JUNIPER NETWORKS | Engineering Simplicity

SRX320 Services Gateway Hardware Guide

Published
2022-01-21

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

SRX320 Services Gateway 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 SRX320 Services Gateway. 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

- SRX320 Services Gateway Quick Start
- SRX300 Series and SRX550 High Memory Gateway Interface Modules Reference
- Wi-Fi Mini-PIM Installation Guide
- LTE Mini-PIM and Antenna Installation Guide
- Transceivers Supported on SRX320 Services Gateways

1

CHAPTER

Overview

SRX320 Services Gateway Overview

IN THIS SECTION

SRX320 Services Gateway Description

The SRX320 Services Gateway consolidates security, routing, switching, and WAN interfaces for small distributed enterprises. With advanced threat mitigation capabilities, the services gateway provides cost-effective and secure connectivity across distributed enterprises.

With a desktop form-factor chassis, the SRX320 Services Gateway has six 1 G Ethernet ports, two 1 G SFP ports, 4 GB of DRAM memory, 8 GB of flash memory, and two Mini-Physical Interface Module (Mini-PIM) slots.

The SRX320 Services Gateway is available with or without Power over Ethernet (PoE) capability. In the PoE model. the six Ethernet ports are PoE capable.

The SRX320 Services Gateway runs the Junos operating system (Junos OS) and supports the following features:

- Firewall support with key features such as IPsec and VPN
- Intrusion Detection and Prevention (IDP)
- High availability
- QoS
- MPLS

You can manage the SRX320 Services Gateway by using the same interfaces that you use for managing other devices that run Junos OS—the CLI, the J-Web graphical interface, and Junos Space.

SRX320 Services Gateway Field Replaceable Units Overview

Field-replaceable units (FRUs) are components that you can replace at your site. The Mini-Physical Interface Module (MPIM) is the only FRU on the SRX320 Services Gateway.

The Mini-PIMs are not hot-swappable. You must power off the services gateway before removing or installing Mini-PIMs.

SEE ALSO

Replacing Mini-Physical Interface Modules in the SRX320 Services Gateway | 69

Benefits of the SRX320 Services Gateway

- **High performance**—The SRX320 supports up to 1-Gbps firewall and 300-Mbps IPsec VPN, and is suited for small distributed enterprise branch office deployments.
- **Simplified deployment with minimal manual intervention**—The Zero Touch Provisioning (ZTP) feature enables you to provision and configure the SRX300 line automatically, thereby reducing operational complexity and simplifying the provisioning of new sites.
- **Multiple WAN connectivity options**—The SRX320 supports multiple options such as Ethernet, serial, T1/E1, VDSL2, and 3G/4G LTE wireless for WAN or Internet connectivity to link sites.
- **Threat protection**—The SRX300 line supports IPsec VPN, Media Access Control Security (MACsec), Juniper Sky Advanced Threat Prevention, and Trusted Platform Module (TPM) to protect against potential vulnerabilities.

RELATED DOCUMENTATION

SRX320 Installation Overview | 33

SRX320 Chassis

IN THIS SECTION

SRX320 Services Gateway Chassis Overview

The SRX320 Services Gateway chassis measures 1.73 in. high, 11.81 in. wide, and 7.52 in. deep. The PoE model weighs 3.4 lb. and the non-PoE model weighs 3.28 lb.

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

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

SRX320 Services Gateway Front Panel

IN THIS SECTION

Figure 1 on page 5 shows the front panel of the SRX320 Services Gateway.

Figure 1: SRX320 Services Gateway Front Panel

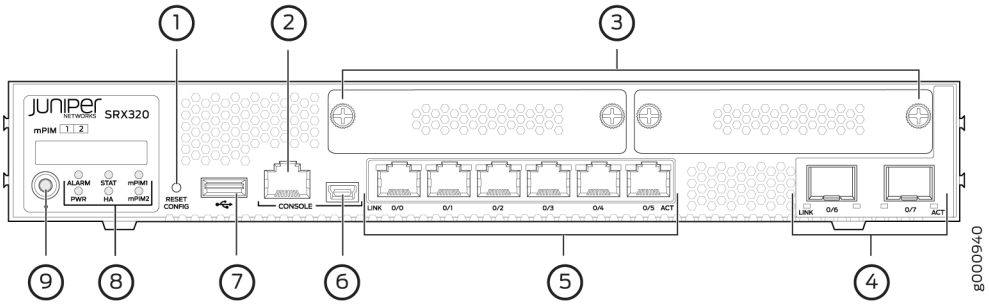


Table 1 on page 5 provides details about the front panel components.

Table 1: SRX320 Services Gateway Front Panel Components

Number	Component	Description
1	Reset Config button	Returns the services gateway to the rescue configuration or the factory-default configuration.

Table 1: SRX320 Services Gateway Front Panel Components *(Continued)*

Number	Component	Description
2,6	Console port	• Serial—Connects a laptop to the services gateway for CLI management. The port uses an RJ-45 serial connection and supports the RS-232 (EIA-232) standard. • USB—Connects a laptop to the services gateway for CLI management through a USB interface. The port accepts a Mini-B type USB cable plug. A USB cable with Mini-B and Type A USB plugs is supplied with the services gateway. To use the mini-USB console port, you must download a USB driver to the management device from the Downloads page at https://www.juniper.net/support/downloads/?p=junos-srx#sw. To download the driver for Windows OS, select 6.5 from the **Version** drop-down list. To download the driver for Mac OS, select 4.10 from the **Version** drop-down list.
3	Mini-PIM slots	Two slots for Mini-PIMs. Mini-PIMs can be used to provide LAN and WAN functionality along with connectivity to various media types.
4	1-GbE small form-factor pluggable (SFP) ports	Two 1-GbE MACsec-capable ports for network traffic.

Table 1: SRX320 Services Gateway Front Panel Components *(Continued)*

Number	Component	Description
5	1-GbE RJ-45 ports	Six LAN ports (0/0 to 0/5) The ports have the following characteristics: • Operate in full-duplex and half-duplex modes • Support autonegotiation The ports can be used to: • Function as front-end network ports • Provide LAN and WAN connectivity to hubs, switches, local servers, and workstations • Forward incoming data packets to the services gateway • Receive outgoing data packets from the services gateway
7	USB port	The services gateway has one USB port that accepts a USB storage device.
8	LEDs	Indicate component and system status at a glance.
9	Power button	Use the Power button to power on or power off the services gateway.

Figure 2 on page 8 shows the LEDs on the front panel.

Figure 2: SRX320 Services Gateway Front Panel LEDs

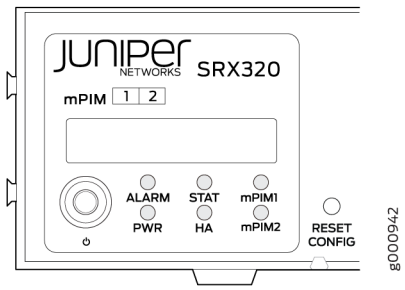


Table 2 on page 8 lists the front panel LEDs.

Table 2: SRX320 Services Gateway Front Panel LEDs

Component	Description
ALARM	• Solid amber (noncritical alarm) • Solid red (critical alarm) • Off (no alarms)
STAT	• Solid green (operating normally) • Solid red (error detected)
PWR	• Solid green (receiving power) • Solid red (power failure) • Off (no power)

Table 2: SRX320 Services Gateway Front Panel LEDs *(Continued)*

Component	Description
HA	• Solid green (all HA links are available) • Solid amber (some HA links are unavailable) • Solid red (HA links are not functional) • Off (HA is disabled)
mPIM0 and mPIM1	• Solid green (Mini-PIM is functioning normally) • Solid red (Mini-PIM hardware failure) • Off (Mini-PIM is not present or Mini-PIM is not detected by the device)

Network Port LEDs

The SFP and Ethernet ports have two status LEDs, LINK and ACT, located above the port.

Table 3: Network Port LEDs

LED	Description
LINK (LED on the left)	• Solid green—There is link activity. • Off—There is no link established.
ACT (LED on the right)	• Blinking green—There is activity on the 1 G link. • Off—There is no link activity.

SRX320 Services Gateway Back Panel

Figure 3 on page 10 shows the back panel of the SRX320 Services Gateway and Table 4 on page 10 lists the components on the back panel.

Figure 3: SRX320 Services Gateway Back Panel

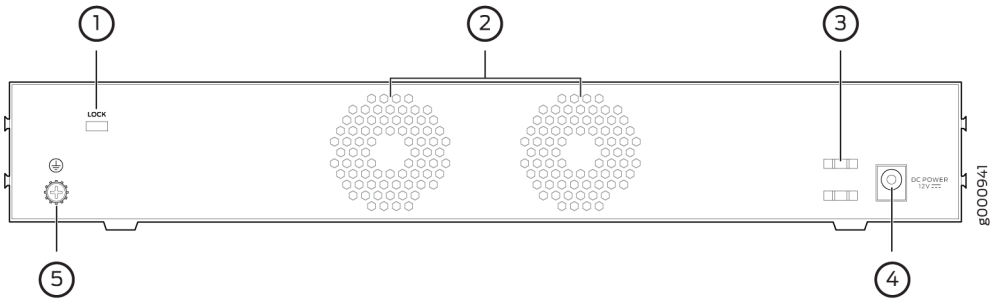


Table 4: SRX320 Services Gateway Back Panel Components

Number	Component	Description
1	Lock	Provides the capability to lock and secure the device at the installation site.
2	Fans	Keeps all the services gateway components within the acceptable temperature range.
3	Cable tie holder	Secures the DC power cord connection to the adapter.
4	Power supply input (DC power input)	Connects the services gateway to the external power supply.

Table 4: SRX320 Services Gateway Back Panel Components *(Continued)*

Number	Component	Description
5	Grounding point	Connects the services gateway chassis to earth ground (optional). **NOTE**: We recommend connecting the services gateway to ground if required.

SRX320 Services Gateway Interface Modules Overview

Mini-Physical Interface Modules (Mini-PIMs) are field-replaceable network interface cards (NICs) supported on the SRX300 line of services gateways. You can easily insert or remove Mini-PIMs from the front slots of the services gateway chassis. The Mini-PIMs provide physical connections to a LAN or a WAN. The Mini-PIMs receive incoming packets from the network and transmit outgoing packets to the network. During this process, they perform framing and line-speed signaling for the medium type.

CAUTION: The Mini-PIMs are not hot-swappable. You must power off the services gateway before removing or installing Mini-PIMs.

The following Mini-PIMs are supported on the SRX320 Services Gateway:

- 1-Port Serial Mini-Physical Interface Module (SRX-MP-1SERIAL-R)
- 1-Port T1/E1 Mini-Physical Interface Module (SRX-MP-1T1E1-R)
- 1-Port VDSL2 (Annex A) Mini-Physical Interface Module (SRX-MP-1VDSL2-R)
- LTE Mini-Physical Interface Module (SRX-MP-LTE-AE and SRX-MP-LTE-AA)
- Wi-Fi Mini-Physical Interface Module (SRX-MP-WLAN-US, SRX-MP-WLAN-IL, and SRX-MP-WLAN-WW)

For more information on the Mini-PIMs, see the SRX300 Series and SRX550 High Memory Gateway Interface Modules Reference.

RELATED DOCUMENTATION

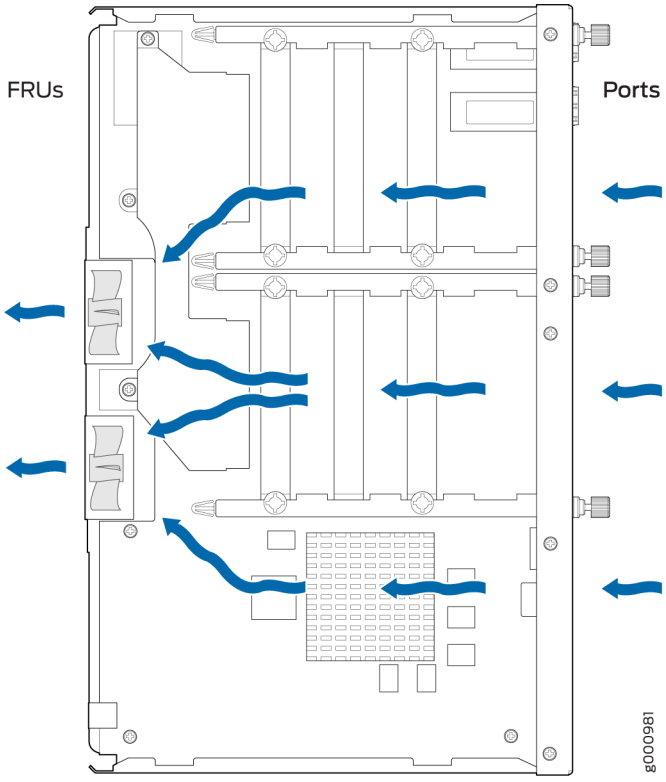
SRX320 Installation Overview | 33

SRX320 Cooling System

The cooling system for the SRX320 Services Gateway includes two fixed fans. The fans draw air through vents on the front of the chassis and exhaust the air through the back of the chassis. The airflow produced by the fans keeps device components within the acceptable temperature range.

Figure 4 on page 12 shows the airflow through the chassis.

