds expected and connected to the PEM:

1. Issue the CLI `show chassis power` command and check how many feeds are connected.

   The sample out put below is the output of a chassis with AC power supplies:

```
user@host# run show chassis power
PEM 0:
  State:     Online
  AC input:  OK (2 feed expected, 2 feed connected)
  Capacity:  4100 W (maximum 4100 W)
  DC output: 798 W (zone 0, 14 A at 57 V, 19% of capacity)

PEM 1:
  State:     Online
  AC input:  OK (1 feed expected, 2 feed connected)
  Capacity:  1700 W (maximum 4100 W)
```

```
  DC output: 741 W (zone 1, 13 A at 57 V, 43% of capacity)

PEM 2:
  State:     Empty
  Input:     Absent

PEM 3:
  State:     Empty
  Input:     Absent

System:
  Zone 0:
      Capacity:          4100 W (maximum 4100 W)
      Allocated power:   1255 W (2845 W remaining)
      Actual usage:      798 W
  Zone 1:
      Capacity:          1700 W (maximum 4100 W)
      Allocated power:   1090 W (610 W remaining)
      Actual usage:      741 W
  Total system capacity: 5800 W (maximum 8200 W)
  Total remaining power: 3455 W
```

The output of the `show chassis power` command shows that; on PEM 0 two AC input feeds are expected and two AC input feeds are connected and on PEM 1 one AC input feed is expected and two AC input feeds are connected.

2. Issue the `show chassis alarms` command to see if there are any active alarms and the position of the PEM DIP switch.

```
> show chassis alarms
1 alarms currently active
Alarm time               Class  Description
2017-01-23 05:05:17 PST  Minor  PEM 1 Dipswitch 0 Feed Connection 2
```

The output of the `show chassis alarms` command shows one active alarm on PEM 1 and the position of the DIP switch as 0.

In this example output, there is an alarm on PEM 1 because there is a need of only one AC feed but the PEM 1 is connected with two AC feeds and the DIP switch position is 0.

3. Change the PEM 1 DIP switch position to **1**. This should clear the alarm.

NOTE: Changing the DIP switch position does not impact traffic. However, it is always recommended to do so in a maintenance window.

4. Issue the CLI `show chassis power` command and check the output to see if the number of feeds expected on PEM 1 is the same as the feeds connected.

```
# run show chassis power
PEM 0:
  State:     Online
  AC input:  OK (2 feed expected, 2 feed connected)
  Capacity:  4100 W (maximum 4100 W)
  DC output: 741 W (zone 0, 13 A at 57 V, 18% of capacity)

PEM 1:
  State:     Online
  AC input:  OK (2 feed expected, 2 feed connected)
  Capacity:  4100 W (maximum 4100 W)
  DC output: 741 W (zone 1, 13 A at 57 V, 18% of capacity)

PEM 2:
  State:     Empty
  Input:     Absent

PEM 3:
  State:     Empty
  Input:     Absent

System:
  Zone 0:
      Capacity:          4100 W (maximum 4100 W)
      Allocated power:   1255 W (2845 W remaining)
      Actual usage:      741 W
  Zone 1:
      Capacity:          4100 W (maximum 4100 W)
      Allocated power:   1090 W (3010 W remaining)
      Actual usage:      741 W
  Total system capacity: 8200 W (maximum 8200 W)
  Total remaining power: 5855 W
```

The output of the `show chassis power` command shows that the number of feeds on PEM 1 expected is the same as the feeds connected.

5. Issue the CLI `show chassis alarms` command to check if the alarm is removed.

```
> show chassis alarms
No alarms currently active
```

The output of the `show chassis alarms` command shows no active alarms.

Behavior of the SRX5400, SRX5600, and SRX5800 Firewalls When the SRX5K-SCBE and SRX5K-RE-1800X4 in a Chassis Cluster Fail

It is important to understand the behavior of the SRX5400, SRX5600, and SRX5800 Firewalls when the Switch Control Board (SRX5K-SCBE) and Routing Engine (SRX5K-RE-1800X4) in the chassis cluster fail.

NOTE: This procedure is also applicable for SCB3 except that SCB3 redundancy is supported.

NOTE: We strongly recommend that you perform the *ISHU* during a maintenance window, or during the lowest possible traffic as the secondary node is not available at this time.

NOTE: The SRX5K-SCBE and SRX5K-RE-1800X4 are not hot-swappable.

NOTE: Four fabric planes must be active at any time in a chassis cluster. If fewer than four fabric planes are active, then the Redundancy Group (RG1+) will fail over to the secondary node. Table 74 on page 463 shows the minimum fabric plane requirements for the SCB.

Table 74: Expected Device Behavior and Minimum SRX5K-SCBE and Fabric Plane Requirements

Platform	Number of SRX5K-SCBs	Active Planes	Redundant Planes	Expected Behavior After the SCB and Routing Engine are Removed
SRX5400	1	4 (virtual)	0 (virtual)	If the SCB in the primary node fails, the device will fail over to the secondary node as the primary node powers off.
SRX5600	2	4 (virtual)	4 (virtual)	If the active SCB in the primary node fails, the behavior of the device does not change as the redundant SCB becomes active provided all four fabric planes are in good condition. If the second SCB in the primary node fails, the device will fail over to the secondary node as the primary node powers off.
SRX5800	3	4	2	This device supports one SCB for two fabric planes, providing a redundancy of three SCBs. If the active SCB fails, the device behavior does not change as the remaining two SCBs fulfill the requirement to have four fabric planes. If the second SCB also fails, no spare planes are available in the chassis triggering inter-chassis redundancy. Therefore, RG1+ will fail over to the secondary node.

NOTE: In SRX5600 and SRX5800 Firewalls, failover does not happen when the secondary Routing Engine in slot 1 fails, while the SCB in slot 1 is inactive.

For detailed information about chassis cluster, see the *Chassis Cluster User Guide for SRX Series Devices* at www.juniper.net/documentation/.

CHAPTER 6

Contacting Customer Support and Returning the Chassis or Components

Returning the SRX5800 Chassis or Components

IN THIS SECTION

Contacting Customer Support

Once you have located the serial numbers of the firewall or component, you can return the firewall or component for repair or replacement. For this, you need to contact Juniper Networks Technical Assistance Center (JTAC).

You can contact JTAC 24 hours a day, 7 days a week, using any of the following methods:

- On the Web: Using the Service Request Manager link at https://support.juniper.net/support/
- By telephone:
  - From the US and Canada: 1-888-314-JTAC
  - From all other locations: 1-408-745-9500

> **NOTE**: If contacting JTAC by telephone, enter your 12-digit service request number followed by the pound (#) key if this is an existing case, or press the star (*) key to be routed to the next available support engineer.

Return Procedure for the SRX5800 Firewall

If a problem cannot be resolved by the JTAC technician, a Return Materials Authorization (RMA) is issued. This number is used to track the returned material at the factory and to return repaired or new components to the customer as needed.

> **NOTE**: Do not return any component to Juniper Networks, Inc. unless you have first obtained an RMA number. Juniper Networks, Inc. reserves the right to refuse shipments that do not have an RMA. Refused shipments will be returned to the customer via collect freight.

For more information about return and repair policies, see the customer support Web page at https://www.juniper.net/support/guidelines.html .

To return a firewall or component to Juniper Networks for repair or replacement:

1. Determine the part number and serial number of the firewall or component. For the serial number locations of cards and modules such as MPCs, SPCs, port modules and Routing Engines, see the *SRX5400, SRX5600, and SRX5800 Firewall Card Reference* at www.juniper.net/documentation/.
2. Obtain a Return Materials Authorization (RMA) number from JTAC.

   > **NOTE**: Do not return the firewall or any component to Juniper Networks unless you have first obtained an RMA number. Juniper Networks reserves the right to refuse shipments that do not have an RMA. Refused shipments are returned to the customer via collect freight.

3. Pack the firewall or component for shipping.

For more information about return and repair policies, see the customer support webpage at https://www.juniper.net/support/guidelines.html .

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

Listing the SRX5800 Firewall Component Serial Numbers with the Command-Line Interface

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

```
user@host> show chassis hardware

Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN10B7ACDAGA      SRX 5800
Midplane         REV 03   710-013698   TR0813            SRX 5800 Backplane
FPM Board        REV 03   710-014974   KC3418            Front Panel Display
PDM              Rev 03   740-013110   QCS1122501L       Power Distribution Modu
le
PEM 1            Rev 03   740-013682   QCS1130409T       PS 1.7kW; 200-240VAC in
PEM 2            Rev 03   740-013682   QCS1130409M       PS 1.7kW; 200-240VAC in
Routing Engine 0 REV 06   740-015113   1000697051        RE-S-1300
CB 0             REV 07   710-013385   KC0433            SRX5k SCB
CB 1             REV 07   710-013385   KC0259            SRX5k SCB
FPC 6            REV 03   750-020235   JS4722            SRX5k DPC 40x 1GE
  CPU            REV 06   710-013713   JZ4019            DPC PMB
  PIC 0                   BUILTIN      BUILTIN           10x 1GE RichQ
    Xcvr 0       REV 01   740-011782   PAQ2K01           SFP-SX
    Xcvr 1       REV 01   740-014132   61531018          SFP-T
    Xcvr 2       REV 01   740-013111   7303709           SFP-T
    Xcvr 4       REV 01   740-011782   PAQ2JZP           SFP-SX
    Xcvr 5       REV 01   740-013111   8043356           SFP-T
    Xcvr 6       REV 01   740-013111   8043257           SFP-T
    Xcvr 7       REV 01   740-013111   8043300           SFP-T
    Xcvr 8       REV 01   740-013111   8043215           SFP-T
    Xcvr 9       REV 01   740-013111   8043184           SFP-T
  PIC 1                   BUILTIN      BUILTIN           10x 1GE RichQ
    Xcvr 0       0        NON-JNPR     AM0619193B        SFP-SX
    Xcvr 9       0        NON-JNPR     AJ054100PH        SFP-SX
  PIC 2                   BUILTIN      BUILTIN           10x 1GE RichQ
    Xcvr 1       REV 01   740-014132   61522010          SFP-T
    Xcvr 2       REV 01   740-013111   7303481           SFP-T
    Xcvr 4       REV 01   740-011782   PAQ2K0H           SFP-SX
    Xcvr 5       REV 01   740-013111   8043179           SFP-T
```

```
    Xcvr 6       REV 01   740-013111   7522572          SFP-T
    Xcvr 7       REV 01   740-013111   8043157          SFP-T
    Xcvr 8       REV 01   740-013111   7522678          SFP-T
    Xcvr 9       REV 01   740-013111   7522683          SFP-T
  PIC 3                   BUILTIN      BUILTIN          10x 1GE RichQ
    Xcvr 0       0        NON-JNPR     AJ06080TKC       SFP-SX
    Xcvr 9       0        NON-JNPR     AJ06020HSJ       SFP-SX
FPC 7            BB_P2_28 710-013699   JS4812           SRX5k SPC
  CPU            REV 06   710-013713   KA7426           DPC PMB
  PIC 0                   BUILTIN      BUILTIN          SPU Cp
  PIC 1                   BUILTIN      BUILTIN          SPU Flow
Fan Tray 0       REV 04   740-014971   TP1433           Fan Tray
Fan Tray 1       REV 04   740-014971   TP1636           Fan Tray
```

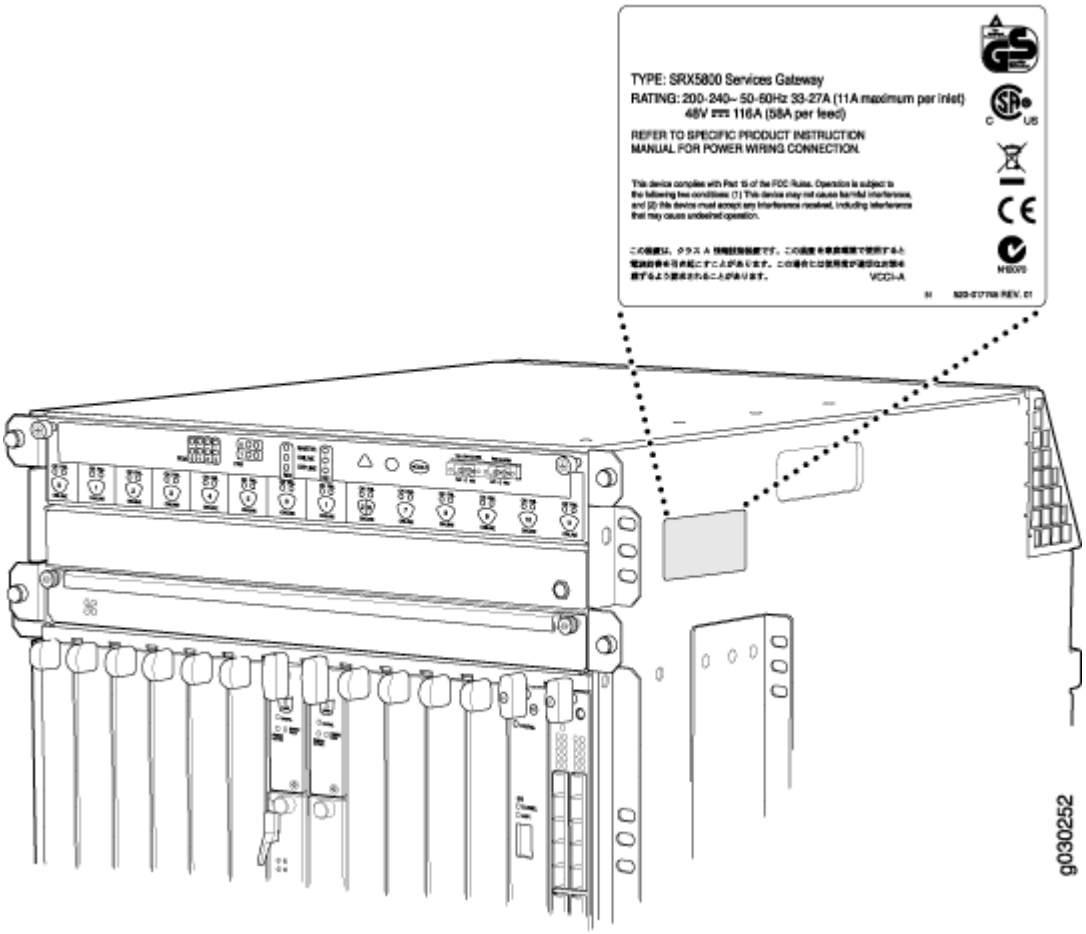
Most components also have a small rectangular serial number ID label (see Figure 180 on page 468) attached to the component body.

