Extreme®

Connect Beyond the Network

PV-FC-180 Application Sensor

Hardware Installation Guide

9034975

Published April 2016

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/documentation/

For information, contact:
Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

About This Guide

This guide provides an overview, installation, troubleshooting, and optional rack mount rail kit installation instructions, and specifications for the Extreme Networks PV-FC-180 Purview application sensor.

Who Should Use This Guide

⚠	ELECTRICAL HAZARD
	Only qualified personnel should install or service this unit.
	RIESGO ELECTRICO
	Nada mas personal capacitado debe de instalar o darle servicio a esta unida.
	ELEKTRISCHER GEFAHRENHINWEIS
	Installationen oder Servicearbeiten sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.
	RISQUES D'ÉLECTROCUTION
	Seul un personnel qualifié doit installer ou effectuer les opérations de maintenance sur cet élément.

This guide is intended for a network administrator who is responsible for installing and setting up the PV-FC-180 application sensor.

How to Use this Guide

Read through this guide completely to familiarize yourself with its contents and to gain an understanding of the features and capabilities of the PV-FC-180 application sensor. A general working knowledge of data communications networks is helpful when setting up the PV-FC-180 application sensor.

This preface provides the following:

- An overview of this guide
- A brief summary of each chapter
- Definitions of the conventions used in this document
- Instructions regarding how to obtain technical support from Extreme Networks.

To locate information about various subjects in this guide, refer to the following table.

For...	Refer to...
An overview of the PV-FC-180 application sensor and its features.	Introduction on page 9
Instructions for installing the PV-FC-180 application sensor hardware and connecting the PV-FC-180 application sensor to the network.	Installation on page 11

For...	Refer to...
Information on port, system, and power supply LEDs; how to replace PV-FC-180 fan modules and power supply; and how to restart or shut down the PV-FC-180 application sensor using the OFFLINE/RESET button.	Troubleshooting on page 36
Specifications, environmental requirements, and physical properties of the PV-FC-180 application sensor.	Specifications on page 45
Details on how to clear either the persistent storage or the system password as troubleshooting tools.	Clearing the Persistent Storage or System Password on page 47
Details on how to install the optional rack mount kit.	Optional Rack Mount Rail Kit Installation on page 52
Details on how to install the optional wall mounting bracket.	Installing the SSA-WALL-MOUNT Kit on page 69
Details environmental guidelines such as operating temperature, air flow, inlet temperature, and dust mitigation and prevention.	Environmental Guidelines on page 79
Regulatory compliance information, including disposal, safety, and the Firmware License Agreement.	Regulatory Compliance Information on page 86

Related Documents

The *S-, K-, and 7100 Series Configuration Guide* and *S-, K-, and 7100 Series CLI Reference Guide* provide information on how to use the CLI to set up and manage the PV-FC-180 application sensor.

These manuals can be obtained in PDF format at: http://documentation.extremenetworks.com

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
👉	General Notice	Helpful tips and notices for using the product.
📝	Note	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚡	Warning	Risk of severe personal injury.
New	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Related Publications

Extreme Control Center® Documentation

Extreme Control Center (ECC, formerly NetSight) documentation, including release notes, are available at: https://extranet.extremenetworks.com/. You must have a valid customer account to access this site.

Extreme Control Center online help is available from the **Help** menu in all ECC software applications. The online help provides detailed explanations of how to configure and manage your network using ECC software applications.

For complete regulatory compliance and safety information, refer to the document *Intel® Server Products Product Safety and Regulatory Compliance*.

Other Documentation

- *ExtremeXOS Command Reference Guide*
- *ExtremeXOS Release Notes*
- *ExtremeXOS User Guide*

Getting Help

If you require assistance, you can contact Extreme Networks using one of the following methods:

- Global Technical Assistance Center (GTAC) for Immediate Support
  - Phone: 1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.

- The Hub — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Network products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related Return Material Authorization (RMA) numbers

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com.

1 Introduction

This chapter provides an overview of the capabilities of the PV-FC-180 application sensor.

For information about firmware features of the PV-FC-180 application sensor and how to configure them, refer to the *S-, K-, and 7100 Series Configuration Guide*.

The PV-FC-180 application sensor has four 10GBASE-X SFP+ ports, as shown in the figure below.