Figure 4: Airflow Through the SRX320 Services Gateway Chassis



RELATED DOCUMENTATION

SRX320 Services Gateway Clearance Requirements for Airflow and Hardware Maintenance | 26

SRX320 Power System

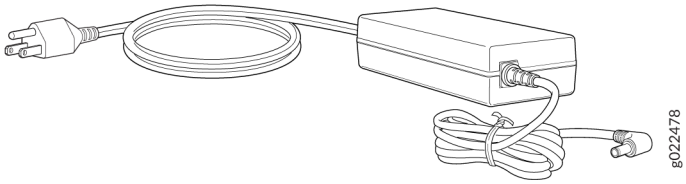
IN THIS SECTION

Understanding the SRX320 Services Gateway Power Supply

The power supply for the SRX320 Services Gateway is external. You must use the following power supply adapters provided by Juniper Networks to provide power to the services gateway.

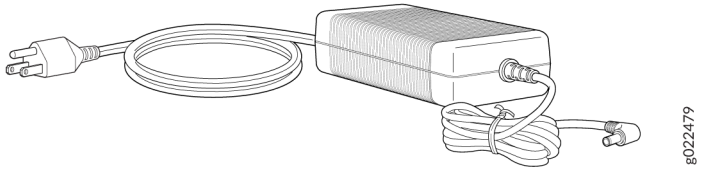
- 75 W, 12 V power supply adapter for non-PoE models

Figure 5: 75 W, 12 V Power Supply Adapter



- 280 W, 54 V power supply adapter for PoE models

Figure 6: 280 W, 54 V Power Supply Adapter



Each PoE port delivers a maximum power of 30 W. Because of line loss, the powered device connected to a PoE port can use only 25.5 W of power. Line loss is influenced by cable length, quality, and other factors and is typically less than 16 percent of the maximum power.

SRX320 Services Gateway Power Specifications and Requirements

Table 5 on page 14 lists the power specifications for the SRX320 Services Gateway power supply adapter.

Table 5: Power Specifications for the SRX320 Services Gateway Power Supply Adapter

Power Supply Adapter Requirement	Specifications	
	Non-PoE model	PoE model
AC input	100 to 240 VAC	100 to 240 VAC
AC input line frequency	50 to 60 Hz	50 to 60 Hz
AC system current rating	1.3 A maximum	3.25 A maximum
Maximum AC inrush current	11 A at 220 V/50 Hz (with two Mini-PIMs installed)	15 A at 220 V/50 Hz (with two Mini-PIMs installed)

WARNING: The AC power cord for the services gateway is intended for use with only the power supply adapter provided with the device.

SEE ALSO

SRX320 Services Gateway Electrical Wiring Guidelines | 22

Power Cord Specifications for SRX320

A detachable power cord is supplied with the device. The coupler is type C13 as described by International Electrotechnical Commission (IEC) standard 60320. The plug end of the power cord fits into the power source outlet that is standard for your geographical location.

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

Table 6 on page 15 lists the AC power cord specifications for the countries and regions listed in the table.

Table 6: AC Power Cord Specifications

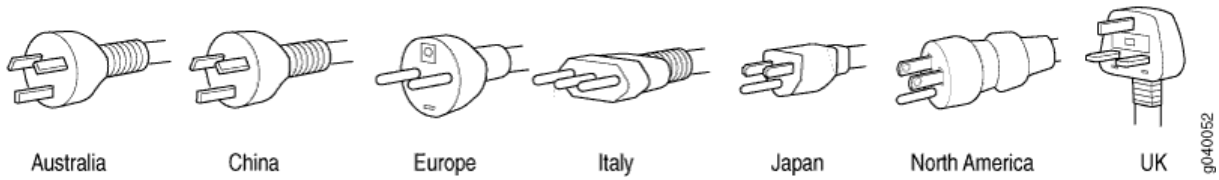
Country/Region	Electrical Specifications	Plug Standards	Juniper Model Number
Australia	250 VAC, 10 A, 50 Hz	AS/NZZS 3112 Type SAA/3	CBL-JX-PWR-AU
China	250 VAC, 10 A, 50 Hz	GB 1002-1996 Type PRC/3	CBL-JX-PWR-CH
Europe (except Italy, Switzerland, and United Kingdom)	250 VAC, 10 A, 50 Hz	CEE (7) VII Type VIIG	CBL-JX-PWR-EU
India	250 VAC, 10 A, 50 Hz	IS 1293 Type IND/3	CBL-EX-PWR-C13-IN
Italy	250 VAC, 10 A, 50 Hz	CEI 23-16 Type I/3G	CBL-JX-PWR-IT
Japan	125 VAC, 12 A, 50 Hz or 60 Hz	SS-00259 Type VCTF	CBL-JX-PWR-JP
Korea	250 VAC, 10 A, 50 Hz or 60 Hz	CEE (7) VII Type VIIGK	CBL-JX-PWR-KR

Table 6: AC Power Cord Specifications *(Continued)*

Country/Region	Electrical Specifications	Plug Standards	Juniper Model Number
Switzerland	250 VAC, 10 A, 50 Hz	SEV 6534-2 Type 12G	CBL-EX-PWR-C13-SZ
United Kingdom	250 VAC, 10 A, 50 Hz	BS 1363/A Type BS89/13	CBL-JX-PWR-UK
United States	125 VAC, 13 A, 60 Hz	NEMA 5-15 Type N5-15	CBL-JX-PWR-US

Figure 7 on page 16 illustrates the plug on the power cord for some of the countries or regions listed in Table 6 on page 15.

Figure 7: AC Plug Types



CHAPTER 2

Site Planning, Preparation, and Specifications

SRX320 Site Preparation Checklist

Table 7 on page 18 provides a checklist of tasks you need to perform when preparing a site for installing the SRX320 Services Gateway.

Table 7: Site Preparation Checklist for SRX320 Services Gateway Installation

Item or Task	Additional Information
Environment	
Verify that environmental factors such as temperature and humidity do not exceed device tolerances.	"SRX320 Services Gateway Environmental Specifications" on page 21
Power	
• Measure the distance between the external power sources and the device installation site. • Locate sites for connection of system grounding. • Calculate the power consumption and requirements.	"SRX320 Services Gateway Electrical Wiring Guidelines" on page 22 "SRX320 Services Gateway Power Specifications and Requirements" on page 14
Rack Requirements	
Verify that your rack meets the minimum requirements.	"SRX320 Site Guidelines and Requirements" on page 20
Rack Installation	

Table 7: Site Preparation Checklist for SRX320 Services Gateway Installation *(Continued)*

Item or Task	Additional Information
• Plan the rack location, including required space clearances. • Secure the rack to the floor and building structure.	"Installing the SRX320 Services Gateway in a Rack" on page 40
Cabinet Requirements	
• Verify that your cabinet meets the minimum requirements. • Plan the cabinet location, including required space clearances.	"SRX320 Site Guidelines and Requirements" on page 20
Wall Installation	
• Verify that the area selected meets the minimum requirements. • Verify that you have the required hardware to proceed with the installation.	"Installing the SRX320 Services Gateway on a Wall" on page 37
Desktop Installation	
• Verify that the area selected meets the minimum requirements. • Plan the installation location, including required space clearances and airflow requirements.	"Installing the SRX320 Services Gateway on a Desk" on page 37

Table 7: Site Preparation Checklist for SRX320 Services Gateway Installation *(Continued)*

Item or Task	Additional Information
Cables	
• Acquire cables and connectors. • Review the maximum distance allowed for each cable. Choose the length of cable based on the distance between the hardware components being connected. • Plan the cable routing and management.	

RELATED DOCUMENTATION

SRX320 Services Gateway General Site Guidelines | 21

SRX320 Site Guidelines and Requirements

IN THIS SECTION

Cabinet Requirements | 27

SRX320 Services Gateway General Site Guidelines

The following precautions help you plan an acceptable operating environment for your SRX320 Services Gateway and avoid environmentally caused equipment failures:

- For the cooling system to function properly, the airflow around the chassis must be unrestricted. Allow sufficient clearance between the front and back of the chassis and adjacent equipment. Ensure that there is adequate circulation in the installation location.
- Follow the ESD procedures to avoid damaging equipment. Static discharge can cause components to fail completely or intermittently over time. For more information, see *Prevention of Electrostatic Discharge Damage*.
- Ensure that a blank Mini-PIM panel is installed in the empty slot to prevent any interruption or reduction in the flow of air across internal components.

SRX320 Services Gateway Environmental Specifications

Table 8 on page 21 provides the required environmental conditions for normal SRX320 Services Gateway operations.

Table 8: Environmental Specifications for the SRX320 Services Gateway

Description	Value
Altitude	No performance degradation up to 10,000 ft (3048 m)
Relative humidity	5% to 95%, noncondensing

Table 8: Environmental Specifications for the SRX320 Services Gateway *(Continued)*

Description	Value
Temperature	• Operational temperature—32° F (0° C) to 104° F (40° C) • Nonoperational temperature—4° F (-20° C) to 158° F (70° C)
Average power consumption	46 W (non-PoE model) 221 W (PoE model)
Rated DC input power	12 VDC, 4.7 A maximum (non-PoE model) 54 VDC, 4.6 A maximum (PoE model)
Average heat dissipation	157 BTU/hr (non-PoE model) 755 BTU/hr (PoE model)
Noise level	37 dBA (non-PoE model) 40 dBA (PoE model)

SRX320 Services Gateway Electrical Wiring Guidelines

Table 9 on page 23 describes the factors you must consider while planning the electrical wiring for the services gateway at your site.

CAUTION: It is particularly important to provide a properly grounded and shielded environment and to use electrical surge-suppression devices.

Table 9: Site Electrical Wiring Guidelines for the SRX320 Services Gateway

Site Wiring Factor	Guideline
Signaling Limitations	To ensure that signaling functions optimally: • Install wires correctly. Improperly installed wires can emit radio interference. • Do not exceed the recommended distances or pass wires between buildings. The potential for damage from lightning strikes increases if wires exceed recommended distances or if wires pass between buildings. • Shield all conductors. The electromagnetic pulse (EMP) caused by lightning can damage unshielded conductors and destroy electronic devices.
Radio Frequency Interference (RFI)	To reduce or eliminate the emission of RFI from your site wiring: • Use twisted-pair cable with a good distribution of grounding conductors. • Use a high-quality twisted-pair cable with one ground conductor for each data signal when applicable, if you must exceed the recommended distances.
Electromagnetic Compatibility (EMC)	Provide a properly grounded and shielded environment and use electrical surge-suppression devices. Strong sources of electromagnetic interference (EMI) can cause the following damage: • Destroy the signal drivers and receivers in the device • Conduct power surges over the lines into the equipment, resulting in an electrical hazard **NOTE**: If your site is susceptible to problems with EMC, particularly from lightning or radio transmitters, you may want to seek expert advice.

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

SEE ALSO

SRX320 Services Gateway Power Specifications and Requirements | **14**

General Electrical Safety Guidelines and Warnings | **101**

SRX320 Services Gateway Grounding Specifications

To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, the SRX320 Services Gateway must be adequately grounded before power is connected. You must provide a grounding lug to connect the services gateway to earth ground.

WARNING: Before you connect power to the services gateway, 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 services gateway (for example, by causing a short circuit).

The services gateway chassis has one grounding point on the back panel.

You must install the SRX320 in a restricted-access location and ensure that the chassis is always properly grounded. The SRX320 has a single hole protective grounding terminal provided on the chassis. We recommend that you use this protective grounding terminal as the preferred method for grounding the chassis regardless of the power supply configuration. However, if additional grounding methods are available, you can also use those methods. For example, you can use the grounding wire in the AC power cord or use the grounding terminal or lug on a DC power supply. This tested system meets or exceeds all applicable EMC regulatory requirements with the single hole protective grounding terminal.

Table 10 on page 24 lists the specifications of the grounding cable used with the device.

Table 10: Grounding Cable Specifications for the Services Gateway

Grounding Requirement	Specification
Grounding cable	14 AWG single-strand wire cable

Table 10: Grounding Cable Specifications for the Services Gateway *(Continued)*

Grounding Requirement	Specification
Amperage of grounding cable	Up to 4 A
Grounding lug	Ring-type, vinyl-insulated TV14-6R lug or equivalent

SEE ALSO

Connecting the SRX320 Services Gateway Grounding Cable | 46

SRX320 Services Gateway Physical Specifications

Table 11 on page 25 lists the physical specifications for the services gateway.

Table 11: Physical Specifications for the SRX320 Services Gateway

Physical Specification of Chassis	SRX320	SRX320-PoE
Depth	7.52 in.	7.52 in.
Width	11.81 in.	11.81 in.
Height	1.73 in.	1.73 in.
Weight	3.28 lb	3.4 lb

SRX320 Services Gateway Clearance Requirements for Airflow and Hardware Maintenance

When planning the installation site for the SRX320 Services Gateway, you need to allow sufficient clearance around the device. Consider the following:

- For the operating temperature of the services gateway to be optimal, the airflow around the chassis must be unrestricted.
- For service personnel to remove and install hardware components, there must be adequate space at the front and back of the device. Allow at least 24 in. (61 cm) both in front of and behind the device.
- If you are mounting the device in a rack with other equipment, or if you are placing it on the desktop near other equipment, ensure that the exhaust from other equipment does not blow into the intake vents of the chassis.

For information on the airflow through the chassis, see "SRX320 Cooling System" on page 12.

Rack Requirements

When installing the services gateway in a rack, you must ensure that the rack complies with a 1U (19 in. or 48.7 cm) rack as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D), published by the Electronic Industries Alliance (http://www.ecaus.org/eia/site/index.html).

When selecting a rack, ensure that the physical characteristics of the rack comply with the following specifications:

- The outer edges of the mounting brackets extend the width of either chassis to 19 in. (48.3 cm).
- The front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting ears.
- Maximum permissible ambient temperature when two devices are placed side by side in a 19 in. rack is 40° C.