Figure 180: Serial Number ID Label

Locating the SRX5800 Firewall Chassis Serial Number Label

The chassis serial number label is located on the side of the chassis (see Figure 181 on page 469).

Figure 181: SRX5800 Chassis Serial Number Label



Locating the SRX5800 Firewall Power Supply Serial Number Label

If you are returning an AC or a DC power supply to Juniper Networks for repair or replacement, you must locate the serial number of the component. You must provide the serial number to the Juniper Networks Technical Assistance Center (JTAC) when you contact them to obtain Return Materials Authorization (RMA).

The location of the serial number labels on Standard-Capacity and High Capacity AC or DC power supplies is explained below:

- AC Power Supplies:
  - Standard-Capacity AC Power Supply—The serial number label is on the AC power supply faceplate under the on/off switch. See Figure 182 on page 470.

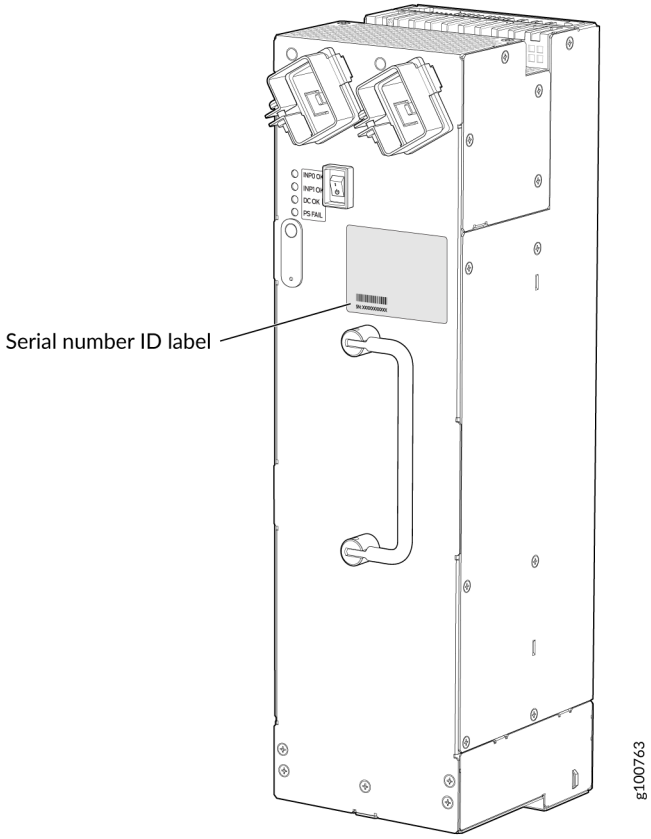
Figure 182: Standard-Capacity AC Power Supply Serial Number Label

- High-Capacity AC Power Supply—The serial number label is on the top of the AC power supply. See Figure 183 on page 470.

Figure 183: High-Capacity AC Power Supply Serial Number Label

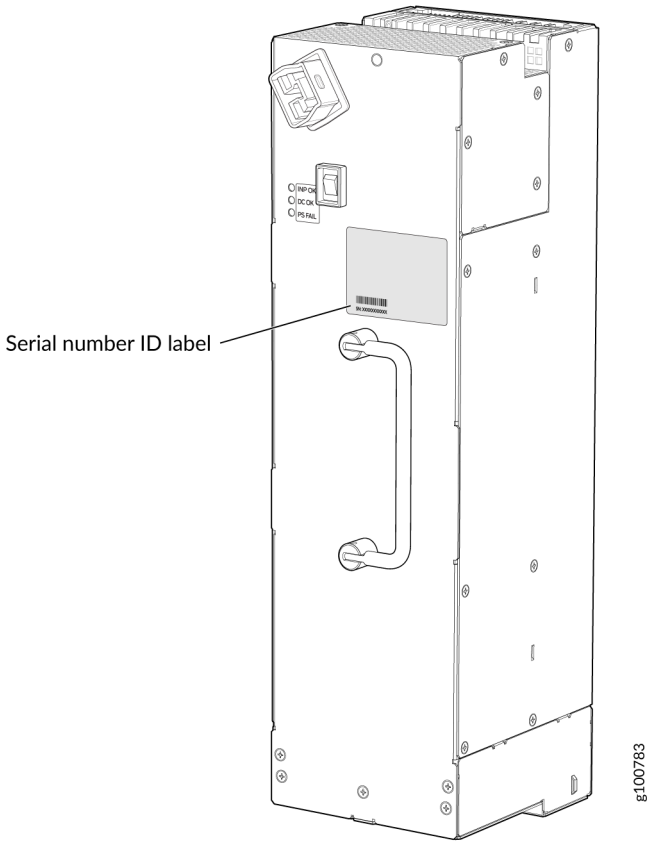
- High-Capacity Second-Generation AC Power Supply—The serial number label is under the on/off switch of the power supply. See Figure 184 on page 471.

Figure 184: High-Capacity Second-Generation AC Power Supply Serial Number Label



- High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supply—The serial number label is under the on/off switch of the power supply. See Figure 185 on page 472.

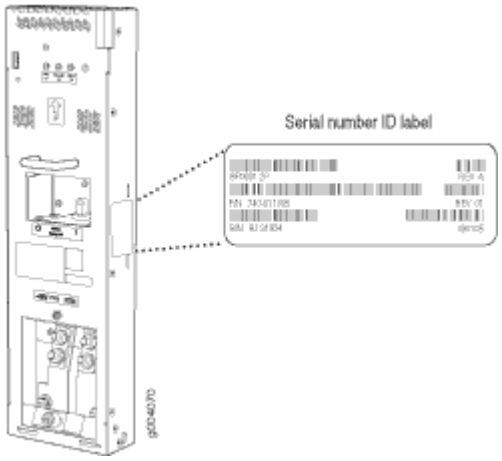
Figure 185: High-Voltage Second-Generation Universal (HVAC/HVDC) Power Supply Serial Number Label



DC power Supplies:

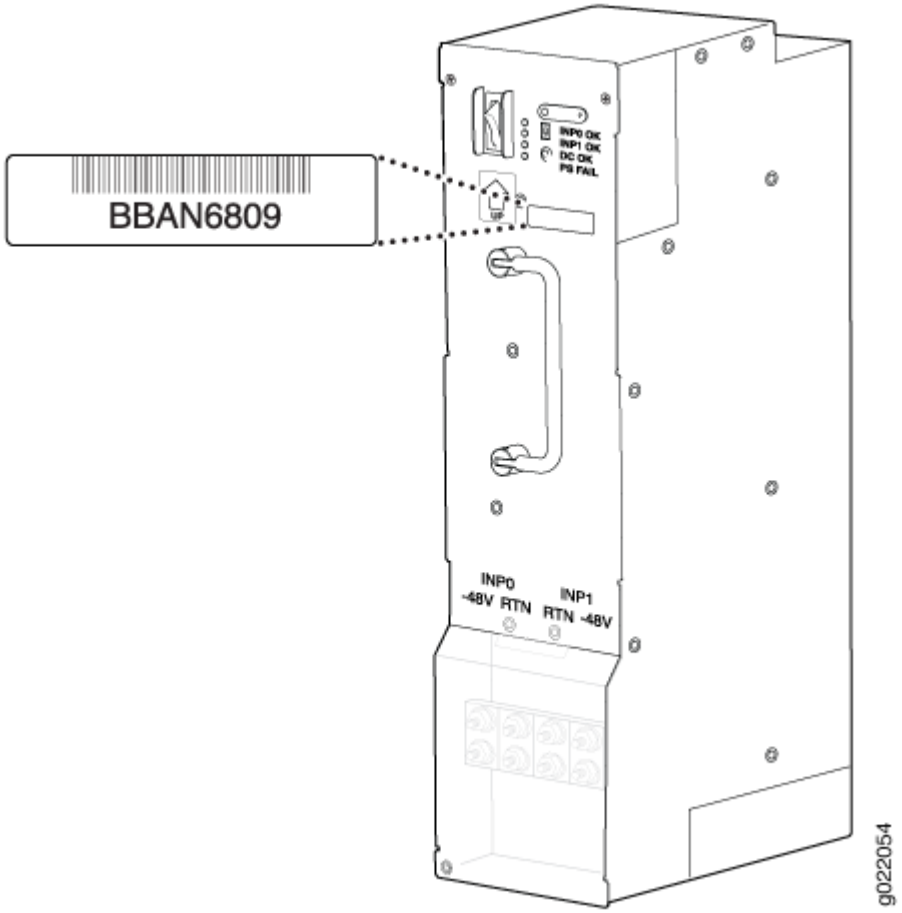
- Standard-Capacity DC Power Supply—The serial number label is on the DC power supply faceplate under the circuit breaker switch. See Figure 186 on page 473.

Figure 186: Standard-Capacity DC Power Supply Serial Number Label



- High-Capacity DC Power Supply—The serial number label is on the top of the DC power supply. See Figure 187 on page 474.

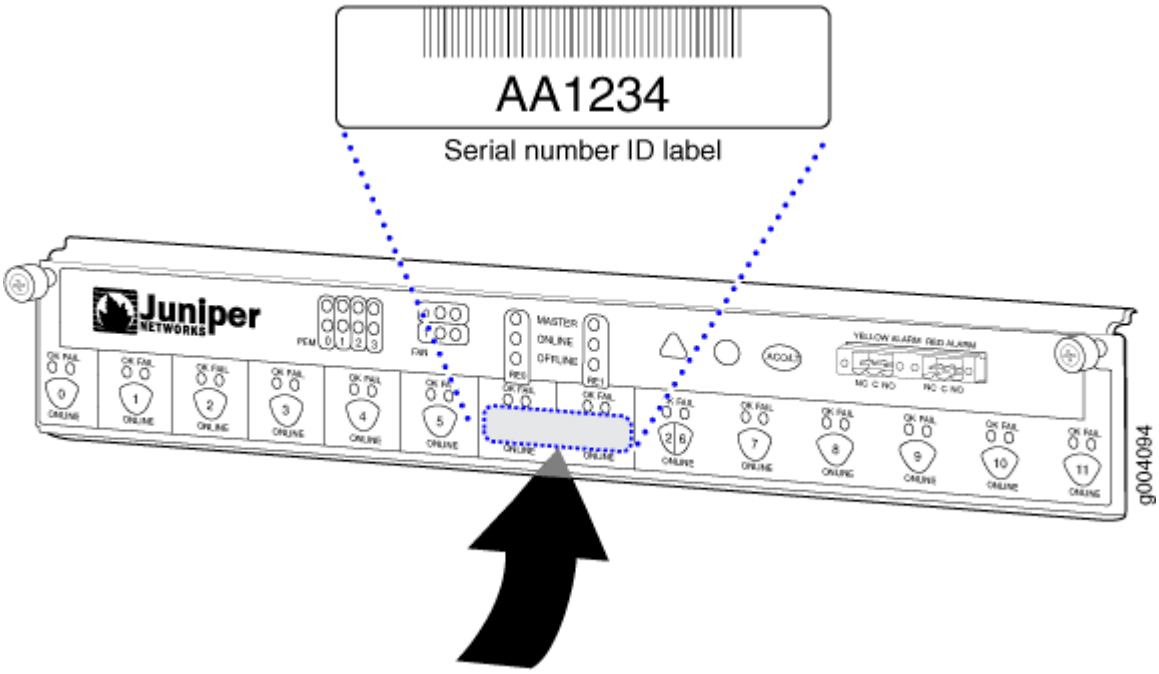
Figure 187: High-Capacity DC Power Supply Serial Number Label



Locating the SRX5800 Firewall Craft Interface Serial Number Label

The serial number is located on the back of the craft interface panel (see Figure 188 on page 475).

Figure 188: Craft Interface Serial Number Label



Information You Might Need to Supply to JTAC

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

- Your existing case number, if you have one
- Details of the failure or problem
- Type of activity being performed on the firewall when the problem occurred
- Configuration data displayed by one or more `show` commands
- Your name, organization name, telephone number, fax number, and shipping address

Required Tools and Parts for Packing the SRX5800 Firewall

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

- 2.5-mm flat-blade (–) screwdriver, for detaching alarm relay terminal block

- 7/16-in. (11 mm) nut driver
- Blank panels to cover empty slots
- Electrostatic bag or antistatic mat, for each component
- Electrostatic discharge (ESD) grounding wrist strap
- Flat-blade (–) screwdriver
- Mechanical lift, if available
- Phillips (+) screwdrivers, numbers 1 and 2
- Rubber safety cap for fiber-optic interfaces or cable
- Wire cutters

Packing the SRX5800 Firewall for Shipment

To pack the firewall for shipment:

1. Retrieve the shipping crate and packing materials in which the firewall was originally shipped. If you do not have these materials, contact your Juniper Networks representative about approved packaging materials.
2. On the console or other management device connected to the primary Routing Engine, enter CLI operational mode and issue the following command to shut down the firewall software.

   ```
   user@host> request system halt
   ```

   Wait until a message appears on the console confirming that the operating system has halted.

   For more information about the command, see *Junos OS System Basics and Services Command Reference* at www.juniper.net/documentation/.
3. Attach an ESD grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
4. Shut down power to the firewall by pressing the AC input switch or DC circuit breaker for all power supplies to the off (**O**) position.
5. Disconnect power from the firewall.
6. Remove the cables that connect to all external devices.
7. Remove all field replaceable units (FRUs) from the firewall.
8. Remove the firewall chassis from the rack:

- If you are using a mechanical lift, place the lift platform under the chassis, unscrew and remove the mounting screws from the rack, and move the chassis to the shipping crate.
- If you are not using a mechanical lift and the chassis weight is fully supported by a shelf or another device, unscrew and remove the mounting screws from the rack. Three people can then lift the chassis and move it to the shipping crate.
- If you are not using a mechanical lift and the chassis weight is not fully supported by a shelf or another device, three people should grasp the chassis while a fourth person unscrews and removes the mounting screws from the rack. The three lifters can then move the chassis to the shipping container.

9. Place the firewall in the shipping crate or onto the pallet. If on a pallet, bolt the firewall to the pallet.
10. Cover the firewall with an ESD bag and place the packing foam on top of and around the firewall.
11. Replace the accessory box on top of the packing foam.
12. Securely tape the box closed or place the crate cover over the firewall.
13. Write the RMA number on the exterior of the box to ensure proper tracking.

Packing SRX5800 Firewall Components for Shipment

Follow these guidelines for packing and shipping individual components of the firewall:

- When you return a component, make sure that it is adequately protected with packing materials and packed so that the pieces are prevented from moving around inside the carton.
- Use the original shipping materials if they are available.
- Place the individual component in an electrostatic bag.
- Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.

CAUTION: Do not stack any of the firewall components during packing.

CHAPTER 7

Safety and Compliance Information

General Safety Guidelines and Warnings

The following guidelines help ensure your safety and protect the device from damage. The list of guidelines might not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

- Perform only the procedures explicitly described in the hardware documentation for this device. Make sure that only authorized service personnel perform other system services.
- Keep the area around the device clear and free from dust before, during, and after installation.
- Keep tools away from areas where people could trip over them while walking.
- Do not wear loose clothing or jewelry, such as rings, bracelets, or chains, which could become caught in the device.
- Wear safety glasses if you are working under any conditions that could be hazardous to your eyes.
- Do not perform any actions that create a potential hazard to people or make the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person to handle.
- Never install or manipulate wiring during electrical storms.
- Never install electrical jacks in wet locations unless the jacks are specifically designed for wet environments.
- Operate the device only when it is properly grounded.
- Follow the instructions in this guide to properly ground the device to earth.
- Replace fuses only with fuses of the same type and rating.
- Do not open or remove chassis covers or sheet-metal parts unless instructions are provided in the hardware documentation for this device. Such an action could cause severe electrical shock.
- Do not push or force any objects through any opening in the chassis frame. Such an action could result in electrical shock or fire.
- Avoid spilling liquid onto the chassis or onto any device component. Such an action could cause electrical shock or damage the device.
- Avoid touching uninsulated electrical wires or terminals that have not been disconnected from their power source. Such an action could cause electrical shock.

- Some parts of the chassis, including AC and DC power supply surfaces, power supply unit handles, SFB card handles, and fan tray handles might become hot. The following label provides the warning for hot surfaces on the chassis:

- Always ensure that all modules, power supplies, and cover panels are fully inserted and that the installation screws are fully tightened.

Definitions of Safety Warning Levels

The documentation uses the following levels of safety warnings (there are two *Warning* formats):

NOTE: You might find this information helpful in a particular situation, or you might overlook this important information if it was not highlighted in a Note.

CAUTION: You need to observe the specified guidelines to prevent minor injury or discomfort to you or severe damage to the device.

Attention Veillez à respecter les consignes indiquées pour éviter toute incommodité ou blessure légère, voire des dégâts graves pour l'appareil.

LASER WARNING: This symbol alerts you to the risk of personal injury from a laser.

Avertissement Ce symbole signale un risque de blessure provoquée par rayon laser.

WARNING: This symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry, and familiarize yourself with standard practices for preventing accidents.

Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

Avertissement Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.

Avvertenza Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

Advarsel Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

¡Atención! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

Restricted Access Area Warning

WARNING: The Firewall is intended for installation in restricted access areas. A restricted access area is an area to which access can be gained only by service personnel through the use of a special tool, lock and key, or other means of security, and which is controlled by the authority responsible for the location.

Waarschuwing Dit toestel is bedoeld voor installatie op plaatsen met beperkte toegang. Een plaats met beperkte toegang is een plaats waar toegang slechts door servicepersoneel verkregen kan worden door middel van een speciaal instrument, een slot en sleutel, of een ander veiligheidsmiddel, en welke beheerd wordt door de overheidsinstantie die verantwoordelijk is voor de locatie.

Varoitus Tämä laite on tarkoitettu asennettavaksi paikkaan, johon pääsy on rajoitettua. Paikka, johon pääsy on rajoitettua, tarkoittaa paikkaa, johon vain huoltohenkilöstö pääsee jonkin erikoistyökalun, lukkoon sopivan avaimen tai jonkin muun turvalaitteen avulla ja joka on paikasta vastuussa olevien toimivaltaisten henkilöiden valvoma.

Attention Cet appareil est à installer dans des zones d'accès réservé. Ces dernières sont des zones auxquelles seul le personnel de service peut accéder en utilisant un outil spécial, un mécanisme de verrouillage et une clé, ou tout autre moyen de sécurité. L'accès aux zones de sécurité est sous le contrôle de l'autorité responsable de l'emplacement.

Warnung Diese Einheit ist zur Installation in Bereichen mit beschränktem Zutritt vorgesehen. Ein Bereich mit beschränktem Zutritt ist ein Bereich, zu dem nur Wartungspersonal mit einem Spezialwerkzeugs, Schloß und Schlüssel oder anderer Sicherheitsvorkehrungen Zugang hat, und der von dem für die Anlage zuständigen Gremium kontrolliert wird.

Avvertenza Questa unità deve essere installata in un'area ad accesso limitato. Un'area ad accesso limitato è un'area accessibile solo a personale di assistenza tramite un'attrezzo speciale, lucchetto, o altri dispositivi di sicurezza, ed è controllata dall'autorità responsabile della zona.

Advarsel Denne enheten er laget for installasjon i områder med begrenset adgang. Et område med begrenset adgang gir kun adgang til servicepersonale som bruker et spesielt verktøy, lås og nøkkel, eller en annen sikkerhetsanordning, og det kontrolleres av den autoriteten som er ansvarlig for området.

Aviso Esta unidade foi concebida para instalação em áreas de acesso restrito. Uma área de acesso restrito é uma área à qual apenas tem acesso o pessoal de serviço autorizado,

que possua uma ferramenta, chave e fechadura especial, ou qualquer outra forma de segurança. Esta área é controlada pela autoridade responsável pelo local.

¡Atención! Esta unidad ha sido diseñada para instalarse en áreas de acceso restringido. Área de acceso restringido significa un área a la que solamente tiene acceso el personal de servicio mediante la utilización de una herramienta especial, cerradura con llave, o algún otro medio de seguridad, y que está bajo el control de la autoridad responsable del local.

Varning! Denna enhet är avsedd för installation i områden med begränsat tillträde. Ett område med begränsat tillträde får endast tillträdas av servicepersonal med ett speciellt verktyg, lås och nyckel, eller annan säkerhetsanordning, och kontrolleras av den auktoritet som ansvarar för området.

RELATED DOCUMENTATION

- *Definitions of Safety Warning Levels*
- *General Safety Guidelines and Warnings*
- *Qualified Personnel Warning*
- *Prevention of Electrostatic Discharge Damage*

Fire Safety Requirements

IN THIS SECTION

In the event of a fire emergency, the safety of people is the primary concern. You should establish procedures for protecting people in the event of a fire emergency, provide safety training, and properly provision fire-control equipment and fire extinguishers.

In addition, you should establish procedures to protect your equipment in the event of a fire emergency. Juniper Networks products should be installed in an environment suitable for electronic equipment. We

recommend that fire suppression equipment be available in the event of a fire in the vicinity of the equipment and that all local fire, safety, and electrical codes and ordinances be observed when you install and operate your equipment.

Fire Suppression

In the event of an electrical hazard or an electrical fire, you should first turn power off to the equipment at the source. Then use a Type C fire extinguisher, which uses noncorrosive fire retardants, to extinguish the fire.

Fire Suppression Equipment

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

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

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

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

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

Qualified Personnel Warning

WARNING: Only trained and qualified personnel should install or replace the device.
Waarschuwing Installatie en reparaties mogen uitsluitend door getraind en bevoegd personeel uitgevoerd worden.

Varoitus Ainoastaan koulutettu ja pätevä henkilökunta saa asentaa tai vaihtaa tämän laitteen.

Avertissement Tout installation ou remplacement de l'appareil doit être réalisé par du personnel qualifié et compétent.

Warnung Gerät nur von geschultem, qualifiziertem Personal installieren oder auswechseln lassen.

Avvertenza Solo personale addestrato e qualificato deve essere autorizzato ad installare o sostituire questo apparecchio.

Advarsel Kun kvalifisert personell med riktig opplæring bør montere eller bytte ut dette utstyret.

Aviso Este equipamento deverá ser instalado ou substituído apenas por pessoal devidamente treinado e qualificado.

¡Atención! Estos equipos deben ser instalados y reemplazados exclusivamente por personal técnico adecuadamente preparado y capacitado.

Varning! Denna utrustning ska endast installeras och bytas ut av utbildad och kvalificerad personal.

Warning Statement for Norway and Sweden

WARNING: The equipment must be connected to an earthed mains socket-outlet.
Advarsel Apparatet skal kobles til en jordet stikkontakt.

Varning! Apparaten skall anslutas till jordat nätuttag.

Installation Instructions Warning

WARNING: Read the installation instructions before you connect the device to a power source.

Waarschuwing Raadpleeg de installatie-aanwijzingen voordat u het systeem met de voeding verbindt.

Varoitus Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.

Avertissement Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.

Warnung Lesen Sie die Installationsanweisungen, bevor Sie das System an die Stromquelle anschließen.

Avvertenza Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.

Advarsel Les installasjonsinstruksjonene før systemet kobles til strømkilden.

Aviso Leia as instruções de instalação antes de ligar o sistema à sua fonte de energia.

¡Atención! Ver las instrucciones de instalación antes de conectar el sistema a la red de alimentación.

Varning! Läs installationsanvisningarna innan du kopplar systemet till dess strömförsörjningsenhet.

Chassis and Component Lifting Guidelines

- Before moving the device to a site, ensure that the site meets the power, environmental, and clearance requirements.
- Before lifting or moving the device, disconnect all external cables and wires.
- As when lifting any heavy object, ensure that your legs bear most of the weight rather than your back. Keep your knees bent and your back relatively straight. Do not twist your body as you lift. Balance the load evenly and be sure that your footing is firm.
- Use the following lifting guidelines to lift devices and components:

- Up to 39.7 lb (18 kg): One person.
- From 39.7 lb (18 kg) to 70.5 lb (32 kg): Two or more people.
- From 70.5 lb (32 kg) to 121.2 lb (55 kg): Three or more people.
- Above 121.2 lb (55 kg): Use material handling systems (such as levers, slings, lifts, and so on). When this is not practical, engage specially trained persons or systems (such as riggers or movers).

Ramp Warning

WARNING: When installing the device, do not use a ramp inclined at more than 10 degrees.

Waarschuwing Gebruik een oprijplaat niet onder een hoek van meer dan 10 graden.

Varoitus Älä käytä sellaista kaltevaa pintaa, jonka kaltevuus ylittää 10 astetta.

Avertissement Ne pas utiliser une rampe dont l'inclinaison est supérieure à 10 degrés.

Warnung Keine Rampen mit einer Neigung von mehr als 10 Grad verwenden.

Avvertenza Non usare una rampa con pendenza superiore a 10 gradi.

Advarsel Bruk aldri en rampe som heller mer enn 10 grader.

Aviso Não utilize uma rampa com uma inclinação superior a 10 graus.

¡Atención! No usar una rampa inclinada más de 10 grados.

Varning! Använd inte ramp med en lutning på mer än 10 grader.

Rack-Mounting and Cabinet-Mounting Warnings

Ensure that the rack or cabinet in which the device is installed is evenly and securely supported. Uneven mechanical loading could lead to a hazardous condition.