The spacing of the mounting brackets and flange holes on the rack and device mounting brackets are as follows:

- The holes within each rack set are spaced at 1 U (1.75 in. or 4.5 cm).
- The mounting brackets and front-mount flanges used to attach the chassis to a rack are designed to fasten to holes spaced at rack distances of 1 U (1.75 in.).
- The mounting holes in the mounting brackets provided with the device are spaced 1.25 in. (3.2 cm) apart (top and bottom mounting hole).

Always secure the rack in which you are installing the services gateway 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.

Cabinet Requirements

You can install the services gateway in a 19 in. (48.7 cm) cabinet as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D) published by the Electronic Industries Alliance (http://www.ecaus.org/eia/site/index.html). You must mount the services gateway horizontally in the cabinet using appropriate rack adapters.

When selecting a cabinet, ensure that it meets the following specifications:

- The cabinet is at least 1U (3.50 in. or 8.89 cm) and can accommodate the services gateway.
- The outer edges of the mounting brackets extend the width of either chassis to 19 in. (48.7 cm), and the front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting brackets.
- The minimum total clearance inside the cabinet is 30.7 in. (78 cm) between the inside of the front door and the inside of the rear door.

NOTE: A cabinet larger than the minimum required provides better airflow and reduces the chance of overheating.

When you mount the services gateway in a cabinet, you must ensure that ventilation through the cabinet is sufficient to prevent overheating. Consider the following when planning for chassis cooling:

- Ensure that the cool air supply you provide through the cabinet can adequately dissipate the thermal output of the services gateway.
- Install the services gateway as close as possible to the front of the cabinet so that the cable management system clears the inside of the front door. Installing the chassis close to the front of the cabinet 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.

RELATED DOCUMENTATION

SRX320 Installation Overview | 33

SRX320 Transceiver Specifications and Pinouts

IN THIS SECTION

SRX320 Transceiver Support

You can find information about the pluggable transceivers supported on your Juniper Networks device by using the Hardware Compatibility Tool. In addition to transceiver and connector type, the optical and cable characteristics—where applicable—are documented for each transceiver. The Hardware Compatibility Tool enables you to search by product, displaying all the transceivers supported on that device, or category, by interface speed or type. The list of supported transceivers for the SRX320 is located at https://apps.juniper.net/hct/product/#prd=SRX320.

RJ-45 Connector Pinouts for the SRX320 Services Gateway Ethernet Port

Table 12 on page 28 describes the RJ-45 connector pinouts for the Ethernet port.

Table 12: RJ-45 Connector Pinouts for the SRX320 Services Gateway Ethernet Port

Pin	Signal
1	BI_DA+
2	BI_DA

Table 12: RJ-45 Connector Pinouts for the SRX320 Services Gateway Ethernet Port *(Continued)*

Pin	Signal
3	BI_DB+
4	BI_DC+
5	BI_DC
6	BI_DB
7	BI_DD+
8	BI_DD

RJ-45 Connector Pinouts for the SRX320 Services Gateway Console Port

Table 13 on page 29 describes the RJ-45 connector pinouts for the console port.

Table 13: RJ-45 Connector Pinouts for the SRX320 Services Gateway Console Port

Pin	Signal	Description
1	RTS	Request to Send
2	DTR	Data Terminal Ready
3	TXD	Transmit Data
4	Ground	Signal Ground
5	Ground	Signal Ground

Table 13: RJ-45 Connector Pinouts for the SRX320 Services Gateway Console Port *(Continued)*

Pin	Signal	Description
6	RXD	Receive Data
7	DSR/DCD	Data Set Ready
8	CTS	Clear to Send

Mini-USB Connector Pinouts for the SRX320 Services Gateway Console Port

The SRX320 Services Gateway has two console ports: an RJ-45 Ethernet port and a mini-USB Type-B port. If your management device (laptop or PC) does not have a DB-9 plug connector pin or an RJ-45 connector pin, you can connect your management device to the Mini-USB Type-B console port of the services gateway by using a cable that has a standard Type-A USB connector on one end and a Mini-USB Type-B (5-pin) connector on the other end. Table 14 on page 30 describes the Mini-USB Type-B connector pinouts for the console port.

NOTE: By design, the mini-USB console port has higher priority over the RJ-45 console port. If the mini-USB and RJ-45 console ports are both connected, then the mini-USB console port will be active.

Table 14: Mini-USB Type-B Connector Pinouts for the Services Gateway Console Port

Pin	Signal	Cable Color	Description
1	VCC	Red	+5 VDC
2	D-	White	Data -
3	D+	Green	Data +

Table 14: Mini-USB Type-B Connector Pinouts for the Services Gateway Console Port *(Continued)*

Pin	Signal	Cable Color	Description
X	N/C		Could be not connected (N/C), connected to ground (GND), or used as an attached device presence indicator
4	GND	Black	Ground

CHAPTER 3

Initial Installation and Configuration

SRX320 Installation Overview

IN THIS SECTION

SRX320 Services Gateway Installation Overview

After you have prepared the site for installation and unpacked the SRX320 Services Gateway, you are ready to install the device. It is important to proceed through the installation process in the following order:

1. Review the safety guidelines explained in *General Safety Guidelines and Warnings*.
2. Prepare your site for the installation of the services gateway as described in "SRX320 Site Preparation Checklist" on page 18.
3. Install the services gateway. See:
   - "Installing the SRX320 Services Gateway in a Rack" on page 40
   - "Installing the SRX320 Services Gateway on a Desk" on page 37
   - "Installing the SRX320 Services Gateway on a Wall" on page 37
4. Connect cables to external devices.
5. Connect the grounding cable as described in "Connecting the SRX320 Services Gateway Grounding Cable" on page 46.
6. Power on the services gateway as described in "Powering On the SRX320 Services Gateway" on page 49.

SRX320 Services Gateway Autoinstallation Overview

The autoinstallation process begins any time a services gateway is powered on and cannot locate a valid configuration file in the internal flash. Typically, a configuration file is unavailable when a services gateway is powered on for the first time or if the configuration file is deleted from the internal flash. The autoinstallation feature enables you to deploy multiple services gateways from a central location in the network.

If you are setting up many devices, autoinstallation can help automate the configuration process by loading configuration files onto new or existing devices automatically over the network. You can use either the J-Web interface or the CLI to configure a device for autoinstallation.

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the services gateway.

Autoinstallation takes place automatically when you connect an Ethernet port on a new services gateway to the network and power on the device. To simplify the process, you can explicitly enable autoinstallation on a device and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

NOTE: If the USB autoinstallation feature is enabled (the default configuration), removal of a USB storage device immediately after insertion is not supported.

After you insert a USB storage device, Junos OS scans the device to check whether it contains the USB autoinstallation file. This process might take up to 50 seconds to complete depending on the quality of the USB storage device and the number and size of the files in the device. Removing the USB storage device while this process is running might cause the services gateway to reboot, the USB port to stop working, and data loss on the USB. We recommend that after inserting a USB storage device, you wait for at least 60 seconds before removing it.

By issuing the `set system autoinstallation usb disable` command (which disables the USB autoinstallation feature) before you insert the USB device, you can reduce the waiting interval between insertion and removal of a USB storage device from 60 seconds to 20 seconds.

For more information about configuring autoinstallation, see the following topics:

- Installation and Upgrade Guide for Security Devices
- Monitoring and Troubleshooting Guide

Unpacking and Mounting the SRX320

IN THIS SECTION

Unpacking the SRX320 Services Gateway

The SRX320 Services Gateway is shipped in a cardboard carton and secured with foam packing material. The carton also contains an accessory box and quick-start instructions.

To unpack the SRX320 Services Gateway:

1. Move the cardboard carton to a staging area as close to the installation site as possible, where you have enough room to remove the components from the chassis.
2. Position the cardboard carton with the arrows pointing up.
3. Carefully open the top of the cardboard carton.
4. Remove the foam covering the top of the services gateway.
5. Remove the accessory box.
6. Verify the parts received against the lists in "Verifying Parts Received with the SRX320 Services Gateway" on page 36.
7. Store the brackets and bolts inside the accessory box.
8. Save the shipping carton and packing materials in case you need to move or ship the services gateway at a later time.

Verifying Parts Received with the SRX320 Services Gateway

The SRX320 Services Gateway shipment package contains a packing list. Check the parts in the shipment against the items on the packing list. The packing list specifies the part numbers and carries a brief description of each part in your order.

If any part is missing, contact a customer service representative.

A fully configured services gateway contains the chassis with installed components, listed in Table 15 on page 36, and an accessory box, which contains the parts listed in Table 16 on page 37.

NOTE: The parts shipped with your services gateway can vary depending on the configuration you ordered. To know the part numbers for ordering the separately orderable mounting kits, see the SRX300 Line of Services Gateways for the Branch Platform Datasheet.

Table 15: Parts List for a Fully Configured SRX320 Services Gateway

Component	Quantity
SRX320 services gateway	1
CAT5E cable	1
DB9-to-RJ45 adapter	1
USB console cable with Type-A and Mini-B USB plugs	1
Documentation Roadmap and Product Warranty	1
Power supply adapter and power cord • 75 W, 12 V power supply adapter for non-PoE models • 280 W, 54 V power supply adapter for PoE models	1

Table 16: Accessory/Upgrade Parts List for the SRX320 Services Gateway

Part	Quantity
End User License Agreement	1
RoHS Card	1

Installing the SRX320 Services Gateway on a Desk

You can mount an SRX320 Services Gateway on a desk or any other level surface horizontally or vertically. The four rubber feet attached to the chassis provide stability. Before mounting an SRX320 Services Gateway on a desk or other level surface:

- Verify that the installation site meets the requirements described in "SRX320 Site Preparation Checklist" on page 18.
- Place the desk in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the building structure.

The horizontal position is the standard installation position. To install the device in a horizontal position:

1. Make sure that the rubber feet are attached to the chassis.
2. Place the device on a desk with the Juniper Networks logo, which is embossed on the top cover, facing up.

NOTE: For information on installing Mini-Physical Interface Modules (Mini-PIMs), see SRX300 Series and SRX550 High Memory Services Gateway Interface Modules Reference.

Installing the SRX320 Services Gateway on a Wall

You can mount an SRX320 Services Gateway on a wall. The four rubber feet attached to the chassis provide stability. Before mounting the SRX320 Services Gateway on a wall:

- Verify that the installation site meets the requirements described in "SRX320 Site Preparation Checklist" on page 18.

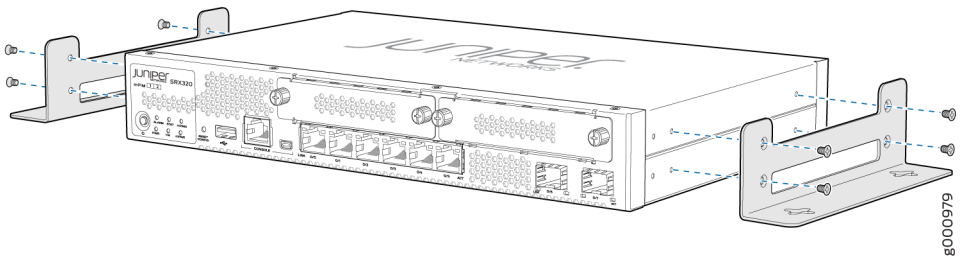
- Verify that you have the following parts available in your wall-mounting kit:
  - Wall-mounting brackets
  - Screws

NOTE: The wall-mounting kit is not shipped with the device and must be ordered separately.

To install the device on a wall:

1. Place the device on a flat, level surface with the Juniper Networks logo, which is embossed on the top cover, facing up. Ensure that the rubber feet are attached to the bottom of the chassis.
2. Position a mounting bracket on each side of the chassis as shown in Figure 8 on page 38.

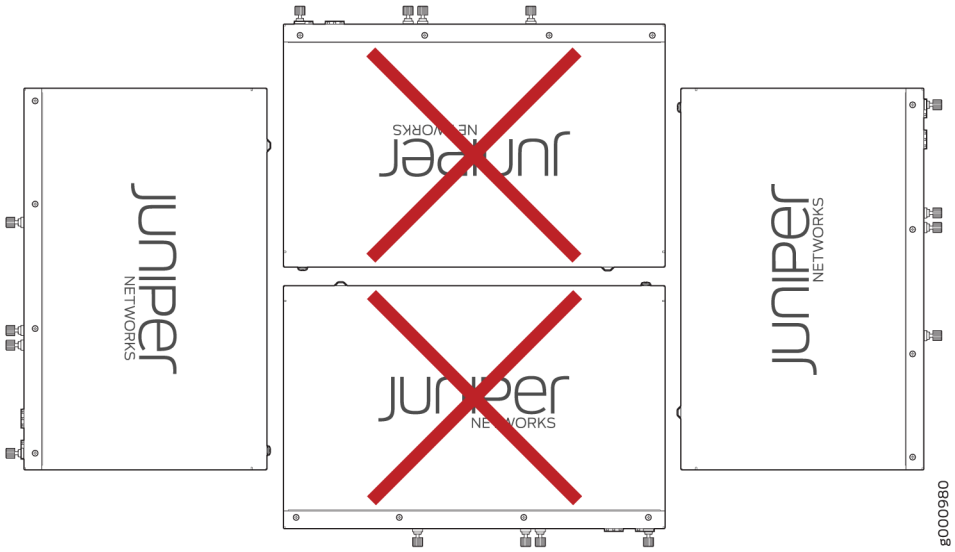
Figure 8: Attaching Wall-Mount Brackets



3. Use a number-2 Phillips screwdriver to install the screws that secure the mounting brackets to the chassis.
4. If you are using wall anchors to support the chassis, install two pairs of anchors on the wall with the mounting brackets attached.
5. Have one person grasp the sides of the device, lift it, and position it on the wall.