WARNING: To prevent bodily injury when mounting or servicing the device in a rack, take the following precautions to ensure that the system remains stable. The following directives help maintain your safety:

- Install the device in a rack that is secured to the building structure.
- Mount the device at the bottom of the rack if it is the only unit in the rack.
- When mounting the device on a partially filled rack, load the rack from the bottom to the top, with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing equipment, install the stabilizers before mounting or servicing the device in the rack.

Waarschuwing Om lichamelijk letsel te voorkomen wanneer u dit toestel in een rek monteert of het daar een servicebeurt geeft, moet u speciale voorzorgsmaatregelen nemen om ervoor te zorgen dat het toestel stabiel blijft. De onderstaande richtlijnen worden verstrekt om uw veiligheid te verzekeren:

- De Juniper Networks switch moet in een stellage worden geïnstalleerd die aan een bouwsel is verankerd.
- Dit toestel dient onderaan in het rek gemonteerd te worden als het toestel het enige in het rek is.
- Wanneer u dit toestel in een gedeeltelijk gevuld rek monteert, dient u het rek van onderen naar boven te laden met het zwaarste onderdeel onderaan in het rek.
- Als het rek voorzien is van stabiliseringshulpmiddelen, dient u de stabilisatoren te monteren voordat u het toestel in het rek monteert of het daar een servicebeurt geeft.

Varoitus Kun laite asetetaan telineeseen tai huolletaan sen ollessa telineessä, on noudatettava erityisiä varotoimia järjestelmän vakavuuden säilyttämiseksi, jotta vältytään loukkaantumiselta. Noudata seuraavia turvallisuusohjeita:

- Juniper Networks switch on asennettava telineeseen, joka on kiinnitetty rakennukseen.
- Jos telineessä ei ole muita laitteita, aseta laite telineen alaosaan.
- Jos laite asetetaan osaksi täytettyyn telineeseen, aloita kuormittaminen sen alaosasta kaikkein raskaimmalla esineellä ja siirry sitten sen yläosaan.

- Jos telinettä varten on vakaimet, asenna ne ennen laitteen asettamista telineeseen tai sen huoltamista siinä.

Avertissement Pour éviter toute blessure corporelle pendant les opérations de montage ou de réparation de cette unité en casier, il convient de prendre des précautions spéciales afin de maintenir la stabilité du système. Les directives ci-dessous sont destinées à assurer la protection du personnel:

- Le rack sur lequel est monté le Juniper Networks switch doit être fixé à la structure du bâtiment.
- Si cette unité constitue la seule unité montée en casier, elle doit être placée dans le bas.
- Si cette unité est montée dans un casier partiellement rempli, charger le casier de bas en haut en plaçant l'élément le plus lourd dans le bas.
- Si le casier est équipé de dispositifs stabilisateurs, installer les stabilisateurs avant de monter ou de réparer l'unité en casier.

Warnung Zur Vermeidung von Körperverletzung beim Anbringen oder Warten dieser Einheit in einem Gestell müssen Sie besondere Vorkehrungen treffen, um sicherzustellen, daß das System stabil bleibt. Die folgenden Richtlinien sollen zur Gewährleistung Ihrer Sicherheit dienen:

- Der Juniper Networks switch muß in einem Gestell installiert werden, das in der Gebäudestruktur verankert ist.
- Wenn diese Einheit die einzige im Gestell ist, sollte sie unten im Gestell angebracht werden.
- Bei Anbringung dieser Einheit in einem zum Teil gefüllten Gestell ist das Gestell von unten nach oben zu laden, wobei das schwerste Bauteil unten im Gestell anzubringen ist.
- Wird das Gestell mit Stabilisierungszubehör geliefert, sind zuerst die Stabilisatoren zu installieren, bevor Sie die Einheit im Gestell anbringen oder sie warten.

Avvertenza Per evitare infortuni fisici durante il montaggio o la manutenzione di questa unità in un supporto, occorre osservare speciali precauzioni per garantire che il sistema rimanga stabile. Le seguenti direttive vengono fornite per garantire la sicurezza personale:

- Il Juniper Networks switch deve essere installato in un telaio, il quale deve essere fissato alla struttura dell'edificio.
- Questa unità deve venire montata sul fondo del supporto, se si tratta dell'unica unità da montare nel supporto.
- Quando questa unità viene montata in un supporto parzialmente pieno, caricare il supporto dal basso all'alto, con il componente più pesante sistemato sul fondo del supporto.
- Se il supporto è dotato di dispositivi stabilizzanti, installare tali dispositivi prima di montare o di procedere alla manutenzione dell'unità nel supporto.

Advarsel Unngå fysiske skader under montering eller reparasjonsarbeid på denne enheten når den befinner seg i et kabinett. Vær nøye med at systemet er stabilt. Følgende retningslinjer er gitt for å verne om sikkerheten:

- Juniper Networks switch må installeres i et stativ som er forankret til bygningsstrukturen.
- Denne enheten bør monteres nederst i kabinettet hvis dette er den eneste enheten i kabinettet.
- Ved montering av denne enheten i et kabinett som er delvis fylt, skal kabinettet lastes fra bunnen og opp med den tyngste komponenten nederst i kabinettet.
- Hvis kabinettet er utstyrt med stabiliseringsutstyr, skal stabilisatorene installeres før montering eller utføring av reparasjonsarbeid på enheten i kabinettet.

Aviso Para se prevenir contra danos corporais ao montar ou reparar esta unidade numa estante, deverá tomar precauções especiais para se certificar de que o sistema possui um suporte estável. As seguintes directrizes ajudá-lo-ão a efectuar o seu trabalho com segurança:

- O Juniper Networks switch deverá ser instalado numa prateleira fixa à estrutura do edificio.
- Esta unidade deverá ser montada na parte inferior da estante, caso seja esta a única unidade a ser montada.
- Ao montar esta unidade numa estante parcialmente ocupada, coloque os itens mais pesados na parte inferior da estante, arrumando-os de baixo para cima.

- Se a estante possuir um dispositivo de estabilização, instale-o antes de montar ou reparar a unidade.

¡Atención! Para evitar lesiones durante el montaje de este equipo sobre un bastidor, oeriormente durante su mantenimiento, se debe poner mucho cuidado en que el sistema quede bien estable. Para garantizar su seguridad, proceda según las siguientes instrucciones:

- El Juniper Networks switch debe instalarse en un bastidor fijado a la estructura del edificio.
- Colocar el equipo en la parte inferior del bastidor, cuando sea la única unidad en el mismo.
- Cuando este equipo se vaya a instalar en un bastidor parcialmente ocupado, comenzar la instalación desde la parte inferior hacia la superior colocando el equipo más pesado en la parte inferior.
- Si el bastidor dispone de dispositivos estabilizadores, instalar éstos antes de montar o proceder al mantenimiento del equipo instalado en el bastidor.

Varning! För att undvika kroppsskada när du installerar eller utför underhållsarbete på denna enhet på en ställning måste du vidta särskilda försiktighetsåtgärder för att försäkra dig om att systemet står stadigt. Följande riktlinjer ges för att trygga din säkerhet:

- Juniper Networks switch måste installeras i en ställning som är förankrad i byggnadens struktur.
- Om denna enhet är den enda enheten på ställningen skall den installeras längst ned på ställningen.
- Om denna enhet installeras på en delvis fylld ställning skall ställningen fyllas nedifrån och upp, med de tyngsta enheterna längst ned på ställningen.
- Om ställningen är försedd med stabiliseringsdon skall dessa monteras fast innan enheten installeras eller underhålls på ställningen.

Grounded Equipment Warning

WARNING: This device must be properly grounded at all times. Follow the instructions in this guide to properly ground the device to earth.

Waarschuwing Dit apparaat moet altijd goed geaard zijn. Volg de instructies in deze gids om het apparaat goed te aarden.

Varoitus Laitteen on oltava pysyvästi maadoitettu. Maadoita laite asianmukaisesti noudattamalla tämän oppaan ohjeita.

Avertissement L'appareil doit être correctement mis à la terre à tout moment. Suivez les instructions de ce guide pour correctement mettre l'appareil à la terre.

Warnung Das Gerät muss immer ordnungsgemäß geerdet sein. Befolgen Sie die Anweisungen in dieser Anleitung, um das Gerät ordnungsgemäß zu erden.

Avvertenza Questo dispositivo deve sempre disporre di una connessione a massa. Seguire le istruzioni indicate in questa guida per connettere correttamente il dispositivo a massa.

Advarsel Denne enheten på jordes skikkelig hele tiden. Følg instruksjonene i denne veiledningen for å jorde enheten.

Aviso Este equipamento deverá estar ligado à terra. Siga las instrucciones en esta guía para conectar correctamente este dispositivo a tierra.

¡Atención! Este dispositivo debe estar correctamente conectado a tierra en todo momento. Siga las instrucciones en esta guía para conectar correctamente este dispositivo a tierra.

Varning! Den här enheten måste vara ordentligt jordad. Följ instruktionerna i den här guiden för att jorda enheten ordentligt.

Laser and LED Safety Guidelines and Warnings

IN THIS SECTION

Juniper Networks devices are equipped with laser transmitters, which are considered a Class 1 Laser Product by the U.S. Food and Drug Administration and are evaluated as a Class 1 Laser Product per IEC/EN 60825-1 requirements.

Observe the following guidelines and warnings:

General Laser Safety Guidelines

When working around ports that support optical transceivers, observe the following safety guidelines to prevent eye injury:

- Do not look into unterminated ports or at fibers that connect to unknown sources.
- Do not examine unterminated optical ports with optical instruments.
- Avoid direct exposure to the beam.

LASER WARNING: Unterminated optical connectors can emit invisible laser radiation. The lens in the human eye focuses all the laser power on the retina, so focusing the eye directly on a laser source—even a low-power laser—could permanently damage the eye.

Avertissement Les connecteurs à fibre optique sans terminaison peuvent émettre un rayonnement laser invisible. Le cristallin de l'œil humain faisant converger toute la puissance du laser sur la rétine, toute focalisation directe de l'œil sur une source laser, —même de faible puissance—, peut entraîner des lésions oculaires irréversibles.

Class 1 Laser Product Warning

LASER WARNING: Class 1 laser product.
Waarschuwing Klasse-1 laser produkt.

Varoitus Luokan 1 lasertuote.

Avertissement Produit laser de classe I.

Warnung Laserprodukt der Klasse 1.

Avvertenza Prodotto laser di Classe 1.

Advarsel Laserprodukt av klasse 1.

Aviso Produto laser de classe 1.

¡Atención! Producto láser Clase I.

Varning! Laserprodukt av klass 1.

Class 1 LED Product Warning

LASER WARNING: Class 1 LED product.
Waarschuwing Klasse 1 LED-product.

Varoitus Luokan 1 valodiodituote.

Avertissement Alarme de produit LED Class I.

Warnung Class 1 LED-Produktwarnung.

Avvertenza Avvertenza prodotto LED di Classe 1.

Advarsel LED-produkt i klasse 1.

Aviso Produto de classe 1 com LED.

¡Atención! Aviso sobre producto LED de Clase 1.

Varning! Lysdiodprodukt av klass 1.

Laser Beam Warning

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

Waarschuwing Niet in de straal staren of hem rechtstreeks bekijken met optische instrumenten.

Varoitus Älä katso säteeseen äläkä tarkastele sitä suoraan optisen laitteen avulla.

Avertissement Ne pas fixer le faisceau des yeux, ni l'observer directement à l'aide d'instruments optiques.

Warnung Nicht direkt in den Strahl blicken und ihn nicht direkt mit optischen Geräten prüfen.

Avvertenza Non fissare il raggio con gli occhi né usare strumenti ottici per osservarlo direttamente.

Advarsel Stirr eller se ikke direkte p strlen med optiske instrumenter.

Aviso Não olhe fixamente para o raio, nem olhe para ele directamente com instrumentos ópticos.

¡Atención! No mirar fijamente el haz ni observarlo directamente con instrumentos ópticos.

Varning! Rikta inte blicken in mot strålen och titta inte direkt på den genom optiska instrument.

Radiation from Open Port Apertures Warning

LASER WARNING: Because invisible radiation might be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.

Waarschuwing Aangezien onzichtbare straling vanuit de opening van de poort kan komen als er geen fiberkabel aangesloten is, dient blootstelling aan straling en het kijken in open openingen vermeden te worden.

Varoitus Koska portin aukosta voi emittoitua näkymätöntä säteilyä, kun kuitukaapelia ei ole kytkettynä, vältä säteilylle altistumista äläkä katso avoimiin aukkoihin.

Avertissement Des radiations invisibles à l'il nu pouvant traverser l'ouverture du port lorsqu'aucun câble en fibre optique n'y est connecté, il est recommandé de ne pas regarder fixement l'intérieur de ces ouvertures.

Warnung Aus der Port-Öffnung können unsichtbare Strahlen emittieren, wenn kein Glasfaserkabel angeschlossen ist. Vermeiden Sie es, sich den Strahlungen auszusetzen, und starren Sie nicht in die Öffnungen!

Avvertenza Quando i cavi in fibra non sono inseriti, radiazioni invisibili possono essere emesse attraverso l'apertura della porta. Evitate di esporvi alle radiazioni e non guardate direttamente nelle aperture.

Advarsel Unngå utsettelse for stråling, og stirr ikke inn i åpninger som er åpne, fordi usynlig stråling kan emiteres fra portens åpning når det ikke er tilkoblet en fiberkabel.

Aviso Dada a possibilidade de emissão de radiação invisível através do orifício da via de acesso, quando esta não tiver nenhum cabo de fibra conectado, deverá evitar an EXposição à radiação e não deverá olhar fixamente para orifícios que se encontrarem a descoberto.

¡Atención! Debido a que la apertura del puerto puede emitir radiación invisible cuando no existe un cable de fibra conectado, evite mirar directamente a las aperturas para no exponerse a la radiación.

Varning! Osynlig strålning kan avges från en portöppning utan ansluten fiberkabel och du bör därför undvika att bli utsatt för strålning genom att inte stirra in i oskyddade öppningar.

Maintenance and Operational Safety Guidelines and Warnings

IN THIS SECTION

While performing the maintenance activities for devices, observe the following guidelines and warnings:

Battery Handling Warning

WARNING: Replacing a battery incorrectly might result in an explosion. Replace a battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Waarschuwing Er is ontploffingsgevaar als de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type dat door de fabrikant aanbevolen is. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften weggeworpen te worden.

Varoitus Räjähdyksen vaara, jos akku on vaihdettu väärään akkuun. Käytä vaihtamiseen ainoastaan saman- tai vastaavantyyppistä akkua, joka on valmistajan suosittelema. Hävitä käytetyt akut valmistajan ohjeiden mukaan.

Avertissement Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.

Warnung Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

Advarsel Det kan være fare for eksplosjon hvis batteriet skiftes på feil måte. Skift kun med samme eller tilsvarende type som er anbefalt av produsenten. Kasser brukte batterier i henhold til produsentens instruksjoner.

Avvertenza Pericolo di esplosione se la batteria non è installata correttamente. Sostituire solo con una di tipo uguale o equivalente, consigliata dal produttore. Eliminare le batterie usate secondo le istruzioni del produttore.

Aviso Existe perigo de explosão se a bateria for substituída incorrectamente. Substitua a bateria por uma bateria igual ou de um tipo equivalente recomendado pelo fabricante. Destrua as baterias usadas conforme as instruções do fabricante.

¡Atención! Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la baterían EXclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.

Varning! Explosionsfara vid felaktigt batteribyte. Ersätt endast batteriet med samma batterityp som rekommenderas av tillverkaren eller motsvarande. Följ tillverkarens anvisningar vid kassering av använda batterier.

Jewelry Removal Warning

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

Waarschuwing Alvorens aan apparatuur te werken die met elektrische leidingen is verbonden, sieraden (inclusief ringen, kettingen en horloges) verwijderen. Metalen voorwerpen worden warm wanneer ze met stroom en aarde zijn verbonden, en kunnen ernstige brandwonden veroorzaken of het metalen voorwerp aan de aansluitklemmen lassen.

Varoitus Ennen kuin työskentelet voimavirtajohtoihin kytkettyjen laitteiden parissa, ota pois kaikki korut (sormukset, kaulakorut ja kellot mukaan lukien). Metalliesineet kuumenevat, kun ne ovat yhteydessä sähkövirran ja maan kanssa, ja ne voivat aiheuttaa vakavia palovammoja tai hitsata metalliesineet kiinni liitäntänapoihin.

Avertissement Avant d'accéder à cet équipement connecté aux lignes électriques, ôter tout bijou (anneaux, colliers et montres compris). Lorsqu'ils sont branchés à l'alimentation et reliés à la terre, les objets métalliques chauffent, ce qui peut provoquer des blessures graves ou souder l'objet métallique aux bornes.

Warnung Vor der Arbeit an Geräten, die an das Netz angeschlossen sind, jeglichen Schmuck (einschließlich Ringe, Ketten und Uhren) abnehmen. Metallgegenstände erhitzen sich, wenn sie an das Netz und die Erde angeschlossen werden, und können schwere Verbrennungen verursachen oder an die Anschlußklemmen angeschweißt werden.

Avvertenza Prima di intervenire su apparecchiature collegate alle linee di alimentazione, togliersi qualsiasi monile (inclusi anelli, collane, braccialetti ed orologi). Gli oggetti metallici si riscaldano quando sono collegati tra punti di alimentazione e massa: possono causare ustioni gravi oppure il metallo può saldarsi ai terminali.

Advarsel Fjern alle smykker (inkludert ringer, halskjeder og klokker) før du skal arbeide på utstyr som er koblet til kraftledninger. Metallgjenstander som er koblet til kraftledninger og jord blir svært varme og kan forårsake alvorlige brannskader eller smelte fast til polene.

Aviso Antes de trabalhar em equipamento que esteja ligado a linhas de corrente, retire todas as jóias que estiver a usar (incluindo anéis, fios e relógios). Os objectos metálicos aquecerão em contacto com a corrente e em contacto com a ligação à terra, podendo causar queimaduras graves ou ficarem soldados aos terminais.

¡Atención! Antes de operar sobre equipos conectados a líneas de alimentación, quitarse las joyas (incluidos anillos, collares y relojes). Los objetos de metal se calientan cuando se conectan a la alimentación y a tierra, lo que puede ocasionar quemaduras graves o que los objetos metálicos queden soldados a los bornes.

Varning! Tag av alla smycken (inklusive ringar, halsband och armbandsur) innan du arbetar på utrustning som är kopplad till kraftledningar. Metallobjekt hettas upp när de kopplas ihop med ström och jord och kan förorsaka allvarliga brännskador; metallobjekt kan också sammansvetsas med kontakterna.

Lightning Activity Warning

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

Waarschuwing Tijdens onweer dat gepaard gaat met bliksem, dient u niet aan het systeem te werken of kabels aan te sluiten of te ontkoppelen.

Varoitus Älä työskentele järjestelmän parissa äläkä yhdistä tai irrota kaapeleita ukkosilmalla.

Avertissement Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage.

Warnung Arbeiten Sie nicht am System und schließen Sie keine Kabel an bzw. trennen Sie keine ab, wenn es gewittert.

Avvertenza Non lavorare sul sistema o collegare oppure scollegare i cavi durante un temporale con fulmini.

Advarsel Utfør aldri arbeid på systemet, eller koble kabler til eller fra systemet når det tordner eller lyner.

Aviso Não trabalhe no sistema ou ligue e desligue cabos durante períodos de mau tempo (trovoada).

¡Atención! No operar el sistema ni conectar o desconectar cables durante el transcurso de descargas eléctricas en la atmósfera.

Varning! Vid åska skall du aldrig utföra arbete på systemet eller ansluta eller koppla loss kablar.

Operating Temperature Warning

WARNING: To prevent the device from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature. To prevent airflow restriction, allow at least 6 in. (15.2 cm) of clearance around the ventilation openings.

Waarschuwing Om te voorkomen dat welke switch van de Juniper Networks router dan ook oververhit raakt, dient u deze niet te bedienen op een plaats waar de maximale aanbevolen omgevingstemperatuur van 40° C wordt overschreden. Om te voorkomen dat de luchtstroom wordt beperkt, dient er minstens 15,2 cm speling rond de ventilatie-openingen te zijn.

Varoitus Ettei Juniper Networks switch-sarjan reititin ylikuumentuisi, sitä ei saa käyttää tilassa, jonka lämpötila ylittää korkeimman suositellun ympäristölämpötilan 40° C. Ettei ilmanvaihto estyisi, tuuletusaukkojen ympärille on jätettävä ainakin 15,2 cm tilaa.

Avertissement Pour éviter toute surchauffe des routeurs de la gamme Juniper Networks switch, ne l'utilisez pas dans une zone où la température ambiante est supérieure à 40° C. Pour permettre un flot d'air constant, dégagez un espace d'au moins 15,2 cm autour des ouvertures de ventilations.

Warnung Um einen Router der switch vor Überhitzung zu schützen, darf dieser nicht in einer Gegend betrieben werden, in der die Umgebungstemperatur das empfohlene

Maximum von 40° C überschreitet. Um Lüftungsverschluß zu verhindern, achten Sie darauf, daß mindestens 15,2 cm lichter Raum um die Lüftungsöffnungen herum frei bleibt.

Avvertenza Per evitare il surriscaldamento dei switch, non adoperateli in un locale che ecceda la temperatura ambientale massima di 40° C. Per evitare che la circolazione dell'aria sia impedita, lasciate uno spazio di almeno 15.2 cm di fronte alle aperture delle ventole.

Advarsel Unngå overoppheting av eventuelle rutere i Juniper Networks switch Disse skal ikke brukes på steder der den anbefalte maksimale omgivelsestemperaturen overstiger 40° C (104° F). Sørg for at klaringen rundt lufteåpningene er minst 15,2 cm (6 tommer) for å forhindre nedsatt luftsirkulasjon.

Aviso Para evitar o sobreaquecimento do encaminhador Juniper Networks switch, não utilize este equipamento numa área que exceda a temperatura máxima recomendada de 40° C. Para evitar a restrição à circulação de ar, deixe pelo menos um espaço de 15,2 cm à volta das aberturas de ventilação.

¡Atención! Para impedir que un encaminador de la serie Juniper Networks switch se recaliente, no lo haga funcionar en un área en la que se supere la temperatura ambiente máxima recomendada de 40° C. Para impedir la restricción de la entrada de aire, deje un espacio mínimo de 15,2 cm alrededor de las aperturas para ventilación.

Varning! Förhindra att en Juniper Networks switch överhettas genom att inte använda den i ett område där den maximalt rekommenderade omgivningstemperaturen på 40° C överskrids. Förhindra att luftcirkulationen inskränks genom att se till att det finns fritt utrymme på minst 15,2 cm omkring ventilationsöppningarna.

Product Disposal Warning

WARNING: Disposal of this device must be handled according to all national laws and regulations.

Waarschuwing Dit produkt dient volgens alle landelijke wetten en voorschriften te worden afgedankt.

Varoitus Tämän tuotteen lopullisesta hävittämisestä tulee huolehtia kaikkia valtakunnallisia lakeja ja säännöksiä noudattaen.

Avertissement La mise au rebut définitive de ce produit doit être effectuée conformément à toutes les lois et réglementations en vigueur.

Warnung Dieses Produkt muß den geltenden Gesetzen und Vorschriften entsprechend entsorgt werden.

Avvertenza L'eliminazione finale di questo prodotto deve essere eseguita osservando le normative italiane vigenti in materia

Advarsel Endelig disponering av dette produktet må skje i henhold til nasjonale lover og forskrifter.

Aviso A descartagem final deste produto deverá ser efectuada de acordo com os regulamentos e a legislação nacional.

¡Atención! El desecho final de este producto debe realizarse según todas las leyes y regulaciones nacionales

Varning! Slutlig kassering av denna produkt bör skötas i enlighet med landets alla lagar och föreskrifter.

General Electrical Safety Guidelines and Warnings

WARNING: Certain ports on the device are designed for use as intrabuilding (within-the-building) interfaces only (Type 2 or Type 4 ports as described in *GR-1089-CORE*) and require isolation from the exposed outside plant (OSP) cabling. To comply with NEBS (Network Equipment-Building System) requirements and protect against lightning surges and commercial power disturbances, the intrabuilding ports *must not* be metallically connected to interfaces that connect to the OSP or its wiring. The intrabuilding ports on the device are suitable for connection to intrabuilding or unexposed wiring or cabling only. The addition of primary protectors is not sufficient protection for connecting these interfaces metallically to OSP wiring.

Avertissement Certains ports de l'appareil sont destinés à un usage en intérieur uniquement (ports Type 2 ou Type 4 tels que décrits dans le document *GR-1089-CORE*) et doivent être isolés du câblage de l'installation extérieure exposée. Pour respecter les exigences NEBS et assurer une protection contre la foudre et les perturbations de tension secteur, les ports pour intérieur *ne doivent pas* être raccordés physiquement aux interfaces prévues pour la connexion à l'installation extérieure ou à son câblage. Les

ports pour intérieur de l'appareil sont réservés au raccordement de câbles pour intérieur ou non exposés uniquement. L'ajout de protections ne constitue pas une précaution suffisante pour raccorder physiquement ces interfaces au câblage de l'installation extérieure.

CAUTION: Before removing or installing components of a device, connect an electrostatic discharge (ESD) grounding strap to an ESD point and wrap and fasten the other end of the strap around your bare wrist. Failure to use an ESD grounding strap could result in damage to the device.

Attention Avant de retirer ou d'installer des composants d'un appareil, raccordez un bracelet antistatique à un point de décharge électrostatique et fixez le bracelet à votre poignet nu. L'absence de port d'un bracelet antistatique pourrait provoquer des dégâts sur l'appareil.

- Install the device in compliance with the following local, national, and international electrical codes:
  - United States—National Fire Protection Association (NFPA 70), United States National Electrical Code.
  - Other countries—International Electromechanical Commission (IEC) 60364, Part 1 through Part 7.
  - Evaluated to the TN power system.
  - Canada—Canadian Electrical Code, Part 1, CSA C22.1.
  - Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.

    Peut être installé dans des salles de matériel de traitement de l'information conformément à l'article 645 du National Electrical Code et à la NFPA 75.
- Locate the emergency power-off switch for the room in which you are working so that if an electrical accident occurs, you can quickly turn off the power.
- Make sure that you clean grounding surface and give them a bright finish before making grounding connections.
- Do not work alone if potentially hazardous conditions exist anywhere in your workspace.
- Never assume that power is disconnected from a circuit. Always check the circuit before starting to work.
- Carefully look for possible hazards in your work area, such as moist floors, ungrounded power extension cords, and missing safety grounds.