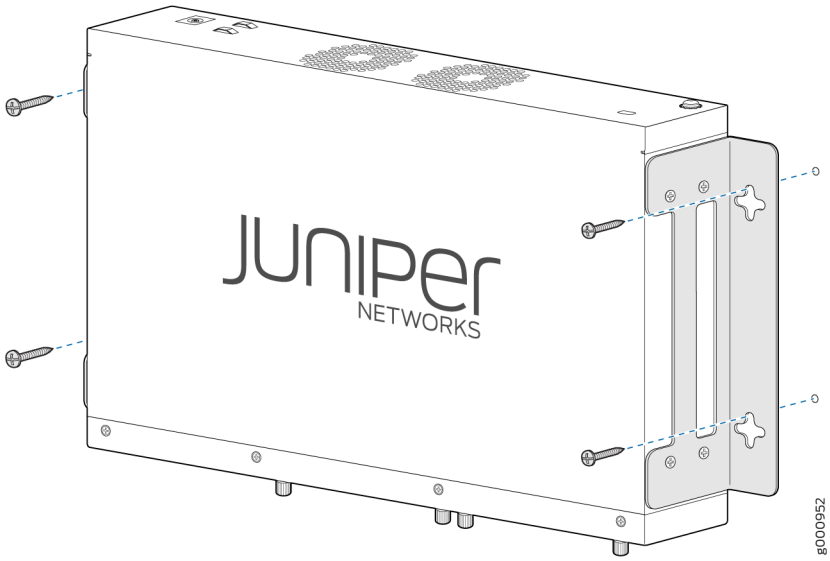
6. Have a second person install two pairs of mounting screws through the bracket holes on either side of the device to secure it to the wall. Figure 9 on page 39 shows the two different orientations in which you can mount the services gateway on a wall.

Figure 9: Orienting the SRX320 Services Gateway on a Wall



7. Verify that the mounting screws on one side are aligned with the mounting screws on the opposite side and that the device is level.

Figure 10: Mounting the SRX320 Services Gateway on a Wall



NOTE: For information on installing Mini-Physical Interface Modules (Mini-PIMs), see SRX300 Series and SRX550 High Memory Services Gateway Interface Modules Reference.

Installing the SRX320 Services Gateway in a Rack

You can mount an SRX320 Services Gateway in four-post (telco) racks, enclosed cabinets, and open-frame racks.

NOTE: The SRX320 Services Gateway cannot be center-mounted in racks.

Before mounting the SRX320 Services Gateway in a rack:

- Verify that the installation site meets the requirements described in "SRX320 Site Preparation Checklist" on page 18.

- Verify that the racks or cabinets meet the specific requirements described in SRX320 Services Gateway Rack-Mounting Requirements and Warnings.
- Place the rack or cabinet in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the building structure. For more information, see "SRX320 Services Gateway Clearance Requirements for Airflow and Hardware Maintenance" on page 26.
- Verify that you have the following parts available in your rack-mounting kit:
  - Rack-mount tray
  - Screws

NOTE: The rack-mounting kit is not shipped with the device and must be ordered separately.

NOTE: If you are installing multiple devices in one rack, install the lowest one first and proceed upward in the rack. Ensure that the rubber feet from the base of the chassis are removed for rack installation.

To install the device in a rack:

1. Position a mounting bracket on each side of the chassis as shown in Figure 11 on page 42 and Figure 12 on page 42.

Figure 11: Positioning the Mounting Brackets (75 W Power Supply Adapter)

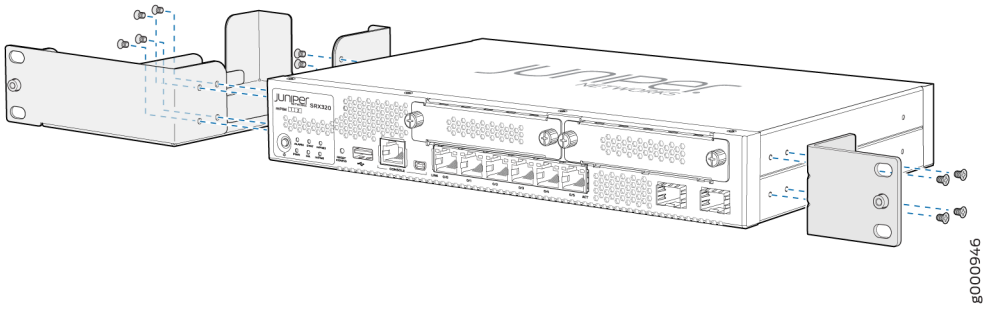
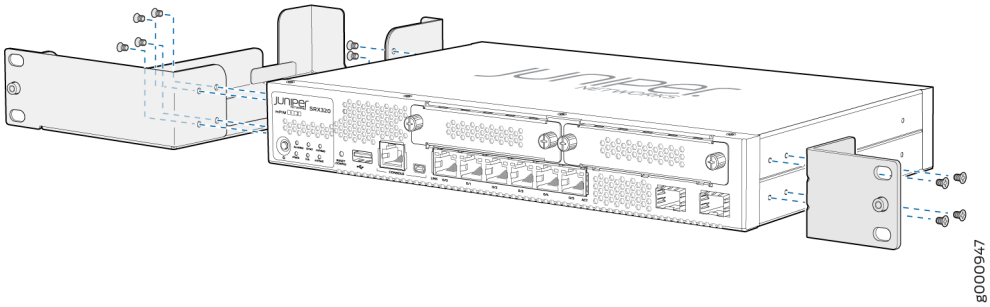
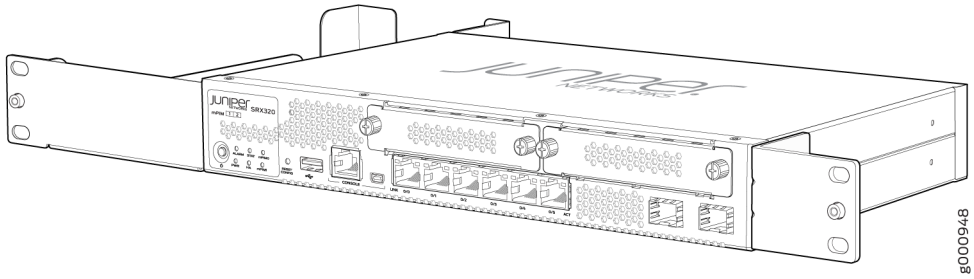


Figure 12: Positioning the Mounting Brackets (280 W Power Supply Adapter)



2. Use a number-2 Phillips screwdriver to install the screws that secure the mounting brackets and power supply adapter tray to the chassis as shown in Figure 13 on page 42.

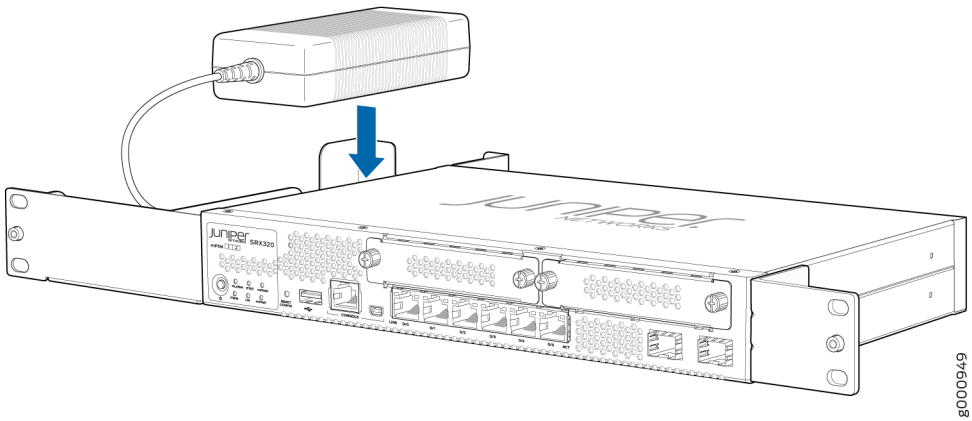
Figure 13: Securing the Mounting Brackets



3. Place the power supply adapter in the tray as shown in Figure 14 on page 43.

NOTE: The 280 W power adapter for the PoE model is more than 1 RU tall. When installing the PoE model in a rack, note that you will not be able to install devices in the adjacent slots in a rack.

Figure 14: Positioning the Power Supply Adapter



4. Have one person grasp the sides of the device, lift it, and position it in the rack.

5. Align the bottom hole in each mounting bracket with a hole in each rack rail as shown in Figure 15 on page 44 and Figure 16 on page 45, making sure the chassis is level.

Figure 15: Positioning the SRX320 Services Gateway (PoE Model with 280 W Power Supply Adapter) in a Rack

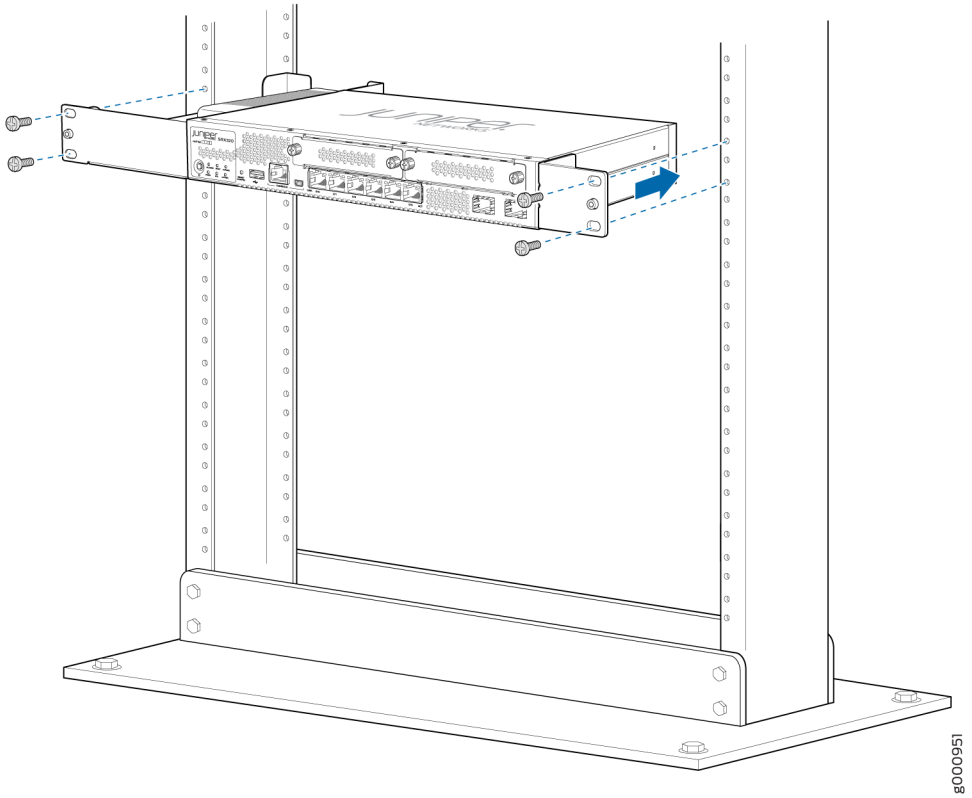
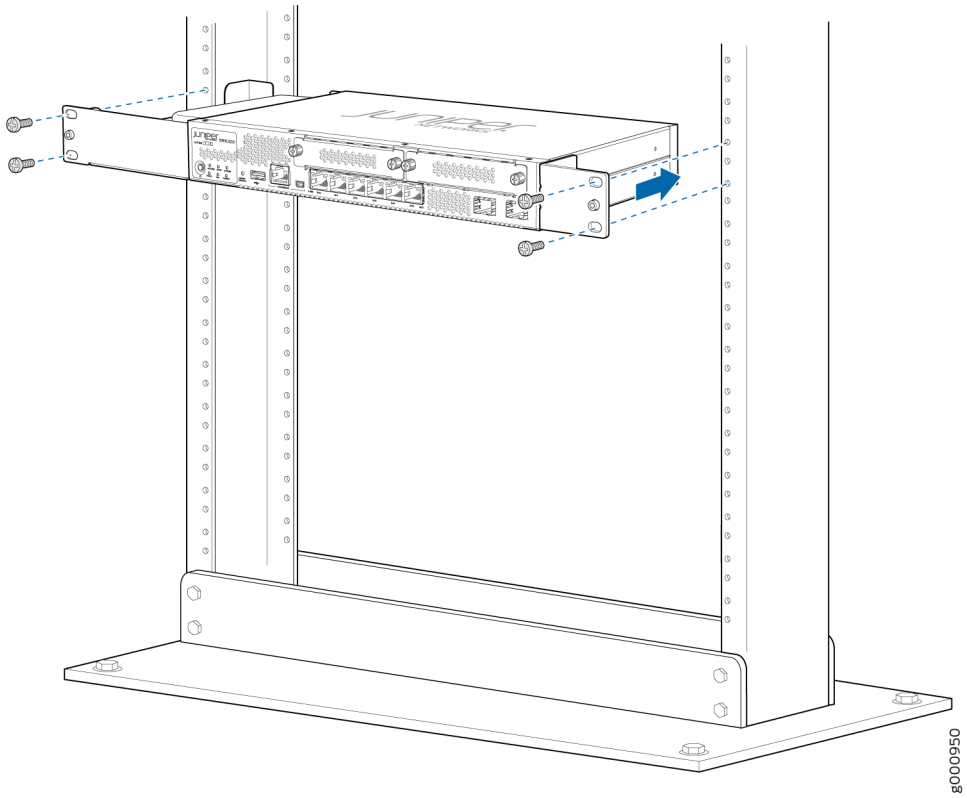


Figure 16: Positioning the SRX320 Services Gateway (with 75 W Power Supply Adapter) in a Rack



6. Have a second person install a mounting screw into each of the two aligned holes. Tighten the mounting screws.
7. Install the second screw in each mounting bracket.
8. Verify that the mounting screws on one side of the rack are aligned with the mounting screws on the opposite side and that the device is level.