- Operate the device within marked electrical ratings and product usage instructions.
- To ensure that the device and peripheral equipment function safely and correctly, use the cables and connectors specified for the attached peripheral equipment, and make certain they are in good condition.

You can remove and replace many device components without powering off or disconnecting power to the device, as detailed elsewhere in the hardware documentation for this device. Never install equipment that appears to be damaged.

Prevention of Electrostatic Discharge Damage

Device components that are shipped in antistatic bags are sensitive to damage from static electricity. Some components can be impaired by voltages as low as 30 V. You can easily generate potentially damaging static voltages whenever you handle plastic or foam packing material or if you move components across plastic or carpets. Observe the following guidelines to minimize the potential for electrostatic discharge (ESD) damage, which can cause intermittent or complete component failures:

- Always use an ESD wrist strap when you are handling components that are subject to ESD damage, and make sure that it is in direct contact with your skin.

  If a grounding strap is not available, hold the component in its antistatic bag (see Figure 189 on page 506) in one hand and touch the exposed, bare metal of the device with the other hand immediately before inserting the component into the device.

  > **WARNING**: For safety, periodically check the resistance value of the ESD grounding strap. The measurement must be in the range 1 through 10 Mohms.
  >
  > **Avertissement** Par mesure de sécurité, vérifiez régulièrement la résistance du bracelet antistatique. Cette valeur doit être comprise entre 1 et 10 mégohms (Mohms).

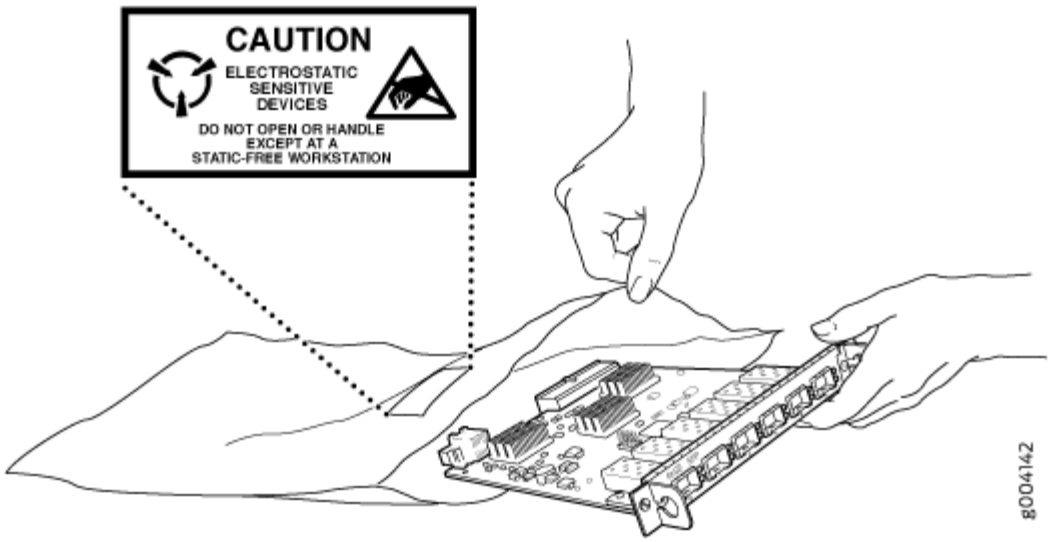
- When handling any component that is subject to ESD damage and that is removed from the device, make sure the equipment end of your ESD wrist strap is attached to the ESD point on the chassis.

  If no grounding strap is available, touch the exposed, bare metal of the device to ground yourself before handling the component.

- Avoid contact between the component that is subject to ESD damage and your clothing. ESD voltages emitted from clothing can damage components.

- When removing or installing a component that is subject to ESD damage, always place it component-side up on an antistatic surface, in an antistatic card rack, or in an antistatic bag (see Figure 189 on page 506). If you are returning a component, place it in an antistatic bag before packing it.

Figure 189: Placing a Component into an Antistatic Bag



CAUTION: ANSI/TIA/EIA-568 cables such as Category 5e and Category 6 can get electrostatically charged. To dissipate this charge, always ground the cables to a suitable and safe earth ground before connecting them to the system.

Attention Les câbles ANSI/TIA/EIA-568, par exemple Cat 5e et Cat 6, peuvent emmagasiner des charges électrostatiques. Pour évacuer ces charges, reliez toujours les câbles à une prise de terre adaptée avant de les raccorder au système.

AC Power Electrical Safety Guidelines

The following electrical safety guidelines apply to AC-powered devices:

- Note the following warnings printed on the device:

  "**CAUTION:** THIS UNIT HAS MORE THAN ONE POWER SUPPLY CORD. DISCONNECT ALL POWER SUPPLY CORDS BEFORE SERVICING TO AVOID ELECTRIC SHOCK."

"**ATTENTION:** CET APPAREIL COMPORTE PLUS D'UN CORDON D'ALIMENTATION. AFIN DE PRÉVENIR LES CHOCS ÉLECTRIQUES, DÉBRANCHER TOUT CORDON D'ALIMENTATION AVANT DE FAIRE LE DÉPANNAGE."

- AC-powered devices are shipped with a three-wire electrical cord with a grounding-type plug that fits only a grounding-type power outlet. Do not circumvent this safety feature. Equipment grounding must comply with local and national electrical codes.
- You must provide an external certified circuit breaker (2-pole circuit breaker or 4-pole circuit breaker based on your device) rated minimum 20 A in the building installation.
- The power cord serves as the main disconnecting device for the AC-powered device. The socket outlet must be near the AC-powered device and be easily accessible.
- For devices that have more than one power supply connection, you must ensure that all power connections are fully disconnected so that power to the device is completely removed to prevent electric shock. To disconnect power, unplug all power cords (one for each power supply).

Power Cable Warning (Japanese)

WARNING: The attached power cable is only for this product. Do not use the cable for another product.

注意

附属の電源コードセットはこの製品専用です。
他の電気機器には使用しないでください。

AC Power Disconnection Warning

WARNING: Before working on the device or near power supplies, unplug all the power cords from an AC-powered device.

Waarschuwing Voordat u aan een frame of in de nabijheid van voedingen werkt, dient u bij wisselstroom toestellen de stekker van het netsnoer uit het stopcontact te halen.

Varoitus Kytke irti vaihtovirtalaitteiden virtajohto, ennen kuin teet mitään asennuspohjalle tai työskentelet virtalähteiden läheisyydessä.

Avertissement Avant de travailler sur un châssis ou à proximité d'une alimentation électrique, débrancher le cordon d'alimentation des unités en courant alternatif.

Warnung Bevor Sie an einem Chassis oder in der Nähe von Netzgeräten arbeiten, ziehen Sie bei Wechselstromeinheiten das Netzkabel ab bzw.

Avvertenza Prima di lavorare su un telaio o intorno ad alimentatori, scollegare il cavo di alimentazione sulle unità CA.

Advarsel Før det utføres arbeid på kabinettet eller det arbeides i nærheten av strømforsyningsenheter, skal strømledningen trekkes ut på vekselstrømsenheter.

Aviso Antes de trabalhar num chassis, ou antes de trabalhar perto de unidades de fornecimento de energia, desligue o cabo de alimentação nas unidades de corrente alternada.

¡Atención! Antes de manipular el chasis de un equipo o trabajar cerca de una fuente de alimentación, desenchufar el cable de alimentación en los equipos de corriente alterna (CA).

Varning! Innan du arbetar med ett chassi eller nära strömförsörjningsenheter skall du för växelströmsenheter dra ur nätsladden.

DC Power Electrical Safety Guidelines

IN THIS SECTION

DC Power Electrical Safety Guidelines

The following electrical safety guidelines apply to a DC-powered firewall:

- A DC-powered firewall is equipped with a DC terminal block that is rated for the power requirements of a maximally configured firewall. To supply sufficient power, terminate the DC input wiring on a facility DC source capable of supplying at least 15 A @ -48 VDC for the system. We recommend that the 48 VDC facility DC source be equipped with a circuit breaker rated at 15 A (-48 VDC) minimum, or as required by local code. Incorporate an easily accessible disconnect device into the facility wiring. In the United States and Canada, the -48 VDC facility should be equipped with a circuit breaker rated a minimum of 125% of the power provisioned for the input in accordance with the National Electrical Code in the US and the Canadian Electrical Code in Canada. Be sure to connect the ground wire or conduit to a solid office (earth) ground. A closed loop ring is recommended for terminating the ground conductor at the ground stud.
- Run two wires from the circuit breaker box to a source of 48 VDC. Use appropriate gauge wire to handle up to 15 A.
- A DC-powered firewall that is equipped with a DC terminal block is intended only for installation in a restricted access location. In the United States, a restricted access area is one in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code ANSI/NFPA 70.

  NOTE: Primary overcurrent protection is provided by the building circuit breaker. This breaker should protect against excess currents, short circuits, and earth faults in accordance with NEC ANSI/NFPA70.

- Ensure that the polarity of the DC input wiring is correct. Under certain conditions, connections with reversed polarity might trip the primary circuit breaker or damage the equipment.
- For personal safety, connect the green and yellow wire to safety (earth) ground at both the firewall and the supply side of the DC wiring.
- The marked input voltage of -48 VDC for a DC-powered firewall is the nominal voltage associated with the battery circuit, and any higher voltages are only to be associated with float voltages for the charging function.
- Because the firewall is a positive ground system, you must connect the positive lead to the terminal labeled **RETURN**, the negative lead to the terminal labeled **-48V**, and the earth ground to the chassis grounding points.

DC Power Disconnection Warning

WARNING: Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the **OFF** position, and tape the switch handle of the circuit breaker in the **OFF** position.

Waarschuwing Voordat u een van de onderstaande procedures uitvoert, dient u te controleren of de stroom naar het gelijkstroom circuit uitgeschakeld is. Om u ervan te verzekeren dat alle stroom UIT is geschakeld, kiest u op het schakelbord de stroomverbreker die het gelijkstroom circuit bedient, draait de stroomverbreker naar de UIT positie en plakt de schakelaarhendel van de stroomverbreker met plakband in de UIT positie vast.

Varoitus Varmista, että tasavirtapiirissä ei ole virtaa ennen seuraavien toimenpiteiden suorittamista. Varmistaaksesi, että virta on KATKAISTU täysin, paikanna tasavirrasta huolehtivassa kojetaulussa sijaitseva suojakytkin, käännä suojakytkin KATKAISTU-asentoon ja teippaa suojakytkimen varsi niin, että se pysyy KATKAISTU-asennossa.

Attention Avant de pratiquer l'une quelconque des procédures ci-dessous, vérifier que le circuit en courant continu n'est plus sous tension. Pour en être sûr, localiser le disjoncteur situé sur le panneau de service du circuit en courant continu, placer le disjoncteur en position fermée (OFF) et, à l'aide d'un ruban adhésif, bloquer la poignée du disjoncteur en position OFF.

Warnung Vor Ausführung der folgenden Vorgänge ist sicherzustellen, daß die Gleichstromschaltung keinen Strom erhält. Um sicherzustellen, daß sämtlicher Strom abgestellt ist, machen Sie auf der Schalttafel den Unterbrecher für die Gleichstromschaltung ausfindig, stellen Sie den Unterbrecher auf AUS, und kleben Sie den Schaltergriff des Unterbrechers mit Klebeband in der AUS-Stellung fest.

Avvertenza Prima di svolgere una qualsiasi delle procedure seguenti, verificare che il circuito CC non sia alimentato. Per verificare che tutta l'alimentazione sia scollegata (OFF), individuare l'interruttore automatico sul quadro strumenti che alimenta il circuito CC, mettere l'interruttore in posizione OFF e fissarlo con nastro adesivo in tale posizione.

Advarsel Før noen av disse prosedyrene utføres, kontroller at strømmen er frakoblet likestrømkretsen. Sørg for at all strøm er slått AV. Dette gjøres ved å lokalisere strømbryteren på brytertavlen som betjener likestrømkretsen, slå strømbryteren AV og teipe bryterhåndtaket på strømbryteren i AV-stilling.

Aviso Antes de executar um dos seguintes procedimentos, certifique-se que desligou a fonte de alimentação de energia do circuito de corrente contínua. Para se assegurar que toda a corrente foi DESLIGADA, localize o disjuntor no painel que serve o circuito de corrente contínua e coloque-o na posição OFF (Desligado), segurando nessa posição a manivela do interruptor do disjuntor com fita isoladora.

¡Atención! Antes de proceder con los siguientes pasos, comprobar que la alimentación del circuito de corriente continua (CC) esté cortada (OFF). Para asegurarse de que toda la alimentación esté cortada (OFF), localizar el interruptor automático en el panel que alimenta al circuito de corriente continua, cambiar el interruptor automático a la posición de Apagado (OFF), y sujetar con cinta la palanca del interruptor automático en posición de Apagado (OFF).

Varning! Innan du utför någon av följande procedurer måste du kontrollera att strömförsörjningen till likströmskretsen är bruten. Kontrollera att all strömförsörjning är BRUTEN genom att slå AV det överspänningsskydd som skyddar likströmskretsen och tejpa fast överspänningsskyddets omkopplare i FRÅN-läget.

DC Power Grounding Requirements and Warning

An insulated grounding conductor that is identical in size to the grounded and ungrounded branch circuit supply conductors, but is identifiable by green and yellow stripes, is installed as part of the branch circuit that supplies the unit. The grounding conductor is a separately derived system at the supply transformer or motor generator set.

WARNING: When installing the firewall, the ground connection must always be made first and disconnected last.

Waarschuwing Bij de installatie van het toestel moet de aardverbinding altijd het eerste worden gemaakt en het laatste worden losgemaakt.

Varoitus Laitetta asennettaessa on maahan yhdistäminen aina tehtävä ensiksi ja maadoituksen irti kytkeminen viimeiseksi.

Attention Lors de l'installation de l'appareil, la mise à la terre doit toujours être connectée en premier et déconnectée en dernier.

Warnung Der Erdanschluß muß bei der Installation der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.

Avvertenza In fase di installazione dell'unità, eseguire sempre per primo il collegamento a massa e disconnetterlo per ultimo.

Advarsel Når enheten installeres, må jordledningen alltid tilkobles først og frakobles sist.

Aviso Ao instalar a unidade, a ligação à terra deverá ser sempre a primeira a ser ligada, e a última a ser desligada.

¡Atención! Al instalar el equipo, conectar la tierra la primera y desconectarla la última.

Varning! Vid installation av enheten måste jordledningen alltid anslutas först och kopplas bort sist.

DC Power Wiring Sequence Warning

WARNING: Wire the DC power supply using the appropriate lugs. When connecting power, the proper wiring sequence is ground to ground, +RTN to +RTN, then -48 V to -48 V. When disconnecting power, the proper wiring sequence is -48 V to -48 V, +RTN to +RTN, then ground to ground. Note that the ground wire should always be connected first and disconnected last.

Waarschuwing De juiste bedradingsvolgorde verbonden is aarde naar aarde, +RTN naar +RTN, en -48 V naar – 48 V. De juiste bedradingsvolgorde losgemaakt is en -48 V naar – 48 V, +RTN naar +RTN, aarde naar aarde.

Varoitus Oikea yhdistettava kytkentajarjestys on maajohto maajohtoon, +RTN varten +RTN, -48 V varten – 48 V. Oikea irrotettava kytkentajarjestys on -48 V varten – 48 V, +RTN varten +RTN, maajohto maajohtoon.

Attention Câblez l'approvisionnement d'alimentation CC En utilisant les crochets appropriés à l'extrémité de câblage. En reliant la puissance, l'ordre approprié de câblage est rectifié pour rectifier, +RTN à +RTN, puis -48 V à -48 V. En débranchant la puissance, l'ordre approprié de câblage est -48 V à -48 V, +RTN à +RTN, a alors rectifié pour rectifier. Notez que le fil de masse devrait toujours être relié d'abord et débranché pour la dernière fois. Notez que le fil de masse devrait toujours être relié d'abord et débranché pour la dernière fois.

Warnung Die Stromzufuhr ist nur mit geeigneten Ringösen an das DC Netzteil anzuschliessen. Die richtige Anschlusssequenz ist: Erdanschluss zu Erdanschluss, +RTN zu +RTN und dann -48V zu -48V. Die richtige Sequenz zum Abtrennen der

Stromversorgung ist -48V zu -48V, +RTN zu +RTN und dann Erdanschluss zu Erdanschluss. Es ist zu beachten dass der Erdanschluss immer zuerst angeschlossen und als letztes abgetrennt wird.

Avvertenza Mostra la morsettiera dell alimentatore CC. Cablare l'alimentatore CC usando i connettori adatti all'estremità del cablaggio, come illustrato. La corretta sequenza di cablaggio è da massa a massa, da positivo a positivo (da linea ad L) e da negativo a negativo (da neutro a N). Tenere presente che il filo di massa deve sempre venire collegato per primo e scollegato per ultimo.

Advarsel Riktig tilkoples tilkoplingssekvens er jord til jord, +RTN til +RTN, -48 V til – 48 V. Riktig frakoples tilkoplingssekvens er -48 V til – 48 V, +RTN til +RTN, jord til jord.

Aviso Ate con alambre la fuente de potencia cc Usando los terminales apropiados en el extremo del cableado. Al conectar potencia, la secuencia apropiada del cableado se muele para moler, +RTN a +RTN, entonces -48 V a -48 V. Al desconectar potencia, la secuencia apropiada del cableado es -48 V a -48 V, +RTN a +RTN, entonces molió para moler. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último.

¡Atención! Wire a fonte de alimentação de DC Usando os talões apropriados na extremidade da fiação. Ao conectar a potência, a seqüência apropriada da fiação é moída para moer, +RTN a +RTN, então -48 V a -48 V. Ao desconectar a potência, a seqüência apropriada da fiação é -48 V a -48 V, +RTN a +RTN, moeu então para moer. Anote que o fio à terra deve sempre ser conectado primeiramente e desconectado por último. Anote que o fio à terra deve sempre ser conectado primeiramente e desconectado por último.

Varning! Korrekt kopplingssekvens ar jord till jord, +RTN till +RTN, -48 V till – 48 V. Korrekt kopplas kopplingssekvens ar -48 V till -48 V, +RTN till +RTN, jord till jord.

DC Power Wiring Terminations Warning

WARNING: When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and conductor.

Waarschuwing Wanneer geslagen bedrading vereist is, dient u bedrading te gebruiken die voorzien is van goedgekeurde aansluitingspunten, zoals het gesloten-lus type of het

grijperschop type waarbij de aansluitpunten omhoog wijzen. Deze aansluitpunten dienen de juiste maat voor de draden te hebben en dienen zowel de isolatie als de geleider vast te klemmen.

Varoitus Jos säikeellinen johdin on tarpeen, käytä hyväksyttyä johdinliitäntää, esimerkiksi suljettua silmukkaa tai kourumaista liitäntää, jossa on ylöspäin käännetyt kiinnityskorvat. Tällaisten liitäntöjen tulee olla kooltaan johtimiin sopivia ja niiden tulee puristaa yhteen sekä eristeen että johdinosan.

Attention Quand des fils torsadés sont nécessaires, utiliser des douilles terminales homologuées telles que celles à circuit fermé ou du type à plage ouverte avec cosses rebroussées. Ces douilles terminales doivent être de la taille qui convient aux fils et doivent être refermées sur la gaine isolante et sur le conducteur.

Warnung Wenn Litzenverdrahtung erforderlich ist, sind zugelassene Verdrahtungsanschlüsse, z.B. Ringoesen oder gabelförmige Kabelschuhe mit nach oben gerichteten Enden zu verwenden. Diese Abschlüsse sollten die angemessene Größe für die Drähte haben und sowohl die Isolierung als auch den Leiter festklemmen.

Avvertenza Quando occorre usare trecce, usare connettori omologati, come quelli a occhiello o a forcella con linguette rivolte verso l'alto. I connettori devono avere la misura adatta per il cablaggio e devono serrare sia l'isolante che il conduttore.

Advarsel Hvis det er nødvendig med flertrådede ledninger, brukes godkjente ledningsavslutninger, som for eksempel lukket sløyfe eller spadetype med oppoverbøyde kabelsko. Disse avslutningene skal ha riktig størrelse i forhold til ledningene, og skal klemme sammen både isolasjonen og lederen.

Aviso Quando forem requeridas montagens de instalação eléctrica de cabo torcido, use terminações de cabo aprovadas, tais como, terminações de cabo em circuito fechado e planas com terminais de orelha voltados para cima. Estas terminações de cabo deverão ser do tamanho apropriado para os respectivos cabos, e deverão prender simultaneamente o isolamento e o fio condutor.

¡Atención! Cuando se necesite hilo trenzado, utilizar terminales para cables homologados, tales como las de tipo "bucle cerrado" o "espada", con las lengüetas de conexión vueltas hacia arriba. Estos terminales deberán ser del tamaño apropiado para los cables que se utilicen, y tendrán que sujetar tanto el aislante como el conductor.

Varning! När flertrådiga ledningar krävs måste godkända ledningskontakter användas, t.ex. kabelsko av sluten eller öppen typ med uppåtvänd tapp. Storleken på dessa kontakter måste vara avpassad till ledningarna och måste kunna hålla både isoleringen och ledaren fastklämda.

RELATED DOCUMENTATION

- *Action to Take After an Electrical Accident*
- *General Electrical Safety Guidelines and Warnings*
- *AC Power Electrical Safety Guidelines*

DC Power Disconnection Warning

WARNING: Before performing any of the DC power procedures, ensure that power is removed from the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the device handle of the circuit breaker in the OFF position.

Waarschuwing Voordat u een van de onderstaande procedures uitvoert, dient u te controleren of de stroom naar het gelijkstroom circuit uitgeschakeld is. Om u ervan te verzekeren dat alle stroom UIT is geschakeld, kiest u op het schakelbord de stroomverbreker die het gelijkstroom circuit bedient, draait de stroomverbreker naar de UIT positie en plakt de schakelaarhendel van de stroomverbreker met plakband in de UIT positie vast.

Varoitus Varmista, että tasavirtapiirissä ei ole virtaa ennen seuraavien toimenpiteiden suorittamista. Varmistaaksesi, että virta on KATKAISTU täysin, paikanna tasavirrasta huolehtivassa kojetaulussa sijaitseva suojakytkin, käännä suojakytkin KATKAISTU-asentoon ja teippaa suojakytkimen varsi niin, että se pysyy KATKAISTU-asennossa.

Avertissement Avant de pratiquer l'une quelconque des procédures ci-dessous, vérifier que le circuit en courant continu n'est plus sous tension. Pour en être sûr, localiser le disjoncteur situé sur le panneau de service du circuit en courant continu, placer le disjoncteur en position fermée (OFF) et, à l'aide d'un ruban adhésif, bloquer la poignée du disjoncteur en position OFF.

Warnung Vor Ausführung der folgenden Vorgänge ist sicherzustellen, daß die Gleichstromschaltung keinen Strom erhält. Um sicherzustellen, daß sämtlicher Strom abgestellt ist, machen Sie auf der Schalttafel den Unterbrecher für die Gleichstromschaltung ausfindig, stellen Sie den Unterbrecher auf AUS, und kleben Sie den Schaltergriff des Unterbrechers mit Klebeband in der AUS-Stellung fest.

Avvertenza Prima di svolgere una qualsiasi delle procedure seguenti, verificare che il circuito CC non sia alimentato. Per verificare che tutta l'alimentazione sia scollegata

(OFF), individuare l'interruttore automatico sul quadro strumenti che alimenta il circuito CC, mettere l'interruttore in posizione OFF e fissarlo con nastro adesivo in tale posizione.

Advarsel Før noen av disse prosedyrene utføres, kontroller at strømmen er frakoblet likestrømkretsen. Sørg for at all strøm er slått AV. Dette gjøres ved å lokalisere strømbryteren på brytertavlen som betjener likestrømkretsen, slå strømbryteren AV og teipe bryterhåndtaket på strømbryteren i AV-stilling.

Aviso Antes de executar um dos seguintes procedimentos, certifique-se que desligou a fonte de alimentação de energia do circuito de corrente contínua. Para se assegurar que toda a corrente foi DESLIGADA, localize o disjuntor no painel que serve o circuito de corrente contínua e coloque-o na posição OFF (Desligado), segurando nessa posição a manivela do interruptor do disjuntor com fita isoladora.

¡Atención! Antes de proceder con los siguientes pasos, comprobar que la alimentación del circuito de corriente continua (CC) esté cortada (OFF). Para asegurarse de que toda la alimentación esté cortada (OFF), localizar el interruptor automático en el panel que alimenta al circuito de corriente continua, cambiar el interruptor automático a la posición de Apagado (OFF), y sujetar con cinta la palanca del interruptor automático en posición de Apagado (OFF).

Varning! Innan du utför någon av följande procedurer måste du kontrollera att strömförsörjningen till likströmskretsen är bruten. Kontrollera att all strömförsörjning är BRUTEN genom att slå AV det överspänningsskydd som skyddar likströmskretsen och tejpa fast överspänningsskyddets omkopplare i FRÅN-läget.

DC Power Grounding Requirements and Warning

An insulated grounding conductor that is identical in size to the grounded and ungrounded branch circuit supply conductors but is identifiable by green and yellow stripes is installed as part of the branch circuit that supplies the device. The grounding conductor is a separately derived system at the supply transformer or motor generator set.

WARNING: When you install the device, the ground connection must always be made first and disconnected last.

Waarschuwing Bij de installatie van het toestel moet de aardverbinding altijd het eerste worden gemaakt en het laatste worden losgemaakt.

Varoitus Laitetta asennettaessa on maahan yhdistäminen aina tehtävä ensiksi ja maadoituksen irti kytkeminen viimeiseksi.

Avertissement Lors de l'installation de l'appareil, la mise à la terre doit toujours être connectée en premier et déconnectée en dernier.

Warnung Der Erdanschluß muß bei der Installation der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.

Avvertenza In fase di installazione dell'unità, eseguire sempre per primo il collegamento a massa e disconnetterlo per ultimo.

Advarsel Når enheten installeres, må jordledningen alltid tilkobles først og frakobles sist.

Aviso Ao instalar a unidade, a ligação à terra deverá ser sempre a primeira a ser ligada, e a última a ser desligada.

¡Atención! Al instalar el equipo, conectar la tierra la primera y desconectarla la última.

Varning! Vid installation av enheten måste jordledningen alltid anslutas först och kopplas bort sist.

DC Power Wiring Sequence Warning

WARNING: Wire the DC power supply using the appropriate lugs. When connecting power, the proper wiring sequence is ground to ground, +RTN to +RTN, then –48 V to –48 V. When disconnecting power, the proper wiring sequence is –48 V to –48 V, +RTN to +RTN, then ground to ground. Note that the ground wire must always be connected first and disconnected last.