NOTE: For information on installing Mini-Physical Interface Modules (Mini-PIMs), see SRX300 Series and SRX550 High Memory Services Gateway Interface Modules Reference.

RELATED DOCUMENTATION

SRX320 Site Guidelines and Requirements | 20

Connecting the SRX320 to Power

IN THIS SECTION

Required Tools and Parts for Grounding the SRX320 Services Gateway

To ground and to provide power to the services gateway, you need the following tools:

- Phillips (+) screwdrivers, numbers 1 and 2
- Electrostatic discharge (ESD) grounding wrist strap
- Wire cutters

Connecting the SRX320 Services Gateway Grounding Cable

You ground the services gateway by connecting a grounding cable to earth ground and then attaching it to the chassis grounding point located on the back panel of the device using one M4 grounding screw. You must install the SRX320 in a restricted-access location and ensure that the chassis is always properly grounded. The SRX320 has a single-hole protective grounding terminal provided on the chassis. See Figure 17 on page 47. We recommend that you use this protective grounding terminal as the preferred method for grounding the chassis regardless of the power supply configuration. However, if additional grounding methods are available, you can also use those methods. For example, you can use the grounding wire in the AC power cord or use the grounding terminal or lug on a DC power supply. This tested system meets or exceeds all applicable EMC regulatory requirements with the single-hole protective grounding terminal.

You must provide the following items:

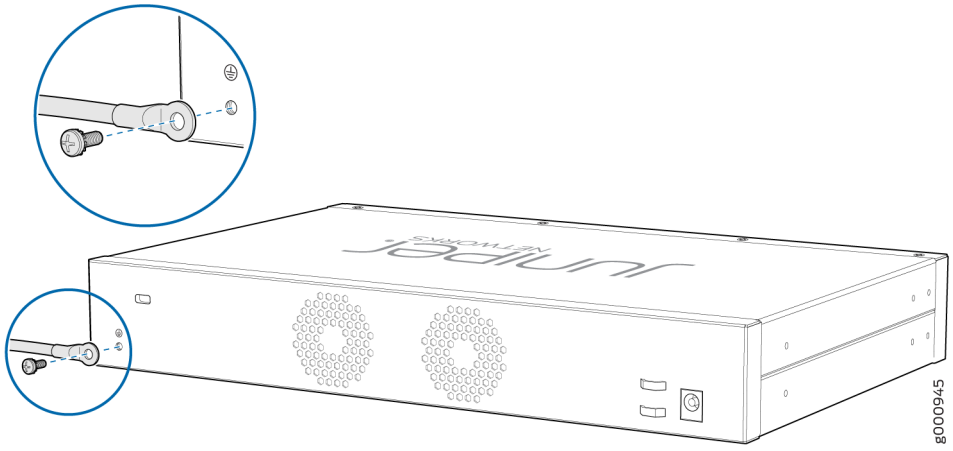
- M4 grounding screw
- Grounding cables
- Cable lugs (for example, Panduit LCC6-10A-L)

> **CAUTION**: Before you connect power to the services gateway, 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 services gateway (for example, by causing a short circuit).

To ground the device:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to the ESD point on the chassis. For more details, see *Prevention of Electrostatic Discharge Damage*.
2. Ensure that all grounding surfaces are clean and brought to a bright finish before grounding connections are made.
3. Connect the grounding cable to a proper earth ground.
4. Place the grounding cable lug over the grounding point (sized for M4 grounding screws) on the rear of the chassis.
5. Secure the grounding cable lug to the grounding point, first with the washer, then with the screw. Apply between 6 in.-lb (0.67 Nm) and 8 in.-lb (0.9 Nm) of torque to the screw.
6. Dress the grounding cable and verify that it does not touch or block access to the services gateway components and that it does not drape where people could trip on it.

Figure 17: Connecting the SRX320 Services Gateway Grounding Cable



NOTE: The device should be permanently connected to ground during operation.

SEE ALSO

SRX320 Services Gateway Grounding Specifications | 24

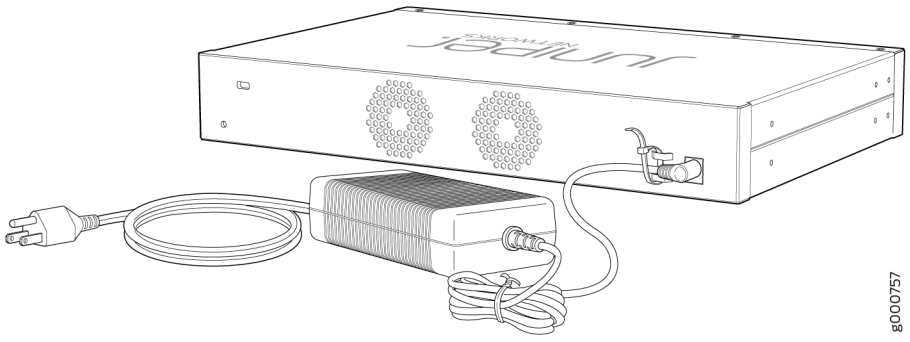
Connecting the SRX320 Services Gateway to the Power Supply

To connect the device to the power supply:

CAUTION: Before connecting the device to the power supply, attach an ESD strap to an ESD point and place the other end of the strap around your bare wrist.

1. Plug the DC connector end of the power cable into the power connector on the back of the device as shown in Figure 18 on page 48.
2. Plug the AC adapter end of the power cable into an AC power outlet.

Figure 18: Connecting the SRX320 Services Gateway to the Power Supply



SEE ALSO

Understanding the SRX320 Services Gateway Power Supply | 13

SRX320 Services Gateway Power Specifications and Requirements | 14

Powering On the SRX320 Services Gateway

To power on the services gateway:

1. Ensure that you have connected the power supply to the device.
2. Insert the plug of the power supply adapter into an AC power source receptacle.
3. Turn on the power to the AC power receptacle.

The device starts automatically as the power supply completes its startup sequence. The PWR LED lights during startup and remains on when the device is operating normally.

NOTE: After the power supply is turned on, it can take up to 60 seconds for status indicators—such as the STAT and PWR LEDs—to show that the power supply is functioning normally. Ignore error indicators that appear during the first 60 seconds.

NOTE: When the system is completely powered off and you turn on the power supply, the device starts as the power supply completes its startup sequence. If the device finishes starting and you need to power off the system again, first issue the CLI `request system power-off` command.

Powering Off the SRX320 Services Gateway

You can power off the services gateway in one of the following ways:

- Graceful shutdown—Press and immediately release the Power button. The device begins gracefully shutting down the operating system and then powers itself off.

  CAUTION: Use the graceful shutdown method to power off or reboot the services gateway.

- Forced shutdown—Press the Power button and hold it for ten seconds. The device immediately powers itself off without shutting down the operating system.

CAUTION: Use the forced shutdown method as a last resort to recover the services gateway if the services gateway operating system is not responding to the graceful shutdown method.

WARNING: Do not press the Power button while the device is shutting down.

CAUTION: Forced shutdown can result in data loss and corruption of the file system.

NOTE: To remove power completely from the device, unplug the power cord or switch off the AC power source.

After powering off a power supply, wait at least 10 seconds before turning it back on. After powering on a power supply, wait at least 10 seconds before turning it off.

The power button on the services gateway is a standby power switch, which will not turn off the input power to the services gateway.

TIP: When you are powering off the device, the CLI displays the following message: `Turning the system power off`. You can now safely remove the power cable to completely power off the device.

NOTE: You can use the **request system reboot** CLI command to schedule a reboot.

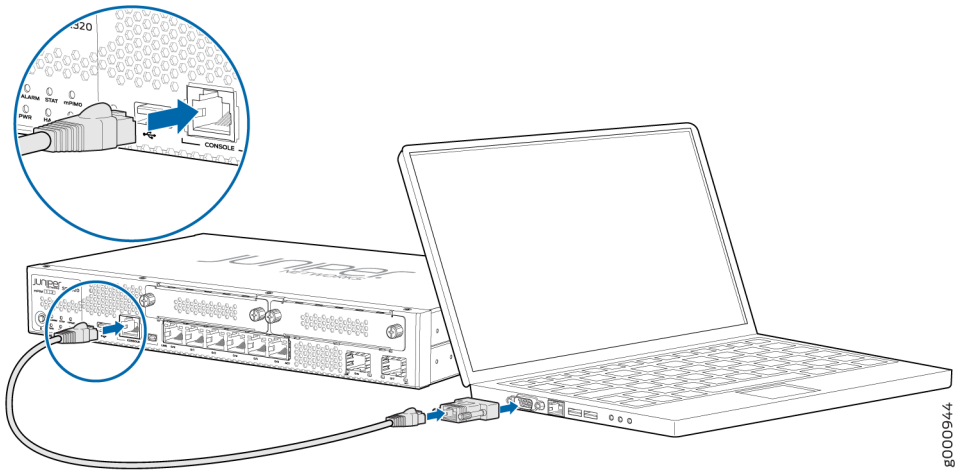
Connecting the SRX320 Services Gateway to a Management Console

Use the CONSOLE port on the services gateway to connect to a management console.

To connect the SRX320 Services Gateway to a management console, use an RJ-45 cable:

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. Plug the RJ-45 end of the cable into the CONSOLE port on the SRX320 Services Gateway as shown in Figure 19 on page 51.

Figure 19: Connecting the SRX320 Services Gateway to a Management Console



3. Connect the other end of the Ethernet cable to the supplied DB-9 adapter, which then connects to the serial port on the management device (serial port settings: 9600-N-1).

> **NOTE**: Alternately, you can use the USB cable to connect to the mini-USB console port on the services gateway. To use the mini-USB console port, you must download a USB driver to the management device from the Downloads page. To download the driver for Windows OS, select **6.5** from the **Version** drop-down list. To download the driver for Mac OS, select **4.10** from the **Version** drop-down list.

SRX320 Services Gateway Factory-Default Settings

IN THIS SECTION

Plug and Play for Cloud-Based Provisioning | 54

The SRX320 ships with the following factory-default settings:

Table 17: Security Policies

Source Zone	Destination Zone	Policy Action
trust	trust	permit
trust	untrust	permit

Table 18: NAT Rules

Source Zone	Destination Zone	Policy Action
trust	untrust	Source NAT to untrust zone interface

Table 19: Ethernet Interfaces

Port Label	Interface	Security Zone	DHCP State	IP Address
0/0 and 0/7	ge-0/0/0 and ge-0/0/7	untrust	Client	Unassigned
0/1 to 0/6	VLAN interface irb.0 (ge-0/0/1 to ge-0/0/6)	trust	Server	192.168.1.1/24

Table 20: LTE Interfaces

Interface	Security Zone	IP Address
cl-1/0/0	N/A	N/A
dl0 (logical)	untrust	ISP assigned*

Table 20: LTE Interfaces *(Continued)*

Interface	Security Zone	IP Address

*Only if the LTE Mini-PIM is present

The SRX320 ships with the following services and protocols enabled by default:

Table 21: Services, Protocols, and Startup Mode

Services	Protocols	Device Startup Mode
SSH HTTPS NETCONF over SSH	RSTP (all interfaces)	Switching

To provide secure traffic, a basic set of screens are configured on the untrust zone. In addition, the default security policy blocks traffic that originates from any untrust zone interface from passing to the trust zone.

How to Load and View Factory-Default Settings

Your device ships with a set of factory-default configuration files. To view the factory-default settings on your device:

1. Log in as the root user and provide your credentials.
2. View the full list of default configuration files for various hardware platforms:

```
user@host> file list /etc/config
```

3. To display the contents of a specific default configuration file:

```
user@host> file show /etc/config/<config file name>
```

When you commit changes to the configuration, a new configuration file is created, which becomes the active configuration. You can always load a fresh factory-default configuration with the `load factory-default` configuration mode command to revert to the factory-default configuration. The Junos software selects the correct default configuration for the hardware platform when you issue the *load factory-default* configuration command.

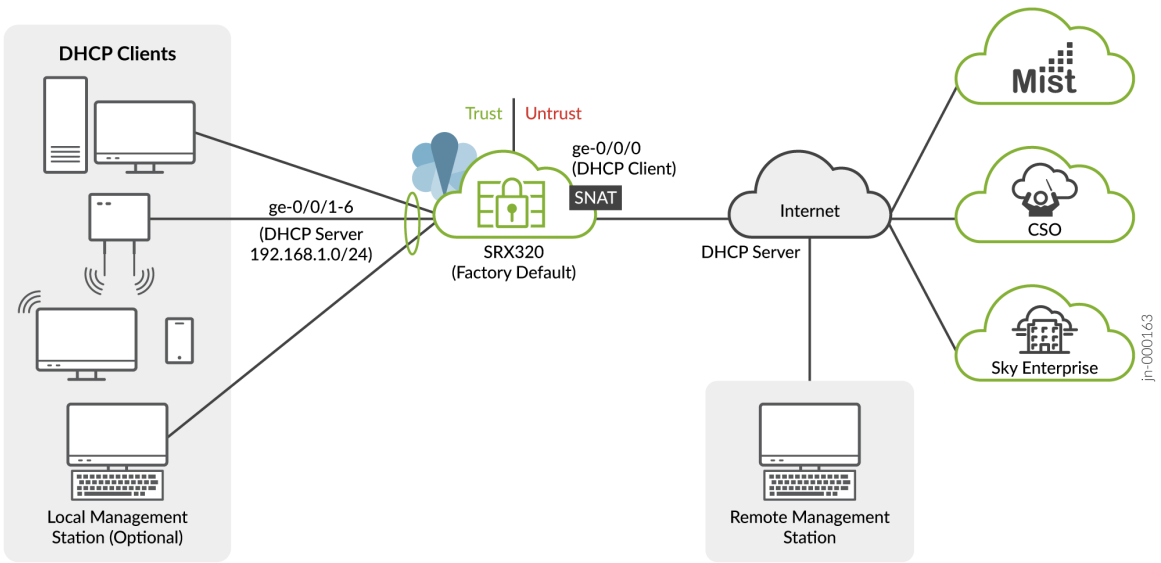
You use the `show configuration` operational mode command, or simply the `show` command when in configuration mode, to view the settings.

NOTE: You can also load a factory default configuration using the front panel RESET CONFIG button. See "Using the RESET CONFIG Button on the SRX320 Services Gateway" on page 74.

Plug and Play for Cloud-Based Provisioning

This section shows you how to leverage the SRX320 factory defaults for Plug and Play Internet connectivity. You use this connectivity to remotely manage and configure the SRX320, either manually or through a cloud-based provisioning service.

Follow these steps to quickly get your SRX320 on the Internet to access cloud-based provisioning services such as Juniper Mist Cloud or Contrail Service Orchestration (CSO). The Plug and Play connectivity of the SRX320 with a factory default configuration is shown below.



1. Connect the WAN network to port 0/0 (ge-0/0/0). In the default configuration the ge-0/0/0 is your WAN interface. In the default configuration this interface is placed in the untrust zone and is configured as a DHCP client. These settings allow the SRX to receive an IP address and default route from the service provider.

2. Configure your LAN clients (PCs, notebooks, APs, etc.) for DHCP address assignment. Attach these devices to any of the LAN ports from 0/1 through 0/6 (ge-0/0/1 through ge-0/0/6). That's it, you're done!

   In the default configuration the LAN ports are configured in a trust VLAN with an associated IRB interface. DHCP services are provided to the trust VLAN through that IRB interface, which is also placed into the trust zone. The result is that all LAN ports share a common IP subnet with full Layer 2 (untagged) connectivity through the SRX. At Layer 3, the IRB interface associates the LAN with a 192.168.1.0/24 subnet, with the 192.168.1.1 address reserved for itself.

   The LAN devices are assigned an IP address and default gateway from the 192.168.1.0/24 subnet through DHCP.

3. Verify that the SRX320 is providing Internet connectivity. Open a browser on a device attached to a LAN port and point it to http://www.juniper.net. If the page doesn't load, check the Internet connection.

   To isolate any faults, try these steps:

   - Power cycle the WAN modem. Verify the modem is correctly connecting to the service provider.
   - Ping an Internet destination from the SRX320 using the CLI to test internet connectivity. Make sure the destination is allowed to reply to pings, and try using both a name and IP address to isolate DNS from connectivity issues.
   - Generate a ping from a LAN device to the 192.168.1.1 address assigned to the IRB interface on the SRX. A successful reply validates DHCP and Layer 2 connectivity between the LAN devices and the SRX.
   - Use the `show dhcp server binding` command to check the LAN side DHCP server address assignments.

   At this point, both the SRX320 and the LAN devices have Internet access. The default policy permits all traffic from the trust to untrust zone. The default policy also perform SNAT on traffic leaving the WAN. By default all response traffic is allowed back from the untrust to the trust zone. Traffic that originates in the untrust (WAN) zone is blocked from the trust zone. HTTPS, TFTP, and DHCP traffic is allowed to originate from the untrust zone and be sent to the local host.

   You are able to access the SRX using J-Web to perform initial configuration both locally and remotely. For local access, use a machine attached to a LAN port and point your browser to https://191.168.1.1. To access remotely, over the WAN interface, you need to know the IP address assigned to the SRX by the WAN provider. See No Link Title for details on performing initial setup using J-

Web setup wizard. You can always access the SRX320 locally using the console port to perform additional configuration. Refer to SRX320 Day One+ for details on using the CLI for initial configuration.

> **NOTE**: In the default configuration a password is not needed to access the SRX320 using J-Web, either locally or remotely. You should either adopt the SRX into a cloud provisioning service, or manually configure a root password (using J-Web or the Junos CLI), as soon as possible after attaching your SRX to the Internet.

Configuring Junos OS on the SRX320

IN THIS SECTION

The SRX320 Services Gateway is shipped with the Juniper Networks Junos operating system (Junos OS) preinstalled and is ready to be configured when the SRX320 is powered on. You can perform the initial software configuration of the SRX320 by using one of the following methods:

- Command-line interface (CLI)
- Zero touch provisioning (ZTP) with a cloud-based provisioning service
- J-Web GUI

Before you configure your new SRX320, we recommend that you understand the factory-default configuration. In many cases you are able to leverage the factory defaults to simplify your configuration tasks. In other cases, you might find it easier to start with a blank configuration when you find that the defaults don't align with your planned usage. See "SRX320 Services Gateway Factory-Default Settings" on page 51 for details on the factory-default configuration.

Initial Configuration Using the CLI

IN THIS SECTION

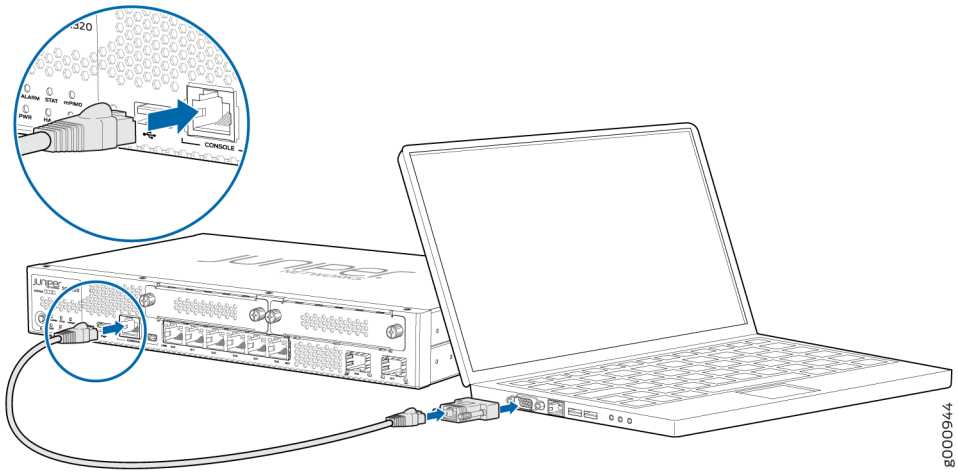
You can use either the serial or the mini-USB console port on the device.

Connect to the Serial Console Port

To connect to the serial console port:

1. Plug one end of the Ethernet cable into the RJ-45 to DB-9 serial port adapter supplied with your SRX320.
2. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device.
3. Connect the other end of the Ethernet cable to the serial console port on the SRX320.

Figure 20: Connect to the Console Port on the SRX320



4. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) and select the appropriate COM port to use (for example, COM1).
5. Configure the serial port settings with the following values:

- Baud rate—9600
- Parity—N
- Data bits—8
- Stop bits—1
- Flow control—none

Connect to the Mini-USB Console Port

To connect to the mini-USB console port:

1. Download the USB driver to the management device from the Downloads page. To download the driver for Windows OS, select **6.5** from the **Version** drop-down list. To download the driver for macOS, select **4.10** from the **Version** drop-down list.
2. Install the USB console driver software:

   > **NOTE**: Install the USB console driver software before attempting to establish a physical connection between the SRX320 and the management device, otherwise the connection will fail.

   a. Copy and extract the **.zip** file to your local folder.

   b. Double-click the **.exe** file. The installer screen appears.

   c. Click **Install**.

   d. Click **Continue Anyway** on the next screen to complete the installation.

      If you chose to stop the installation at any time during the process, then all or part of the software will fail to install. In such a case, we recommend that you uninstall the USB console driver and then reinstall it.

   e. Click **OK** when the installation is complete.
3. Plug the large end of the USB cable supplied with the SRX320 into a USB port on the management device.
4. Connect the other end of the USB cable to the mini-USB console port on the SRX320.
5. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) and select the new COM port installed by the USB console driver software. In most cases, this is the highest-numbered COM port in the selection menu.

   You can locate the COM port under **Ports (COM & LPT)** in **Windows Device Manager** after the driver is installed and initialized. This might take several seconds.

6. Configure the port settings with the following values:
   - Bits per second—9600
   - Parity—None
   - Data bits—8
   - Stop bits—1
   - Flow control—None
7. If you have not already done so, power on the SRX320 by pressing the **Power** button on the front panel. Verify that the **PWR** LED on the front panel turns green.

   The terminal emulation screen on your management device displays the startup sequence. When the SRX320 has finished starting up, a login prompt appears.

Configure the SRX320 Using the CLI

This section assumes you are performing initial configuration of a new SRX320 running a factory default configuration. We show you how to leverage the defaults to quickly get the SRX320 on the internet and able to be managed locally or remotely. See "SRX320 Services Gateway Factory-Default Settings" on page 51 for details on the SRX320 factory defaults.

For this section, however, we assume the service provider does not support DHCP address assignment on the WAN interface. This allows us to show you how to configure an interface and static route using the Junos CLI.

To perform initial configuration on the SRX320 using the CLI:

1. Login as the root user and start the CLI. No password is needed when running the factory default.

```
login: root
root@% cli
root>
```

> **NOTE**: You can view the current configuration, whether factory-default or not, by using the `show configuration` operational mode command.

2. Enter configuration mode.

```
root> configure
[edit]
root#
```

3. Remove the ZTP configuration and set the root user authentication.

   The ZTP configuration is not needed when performing the initial configuration using the CLI. Removing the ZTP configuration stops the periodic log messages that report the ZTP status on the console.

   Set the root authentication password using a cleartext value. You cannot commit the change that deactivates ZTP unless you also set the root password.

```
[edit]
root# delete chassis auto-image-upgrade
root# delete system phone-home
root# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

4. Commit the configuration to activate the changes that removed ZTP and configured the root password.

```
[edit]
root# commit
```

5. Configure the management interface. Given the factory default settings, we recommend using the ge-0/0/0 interface for remote management of the SRX320 over the WAN network. You can also locally manage the SRX320 using one of the LAN ports (ge-0/0/1 through ge-0/0/6).

   If the WAN service provider supports DHCP IP address assignment you skip this step and let the factory default settings work for you. In this example, the Internet provider requires a static IP address configuration. You must remove the default DHCP client setting in order to configure the IP address manually.

```
[edit]
root# delete interfaces ge-0/0/0 unit 0 family inet dhcp
root# set interfaces ge-0/0/0 unit 0 family inet address ip_address/mask
```

6. If the WAN service provider supports DHCP assignment of a default route you skip this step and let the factory default settings work for you. In this example, the Internet provider does not support

DHCP. Therefore, you configure a static default route to provide the management interface. This route is used to reach remote destinations, such as a cloud provisioning service or the remote management station.

```
[edit]
root# set routing-options static route 0.0.0.0/0 next-hop wan_gateway_ip_address
```

7. Enable the SSH protocol for remote access. By default, the root user cannot login remotely. You also enable root login over SSH in this step.

```
[edit]
root# set system services ssh root-login allow
```

8. Enable SSH host support for the ge-0/0/0 interface. Recall that in the default configuration the ge-0/0/0 interface is in the untrust zone, and that the untrust zone does not support host bound SSH.

```
[edit]
root# set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic
system-services ssh
```

9. Configure the hostname.

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

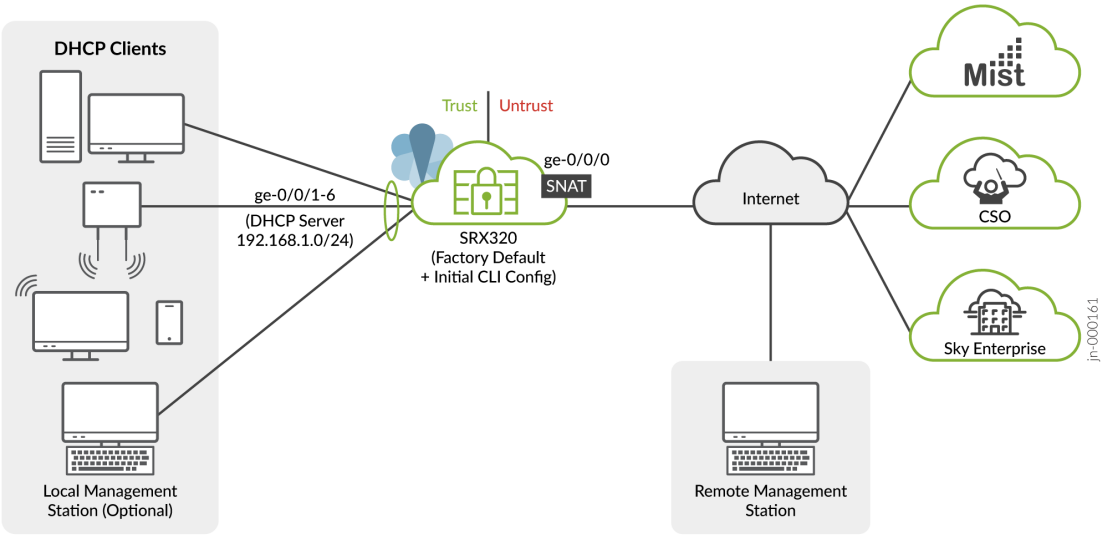
10. (Optional) Configure domain name resolution, the time zone, and an NTP-based clock source.