Waarschuwing De juiste bedradingsvolgorde verbonden is aarde naar aarde, +RTN naar +RTN, en –48 V naar – 48 V. De juiste bedradingsvolgorde losgemaakt is en –48 naar – 48 V, +RTN naar +RTN, aarde naar aarde.

Varoitus Oikea yhdistettava kytkentajarjestys on maajohto maajohtoon, +RTN varten +RTN, –48 V varten – 48 V. Oikea irrotettava kytkentajarjestys on –48 V varten – 48 V, +RTN varten +RTN, maajohto maajohtoon.

Avertissement Câblez l'approvisionnement d'alimentation CC En utilisant les crochets appropriés à l'extrémité de câblage. En reliant la puissance, l'ordre approprié de câblage

est rectifié pour rectifier, +RTN à +RTN, puis –48 V à –48 V. En débranchant la puissance, l'ordre approprié de câblage est –48 V à –48 V, +RTN à +RTN, a alors rectifié pour rectifier. Notez que le fil de masse devrait toujours être relié d'abord et débranché pour la dernière fois. Notez que le fil de masse devrait toujours être relié d'abord et débranché pour la dernière fois.

Warnung Die Stromzufuhr ist nur mit geeigneten Ringösen an das DC Netzteil anzuschliessen. Die richtige Anschlusssequenz ist: Erdanschluss zu Erdanschluss, +RTN zu +RTN und dann -48V zu -48V. Die richtige Sequenz zum Abtrennen der Stromversorgung ist -48V zu -48V, +RTN zu +RTN und dann Erdanschluss zu Erdanschluss. Es ist zu beachten dass der Erdanschluss immer zuerst angeschlossen und als letztes abgetrennt wird.

Avvertenza Mostra la morsettiera dell alimentatore CC. Cablare l'alimentatore CC usando i connettori adatti all'estremità del cablaggio, come illustrato. La corretta sequenza di cablaggio è da massa a massa, da positivo a positivo (da linea ad L) e da negativo a negativo (da neutro a N). Tenere presente che il filo di massa deve sempre venire collegato per primo e scollegato per ultimo.

Advarsel Riktig tilkoples tilkoplingssekvens er jord til jord, +RTN til +RTN, –48 V til –48 V. Riktig frakoples tilkoplingssekvens er –48 V til – 48 V, +RTN til +RTN, jord til jord.

Aviso Ate con alambre la fuente de potencia cc Usando los terminales apropiados en el extremo del cableado. Al conectar potencia, la secuencia apropiada del cableado se muele para moler, +RTN a +RTN, entonces –48 V a –48 V. Al desconectar potencia, la secuencia apropiada del cableado es –48 V a –48 V, +RTN a +RTN, entonces molió para moler. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último.

¡Atención! Wire a fonte de alimentação de DC Usando os talões apropriados nan EXtremidade da fiação. Ao conectar a potência, a seqüência apropriada da fiação é moída para moer, +RTN a +RTN, então –48 V a –48 V. Ao desconectar a potência, a seqüência apropriada da fiação é –48 V a –48 V, +RTN a +RTN, moeu então para moer. Anote que o fio à terra deve sempre ser conectado primeiramente e desconectado por último. Anote que o fio à terra deve sempre ser conectado primeiramente e desconectado por último.

Varning! Korrekt kopplingssekvens ar jord till jord, +RTN till +RTN, –48 V till –48 V. Korrekt kopplas kopplingssekvens ar –48 V till –48 V, +RTN till +RTN, jord till jord.

DC Power Wiring Terminations Warning

WARNING: When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations must be the appropriate size for the wires and must clamp both the insulation and conductor.

Waarschuwing Wanneer geslagen bedrading vereist is, dient u bedrading te gebruiken die voorzien is van goedgekeurde aansluitingspunten, zoals het gesloten-lus type of het grijperschop type waarbij de aansluitpunten omhoog wijzen. Deze aansluitpunten dienen de juiste maat voor de draden te hebben en dienen zowel de isolatie als de geleider vast te klemmen.

Varoitus Jos säikeellinen johdin on tarpeen, käytä hyväksyttyä johdinliitäntää, esimerkiksi suljettua silmukkaa tai kourumaista liitäntää, jossa on ylöspäin käännetyt kiinnityskorvat. Tällaisten liitäntöjen tulee olla kooltaan johtimiin sopivia ja niiden tulee puristaa yhteen sekä eristeen että johdinosan.

Avertissement Quand des fils torsadés sont nécessaires, utiliser des douilles terminales homologuées telles que celles à circuit fermé ou du type à plage ouverte avec cosses rebroussées. Ces douilles terminales doivent être de la taille qui convient aux fils et doivent être refermées sur la gaine isolante et sur le conducteur.

Warnung Wenn Litzenverdrahtung erforderlich ist, sind zugelassene Verdrahtungsabschlüsse, z.B. für einen geschlossenen Regelkreis oder gabelförmig, mit nach oben gerichteten Kabelschuhen zu verwenden. Diese Abschlüsse sollten die angemessene Größe für die Drähte haben und sowohl die Isolierung als auch den Leiter festklemmen.

Avvertenza Quando occorre usare trecce, usare connettori omologati, come quelli a occhiello o a forcella con linguette rivolte verso l'alto. I connettori devono avere la misura adatta per il cablaggio e devono serrare sia l'isolante che il conduttore.

Advarsel Hvis det er nødvendig med flertrådede ledninger, brukes godkjente ledningsavslutninger, som for eksempel lukket sløyfe eller spadetype med oppoverbøyde kabelsko. Disse avslutningene skal ha riktig størrelse i forhold til ledningene, og skal klemme sammen både isolasjonen og lederen.

Aviso Quando forem requeridas montagens de instalação eléctrica de cabo torcido, use terminações de cabo aprovadas, tais como, terminações de cabo em circuito fechado e planas com terminais de orelha voltados para cima. Estas terminações de cabo deverão ser do tamanho apropriado para os respectivos cabos, e deverão prender simultaneamente o isolamento e o fio condutor.

¡Atención! Cuando se necesite hilo trenzado, utilizar terminales para cables homologados, tales como las de tipo "bucle cerrado" o "espada", con las lengüetas de conexión vueltas hacia arriba. Estos terminales deberán ser del tamaño apropiado para los cables que se utilicen, y tendrán que sujetar tanto el aislante como el conductor.

Varning! När flertrådiga ledningar krävs måste godkända ledningskontakter användas, t.ex. kabelsko av sluten eller öppen typ med uppåtvänd tapp. Storleken på dessa kontakter måste vara avpassad till ledningarna och måste kunna hålla både isoleringen och ledaren fastklämda.

Multiple Power Supplies Disconnection Warning

WARNING: The network device has more than one power supply connection. All connections must be removed completely to remove power from the unit completely.

Waarschuwing Deze eenheid heeft meer dan één stroomtoevoerverbinding; alle verbindingen moeten volledig worden verwijderd om de stroom van deze eenheid volledig te verwijderen.

Varoitus Tässä laitteessa on useampia virtalähdekytkentöjä. Kaikki kytkennät on irrotettava kokonaan, jotta virta poistettaisiin täysin laitteesta.

Avertissement Cette unité est équipée de plusieurs raccordements d'alimentation. Pour supprimer tout courant électrique de l'unité, tous les cordons d'alimentation doivent être débranchés.

Warnung Diese Einheit verfügt über mehr als einen Stromanschluß; um Strom gänzlich von der Einheit fernzuhalten, müssen alle Stromzufuhren abgetrennt sein.

Avvertenza Questa unità ha più di una connessione per alimentatore elettrico; tutte le connessioni devono essere completamente rimosse per togliere l'elettricità dall'unità.

Advarsel Denne enheten har mer enn én strømtilkobling. Alle tilkoblinger må kobles helt fra for å eliminere strøm fra enheten.

Aviso Este dispositivo possui mais do que uma conexão de fonte de alimentação de energia; para poder remover a fonte de alimentação de energia, deverão ser desconectadas todas as conexões existentes.

¡Atención! Esta unidad tiene más de una conexión de suministros de alimentación; para eliminar la alimentación por completo, deben desconectarse completamente todas las conexiones.

Varning! Denna enhet har mer än en strömförsörjningsanslutning; alla anslutningar måste vara helt avlägsnade innan strömtillförseln till enheten är fullständigt bruten.

TN Power Warning

WARNING: The device is designed to work with a TN power system.
Waarschuwing Het apparaat is ontworpen om te functioneren met TN energiesystemen.

Varoitus Koje on suunniteltu toimimaan TN-sähkövoimajärjestelmien yhteydessä.

Avertissement Ce dispositif a été conçu pour fonctionner avec des systèmes d'alimentation TN.

Warnung Das Gerät ist für die Verwendung mit TN-Stromsystemen ausgelegt.

Avvertenza Il dispositivo è stato progettato per l'uso con sistemi di alimentazione TN.

Advarsel Utstyret er utfomet til bruk med TN-strømsystemer.

Aviso O dispositivo foi criado para operar com sistemas de corrente TN.

¡Atención! El equipo está diseñado para trabajar con sistemas de alimentación tipo TN.

Varning! Enheten är konstruerad för användning tillsammans med elkraftssystem av TN-typ.

Action to Take After an Electrical Accident

If an electrical accident results in an injury, take the following actions in this order:

1. Use caution. Be aware of potentially hazardous conditions that could cause further injury.
2. Disconnect power from the device.

3. If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.

SRX5800 Firewall Agency Approvals

IN THIS SECTION

The firewall complies with the following standards:

- Safety
  - EN 60825-1 Safety of Laser Products - Part 1: Equipment Classification, Requirements and User's Guide
  - CSA 60950-1 Safety of Information Technology Equipment
  - UL 60950-1 Safety of Information Technology Equipment
  - EN 60950-1 Safety of Information Technology Equipment
  - IEC 60950-1 Safety of Information Technology Equipment (with country deviations)
- EMC/EMI/ETSI
  - AS/NZS CISPR22 (Australia/New Zealand)
  - FCC Part 15 Class A USA Radiated Emissions
  - EN 55022 Class A European Radiated Emissions
  - VCCI Class A Japanese Radiated Emissions
  - ETSI EN-300386 V1.3.3 Telecom Network Equipment. Electromagnetic Compatibility Requirements
- Immunity
  - EN 55024 +A1+A2 Information Technology Equipment Immunity Characteristics
  - EN-61000-3-2 Power Line Harmonics

  - EN-61000-3-3 +A1 +A2 +A3 Power Line Voltage Fluctuations and Flicker
  - EN-61000-4-2 +A1 +A2 Electrostatic Discharge
  - EN-61000-4-3 +A1+A2 Radiated Immunity
  - EN-61000-4-4 Electrical Fast Transients
  - EN-61000-4-5 Surge
  - EN-61000-4-6 Immunity to Conducted Disturbances
  - EN-61000-4-11 Voltage Dips and Sags
- NEBS
  - GR-63-CORE: NEBS, Physical Protection
  - GR-1089-CORE: EMC and Electrical Safety for Network Telecommunications Equipment
  - SR-3580: NEBS Criteria Levels (Level 3 Compliance)

Compliance Statement for Argentina

EQUIPO DE USO IDÓNEO.

RELATED DOCUMENTATION

In Case of Electrical Accident

General Electrical Safety Guidelines and Warnings

DC Power Electrical Safety Guidelines and Warnings

SRX5800 Firewall Compliance Statements for EMC Requirements

IN THIS SECTION

Canada

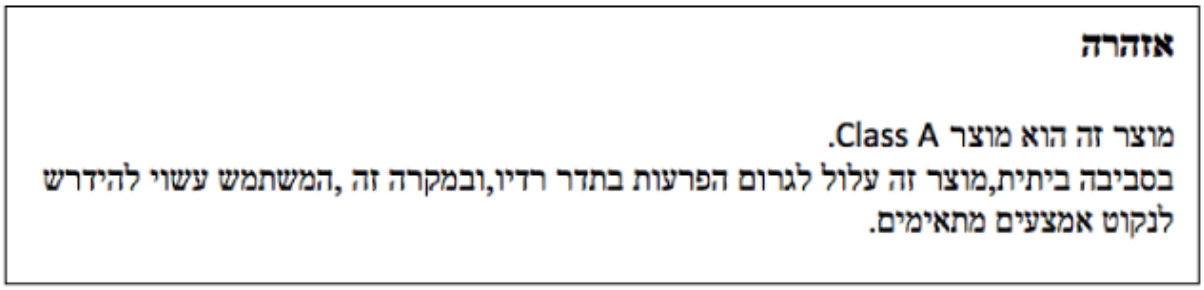
This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Community

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

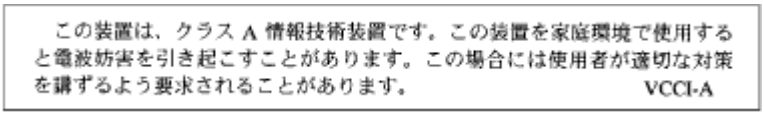
Israel



The preceding translates as follows:

This product is Class A. In residential environments, the product may cause radio interference, and in such a situation, the user may be required to take adequate measures.

Japan



The preceding translates as follows:

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

VCCI-A

United States

The firewall has been tested and found to comply with the limits for a Class A digital device of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.