```
[edit]
root# set system name-server server_ip
root# set system ntp boot-server server_ip
root# set system ntp boot-server server_ip
root# set system time-zone time-zone
```

11. That's it! The initial configuration is complete. Commit the configuration to activate the changes on the SRX320.

```
[edit]
root# commit
```

The resulting connectivity is shown below.



A few things to keep in mind about your new SRX320 branch network:

• You access the SRX CLI or J-Web user interface locally using the 192.168.1.1 address. To access the SRX remotely, specify the IP address assigned by the WAN provider. Simply issue a show interfaces ge-0/0/0 terse CLI command to confirm the address in use by the WAN interface.

• Devices attached to the LAN ports are configured to use DHCP. They receive their network configuration from the SRX. These devices obtain an IP address from the 192.168.1.0/24 address pool and use the SRX as their default gateway.

• All LAN ports are in the same subnet with Layer 2 connectivity. All traffic is permitted between all trust zone interfaces.

• All traffic originating in the trust zone is permitted in the untrust zone. Matching response traffic is allowed back from the untrust to the trust zone. Traffic that originates from the untrust zone is blocked from the trust zone.

•The SRX performs source NAT (S-NAT) using the WAN interface's IP for traffic sent to the WAN that originated from the trust zone.

•Traffic associated with specific system services (HTTPS, DHCP, TFTP, and SSH) is permitted from the untrust zone to the local host. All local host services and protocols are allowed for traffic that originates from the trust zone.

Configure the SRX320 Using J-Web

IN THIS SECTION

Perform Initial Configuration Using J-Web

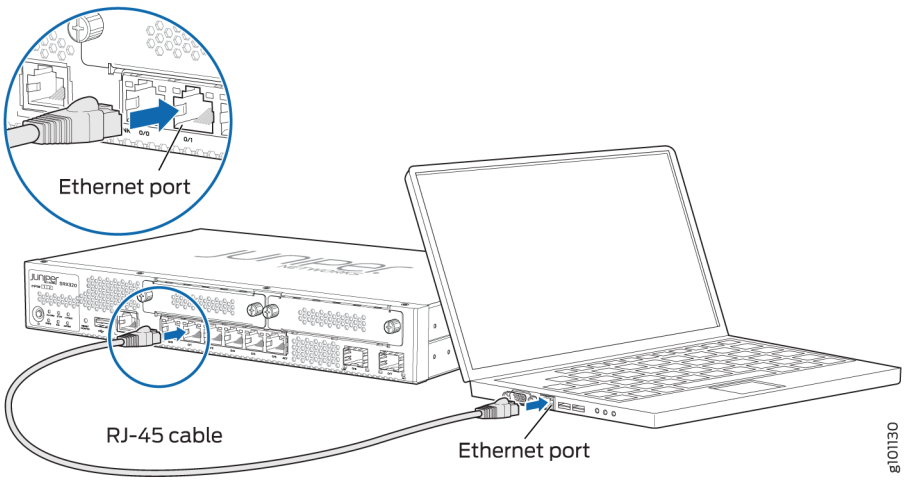
The J-Web user interface supports a setup wizard, which you can use to perform the initial configuration of the device.

1. Connect one end of the Ethernet cable to any of the network ports numbered **0/1** through **0/6** on the device.

   NOTE: The ge-0/0/0 and ge-0/0/7 interfaces (ports **0/0** and **0/7**) are WAN interfaces. Don't use these ports for the initial configuration procedure.

2. Connect the other end of the Ethernet cable to the management device.

Figure 21: Connect the SRX320 to a Management Device



The SRX320 functions as a DHCP server and automatically assigns an IP address to the laptop.

3. Ensure that the management device acquires an IP address on the 192.168.1.0/24 network from the device.

   If an IP address is not assigned to the management device, manually configure an IP address in the 192.168.1.0/24 network.

   > **NOTE**: Don't assign the 192.168.1.1 IP address to the management device, as this IP address is assigned to the SRX320.

4. Open a browser and enter `https://192.168.1.1` as the target URL. The J-Web screen appears. For information on accessing the J-Web interface, see Access the J-Web Interface. For information on using J-Web to perform initial configuration, see The J-Web Setup Wizard.

Manage the SRX320 Using J-Web

After initial device configuration is complete you can use J-Web to perform ongoing configuration, management, and health monitoring of your SRX320 device.

For more information, see the SRX J-Web documentation for your release at https://www.juniper.net/documentation/product/us/en/j-web-srx-series.

Configure the Device Using ZTP with Juniper Networks Network Service Controller

> **NOTE**: You can configure using ZTP for Junos OS Release 19.2 and earlier releases.

You can use ZTP to complete the initial configuration of the SRX320 in your network automatically, with minimum intervention.

Network Service Controller is a component of the Juniper Networks Contrail Service Orchestration platform that simplifies and automates the design and implementation of custom network services that use an open framework.

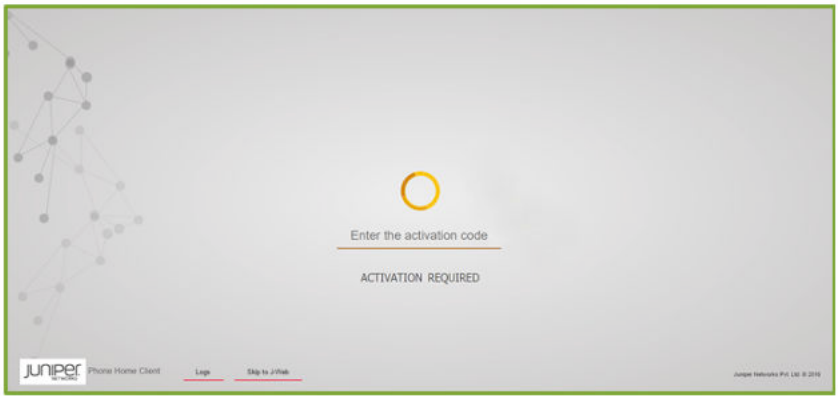
For more information, refer to the Network Service Controller section in the datasheet at http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000559-en.pdf.

To configure the device automatically using ZTP:

NOTE: To complete the ZTP process, ensure that the SRX320 is connected to the Internet.

- If you already have the authentication code, enter the code in the webpage displayed.

Figure 22: Authentication Code Page



On successful authentication, the initial configuration is applied and committed on the SRX320. Optionally, the latest Junos OS image is installed on the SRX320 before the initial configuration is applied.

- If you do not have the authentication code, you can use the J-Web setup wizard to configure the SRX320. Click **Skip to J-Web** and configure the SRX320 using J-Web.

RELATED DOCUMENTATION

Day One: SRX Series Up and Running with Advanced Security Services

4

CHAPTER

Maintaining Components

Maintaining the SRX320 Components

IN THIS SECTION

Required Tools and Parts for Maintaining the SRX320 Services Gateway Hardware Components

The following tools and parts are required to maintain the hardware components of the services gateway:

- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Flat-blade screw-blade screwdriver, approximately 1/8 in. (3 mm)
- Phillips (+) screwdrivers, numbers 1 and 2

Routine Maintenance Procedures for the SRX320 Services Gateway

For optimum performance of the services gateway, perform the following preventive maintenance procedures regularly:

- 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 LEDs on the front panel of the services gateway and on the Mini-Physical Interface Module (Mini-PIM) that you are using.

Maintaining the SRX320 Services Gateway Cooling System Components

The services gateway cooling system works to maintain an optimal temperature for the device. If the fan controller fails, the device temperature will exceed the maximum working temperature, and the device will fail. Ensure that you maintain the recommended clearances behind the device to enable the cooling system to function optimally.

SEE ALSO

SRX320 Cooling System | 12

Maintaining the SRX320 Services Gateway Power Supply

To maintain the power supply on the services gateway:

- Make sure that the power and grounding cables are arranged so that they do not obstruct access to other device components.
- Routinely check the PWR LED on the front panel. If this LED is solid green, the power supplies are functioning normally.
- Periodically inspect the site to ensure that the grounding and power cables connected to the services gateway are securely in place and that there is no moisture accumulating near the services gateway.

CAUTION: We recommend using a surge protector for the power connection.

SEE ALSO

SRX320 Power System | 13

Replacing Mini-Physical Interface Modules in the SRX320 Services Gateway

The Mini-PIMs available on the SRX320 Services Gateway are not hot-swappable. You need to power off the device before removing or installing Mini-PIMs. For information on replacing Mini-PIMs, see SRX300 Series and SRX550 High Memory Services Gateway Interface Modules Reference.

SEE ALSO

SRX320 Services Gateway Interface Modules Overview | 11

5

CHAPTER

Troubleshooting Hardware

Troubleshooting the SRX320

IN THIS SECTION

Troubleshooting Resources for the SRX320 Services Gateway Overview

To troubleshoot a services gateway, you use the Junos OS command-line interface (CLI) and LEDs on the components:

- LEDs—When the services gateway detects an alarm condition, the alarm LED on the interfaces glows red or yellow.
- CLI—The CLI is the primary tool for controlling and troubleshooting hardware, Junos OS, and network connectivity. Use the CLI to display more information about alarms. CLI commands display information about network connectivity derived from the ping and traceroute utilities. For information about using the CLI to troubleshoot Junos OS, see the appropriate Junos OS configuration guide.
- JTAC—If you need assistance during troubleshooting, you can contact the Juniper Networks Technical Assistance Center (JTAC) by using the Web or by telephone. If you encounter software problems, or problems with hardware components not discussed here, contact JTAC.

Troubleshooting Chassis and Interface Alarm Messages on the SRX320 Services Gateway

When the services gateway detects an alarm condition, the alarm LED on the front panel turns red or amber as appropriate. To view a more detailed description of the alarm cause, issue the `show chassis alarms` CLI command.

Table 22 on page 72 describes alarms that can occur for an SRX320 Services Gateway chassis component.

Table 22: SRX320 Services Gateway Chassis Alarm Conditions and Corrective Actions

Component	Alarm Conditions	Action	Alarm Severity
Boot media	The services gateway boots from an alternate boot device.	• If the internal flash memory fails at startup, the services gateway automatically boots itself from the alternative boot device (USB storage device). **NOTE**: If you configured your services gateway to boot from an alternative boot device, ignore this alarm condition. • Reformat the internal flash memory and install a bootable image. (See the Installation and Upgrade Guide for Security Devices and Network Monitoring and Troubleshooting Guide for Security Devices) • If you did not configure the services gateway to boot from an alternative boot device, contact JTAC.	Amber (minor)
Hardware components on the services gateway	The services gateway chassis temperature or chassis is too warm	Check the room temperature. See "SRX320 Services Gateway Environmental Specifications" on page 21.	Amber (minor)
	The services gateway temperature is too high, either because of an internal overheating condition or because the maximum recommended room temperature has been exceeded.	The services gateway shuts down automatically in 4 minutes.	Red (major)

Table 22: SRX320 Services Gateway Chassis Alarm Conditions and Corrective Actions *(Continued)*

Component	Alarm Conditions	Action	Alarm Severity
Mini-PIM	A Mini-PIM has failed.	• Contact the Juniper Networks Technical Assistance Center (JTAC). • If you must replace the failed Mini-PIM, see SRX300 Series and SRX550 High Memory Services Gateway Interface Modules Reference for information about replacing the Mini-PIMs.	Red (major)

Troubleshooting the Power System on the SRX320 Services Gateway

The LEDs on the services gateway enable you to determine the performance and operation. The PWR LED, located on the front panel of the services gateway, indicates the different settings with respect to the power system.

Table 23 on page 73 describes different PWR LED status settings and their corrective actions.

Table 23: SRX320 Services Gateway Power LED Status

LED Status	Meaning	Possible Cause and Corrective Action
Green	Device is receiving power.	Normal indication. No action is required.
Amber	Indicates that the power button has been pressed and quickly released.	Normal indication. No action is required.

Table 23: SRX320 Services Gateway Power LED Status *(Continued)*

LED Status	Meaning	Possible Cause and Corrective Action
Off	Indicates that the device is not receiving power.	• Verify that the AC power cord from the power source to the device is not damaged. If the insulation is cracked or broken, immediately replace the cord or cable. • Ensure that the socket you plug in is in working condition. • Ensure the device has an AC input voltage between 100 and 240 VAC. • If you cannot determine the cause of the problem or need additional assistance, contact JTAC.

Using the RESET CONFIG Button

If a configuration fails or denies management access to the services gateway, you can use the RESET CONFIG button to restore the device to the factory-default configuration or a rescue configuration. For example, if someone inadvertently commits a configuration that denies management access to a services gateway, you can delete the invalid configuration and replace it with a rescue configuration by pressing the RESET CONFIG button.

NOTE: The RESET CONFIG button is recessed to prevent it from being pressed accidentally.

The rescue configuration is a previously committed, valid configuration. You must have previously set the rescue configuration through the J-Web interface or the CLI. To press the RESET CONFIG button, insert a small probe (such as a straightened paper clip) into the pinhole on the front panel.

- By default, pressing and quickly releasing the RESET CONFIG button loads and commits the rescue configuration through the J-Web interface or the CLI. The Status LED is solid amber during this time.
- By default, pressing and holding the RESET CONFIG button for 15 seconds or more—until the Status LED is solid amber — deletes all configurations on the device, including the backup configurations and rescue configuration, and loads and commits the factory configuration.

NOTE: Resetting the configuration does not trigger a reboot automatically. Thus, configuration changes that require a reboot, such as Ethernet switching configurations, do not take effect after you reset the configuration. As a result, connectivity to the device might be lost. For the configuration to take effect, power off and power on the device after resetting the configuration.

Changing the RESET CONFIG Button Behavior

You can change the default operation of the RESET CONFIG button by limiting how the button resets the services gateway:

- To prevent the RESET CONFIG button from setting the device to the factory-default configuration and deleting all other configurations:

  ```
  admin@host# set chassis config-button no-clear
  ```

  You can still press and quickly release the button to reset it to the rescue configuration.

- To prevent the RESET CONFIG button from setting the device to the rescue configuration:

  ```
  admin@host# set chassis config-button no-rescue
  ```

  You can still press and hold the button for 15 seconds or more to reset the gateway to the factory-default configuration.

- To disable the button and prevent the device from resetting to either the factory-default or rescue configuration:

  ```
  admin@host# set chassis config-button no-clear no-rescue
  ```

The **no-clear** option prevents the RESET CONFIG button from deleting all configurations on the services gateway. The **no-rescue** option prevents the RESET CONFIG button from loading the rescue configuration.

To return the function of the RESET CONFIG button to its default behavior, remove the **config-button** statement from the device configuration.

CHAPTER 6

Contacting Customer Support and Returning the Chassis or Components

Returning the SRX320 Chassis or Components

IN THIS SECTION

Contacting Customer Support

Once you have located the serial numbers of the device or component, you can return the device 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.

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

- Your existing service request number, if you have one

- Details of the failure or problem
- Type of activity being performed on the services gateway when the problem occurred
- Configuration data displayed by one or more `show` commands
- Your name, organization name, telephone number, fax number, and shipping address

The support representative validates your request and issues a Return Materials Authorization (RMA) number for return of the device or component.

Returning a SRX320 Services Gateway Component to Juniper Networks

To return an SRX320 Services Gateway or component to Juniper Networks for repair or replacement:

1. Determine the part number and serial number of the services gateway or component.
2. Obtain a Return Materials Authorization (RMA) number from JTAC.

> **NOTE**: Do not return the services gateway 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 SRX320 Services Gateway 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://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

Locating the SRX320 Services Gateway Chassis Serial Number and Agency Labels

The chassis serial number is located on the side of the chassis.

Locating the SRX320 Services Gateway Mini-Physical Interface Module Serial Number Label

Mini-PIMs are field-replaceable on the SRX320 Services Gateway. Each Mini-PIM has a unique serial number. The serial number label is located on the right side of the Mini-PIM, when the Mini-PIM is horizontally oriented (as it would be when installed on the device). The exact location might be slightly different on different Mini-PIMs, depending on the placement of components on the Mini-PIM.

Listing the SRX320 Services Gateway Component Details with the CLI

Before contacting Juniper Networks to request an RMA, you must find the serial number on the SRX320 Services Gateway or component.

To list all of the SRX320 Services Gateway components and their serial numbers, enter the following command:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                CX3315AN0019      SRX320-POE
Routing Engine   REV 02   650-065041   CX3315AN0019      RE-SRX320-POE
FPC 0                                                     FPC
  PIC 0                                                   6xGE,2xGE SFP Base PIC
Power Supply 0
```

NOTE: In the `show chassis hardware` command, the Mini-PIM slot number is reported as an FPC number, and the Mini-PIM number (always 0) is reported as the PIC number.

Most components also have a serial number ID label attached to the component body.

Required Tools and Parts for Packing the SRX320 Services Gateway

To remove the components from the SRX320 Services Gateway or to remove the services gateway from a rack, you need the following tools and parts:

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

Packing the SRX320 Services Gateway for Shipment

To pack the SRX320 Services Gateway for shipment:

1. Retrieve the shipping carton and packing materials in which the services gateway was originally shipped. If you do not have these materials, contact your Juniper Networks representative about approved packaging materials.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the device is disconnected from earth ground. For more information about ESD, see *Prevention of Electrostatic Discharge Damage*.
3. On the console or other management device connected to the services gateway, enter CLI operational mode and issue the following command to shut down the services gateway software:

   ```
   user@host> request system halt
   ```

   Wait until a message appears on the console confirming that the operating system has halted.
4. Shut down power to the services gateway by pressing the Power button on the front of the services gateway.
5. Disconnect power from the services gateway.
6. Remove the cables that connect to all external devices.
7. If the device is installed on a wall or rack, have one person support the weight of the device while another person unscrews and removes the mounting screws.
8. Place the services gateway in the shipping carton.
9. Cover the services gateway with an ESD bag, and place the packing foam on top of and around the device.
10. Replace the accessory box on top of the packing foam.
11. Securely tape the box closed.
12. Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.

Packing SRX320 Services Gateway Components for Shipment

Follow these guidelines for packing and shipping individual components of the services gateway:

- 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 services gateway components during packing.

CHAPTER 7

Safety and Compliance Information

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 be familiar 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.

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 of the 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.

Restricted Access Warning

WARNING: This unit 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.

Avertissement 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.

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.

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 23 on page 89) 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).

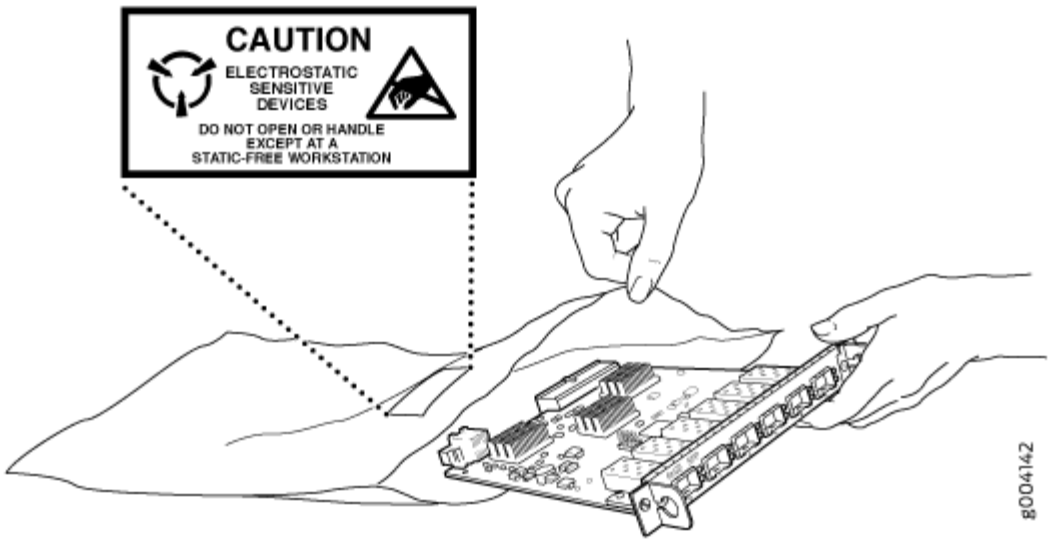
- When handling any component that is subject to ESD damage and that is removed from the device, make sure the equipment end of your ESD wrist strap is attached to the ESD point on the chassis.

  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 23 on page 89). If you are returning a component, place it in an antistatic bag before packing it.

Figure 23: 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.

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.

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 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.

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, then call for help.

General Electrical Safety Guidelines and Warnings

- Install the services gateway in compliance with the following local, national, or international electrical codes:
  - United States—National Fire Protection Association (NFPA 70), United States National Electrical Code
  - Canada—Canadian Electrical Code, Part 1, CSA C22.1
  - Other countries—International Electromechanical Commission (IEC) 60364, Part 1 through Part 7
  - Evaluated to the TN power system
- Locate the emergency power-off switch for the room in which you are working so that if an electrical accident occurs, you can quickly turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your workspace.
- Never assume that power is disconnected from a circuit. Always check the circuit before starting to work.
- Carefully look for possible hazards in your work area, such as moist floors, ungrounded power extension cords, and missing safety grounds.
- Operate the services gateway within marked electrical ratings and product usage instructions.
- For the services gateway and peripheral equipment to function safely and correctly, use the cables and connectors specified for the attached peripheral equipment, and make certain they are in good condition.

RELATED DOCUMENTATION

> *Action to Take After an Electrical Accident*

SRX320 Services Gateway Agency Approvals

IN THIS SECTION

The services gateway complies with the following standards:

- Safety
  - CAN/CSA-C22.2 No.60950-1 (2007) Information Technology Equipment
  - UL 60950-1 (2nd Ed.) Information Technology Equipment
  - EN 60950-1 (2006+ A11:2010) Information Technology Equipment - Safety
  - IEC 60950-1 (2005 +A1:2009) Information Technology Equipment - Safety (All country deviations): CB Scheme report
  - EN 60825-1 (2007) Safety of Laser Products - Part 1: Equipment classification and requirements
- EMC
  - EN 300 386 V1.6.1 Telecom Network Equipment - EMC requirements
  - EN 55032:2012 + EN55032:2012/AC:2013 Electromagnetic compatibility of multimedia equipment - Emission requirements
  - CISPR 32:2012
  - EN 55022:2010/AC:2011 European Radiated Emissions
  - CISPR 22 edition 6.0 : 2008-09
  - EN 55024: 2010 Information Technology Equipment Immunity Characteristics
  - CISPR 24 edition 2b :2010 COREC 2011 IT Equipment Immunity Characteristics
- EMI
  - FCC 47CFR , Part 15 Class A (2012) USA Radiated Emissions
  - ICES-003 Issue 5, August 2012 Canada Radiated Emissions

  - VCCI-V-3/2013.04 and V-4/2012.04 Japanese Radiated Emissions
  - BSMI CNS 13438 and NCC C6357 Taiwan Radiated Emissions
- Immunity
  - EN-61000-3-2 Power Line Harmonics
  - EN-61000-3-3 Voltage Fluctuations and Flicker
  - EN-61000-4-2 Electrostatic Discharge
  - EN-61000-4-3 Radiated Immunity
  - EN-61000-4-4 (2004) Electrical Fast Transients
  - EN-61000-4-5 (2006) Surge
  - EN-61000-4-6 (2007) Low Frequency Common Immunity
  - EN-61000-4-11 (2004) Voltage Dips and Sags
  - EN 55024 +A1+A2 (1998) Information Technology Equipment Immunity Characteristics
- Environmental
  - Reduction of Hazardous Substances (ROHS) 6
- Telco
  - Common Language Equipment Identifier (CLEI) code

Compliance Statement for Argentina

EQUIPO DE USO IDÓNEO.

RELATED DOCUMENTATION

SRX320 Services Gateway Acoustic Noise Compliance Statements | **104**

SRX320 Services Gateway EMC Requirements | **104**

SRX320 Services Gateway Acoustic Noise Compliance Statements

The maximum emitted sound pressure level is 70 dB(A) or less per EN ISO 7779.

German Translation:

Maschinenlärminformations-Verordnung - 3. GPSGV, der höchste Schalldruckpegel beträgt 70 dB(A) oder weniger gemäss EN ISO 7779.

RELATED DOCUMENTATION

SRX320 Services Gateway Agency Approvals | 102

SRX320 Services Gateway EMC Requirements | 104

SRX320 Services Gateway EMC Requirements

IN THIS SECTION

Canada

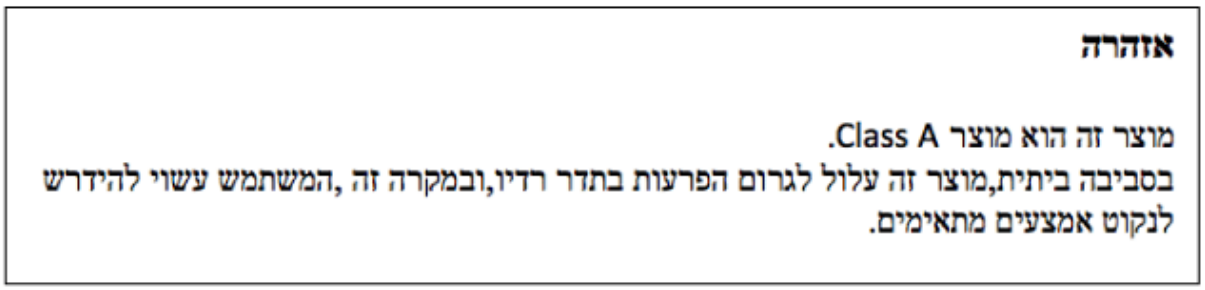
This Class A digital apparatus complies with Canadian ICES-003.

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.

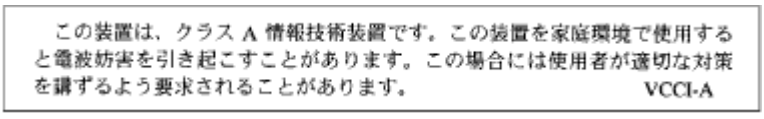
Israel



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 services gateway 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.

RELATED DOCUMENTATION

SRX320 Services Gateway Agency Approvals | **102**

SRX320 Services Gateway Acoustic Noise Compliance Statements | **104**