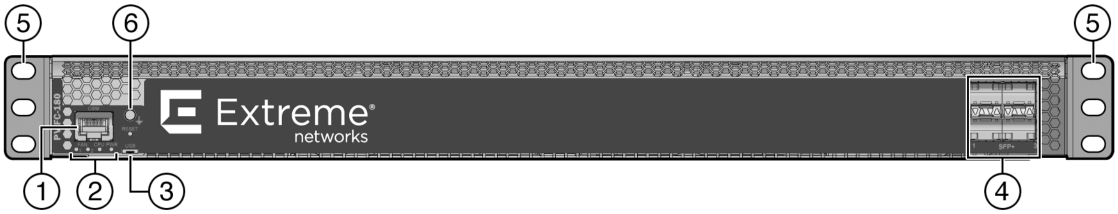


Figure 1: PV-FC-180 I/O Port Panel

1	COM port	4	10GBASE-X SFP+ ports
	System LEDs	5	Mounting ears
	Micro-USB port	6	Ground receptacle

The SFP+ ports support a number of pluggable transceivers. For more information about the transceivers, see the following: http://learn.extremenetworks.com/rs/extreme/images/Pluggable-Transceivers-DS.pdf

AC Power Supplies

Two 460 watt AC power supply models, which you must order separately, are available for the PV-FC-180 application sensor:

- SSA-FB-AC-PS-A—I/O port side air exhaust
- SSA-FB-AC-PS-B—I/O port side air intake

Each power supply option contains a single non-reversible fan. The two power supply options are differentiated by the direction of the power supply fan air flow. Power supply air flow must agree with the air flow direction of the installed fan modules.

The PV-FC-180 AC power supplies automatically adjust to the input voltage and frequency, which allows for an input voltage of 100 to 240 Vac, and a frequency between 50 and 60 Hz. See the operating specifications in Specifications on page 45. No additional adjustments are necessary. For installations in North America, a 15 Amp power cord is required. See Powering Up the PV-FC-180 Application Sensor on page 27 for more details.

You can install up to two power supplies in the rear of the PV-FC-180 chassis. All the power supply needs of the PV-FC-180 application sensor can be met by installing a single power supply. If you choose to use two power supplies, system power redundancy is guaranteed if one supply is lost. Power supplies are hot swappable in redundant power supply mode.

For more information, see Installing the Power Supplies on page 25. For information on the power supply LED, see Power Supply LED on page 39.

Fans

The PV-FC-180 appliance comes with two installed fan modules to cool the system. The direction of the fan module air flow is reversible. By default, air flows from the I/O port side to the power supply side of the unit. If your PV-FC-180 configuration requires power supply side to I/O port side air flow, see Reversing the Fan Module Air Flow on page 15 for details about how to reverse the fan module air flow.

The PV-FC-180 fan modules are both field replaceable and hot swappable. For information on how to replace PV-FC-180 fan modules, see Replacing the Fan Module on page 41.

Micro-USB Port

The micro-USB port is provided for local file transfer.

Management

You can manage the PV-FC-180 either in-band or out-of-band. In-band remote management is possible using the Extreme Networks Extreme Control Center® management application or the command line interface (CLI) via Telnet. Out-of-band management is provided through the RJ45 COM (Communication) port on the front panel using a PC, a VT terminal, or a VT terminal emulator. For more information, see Connecting to the Network on page 29.

2 Installation

⚠	ELECTRICAL HAZARD
	Only qualified personnel should install or service this unit.
	RIESGO ELECTRICO
	Nada mas personal capacitado debe de instalar o darle servicio a esta unida.
	ELEKTRISCHER GEFAHRENHINWEIS
	Installationen oder Servicearbeiten sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.
	RISQUES D'ÉLECTROCUTION
	Seul un personnel qualifié doit installer ou effectuer les opérations de maintenance sur cet élément.

⚠

Warning

To prevent possible injury when installing your Extreme switch product, avoid contacting the edges of I/O ports with your fingers.

ADVERTENCIA

Para evitar posibles lesiones durante la instalación de su producto interruptor Extreme, evite tocar con los dedos los bordes de los puertos de entrada/salida.

WARNHINWEIS

Verletzungsgefahr beim Installieren des Extreme Switch – berühren Sie die Ränder der E/A-Anschlüsse nicht mit den Fingern.

AVERTISSEMENTS

Afin d'éviter toute blessure possible lors de l'installation de votre commutateur Extreme, évitez que vos doigts touchent les rebords des ports d'entrée et de sortie.

Required Tools

- ESD wrist strap (included with the PV-FC-180 application sensor)

- Phillips screwdriver

Installation Site Requirements

You need to have 3–4 inches of clearance on the switch I/O port side of the PV-FC-180 application sensor depending upon the cabling used.

See Environmental Guidelines on page 79 for environmental guidelines relating to the PV-FC-180 application sensor installation.

The installation site must be within reach of the network cabling and meet the requirements listed below:

- Appropriate grounded power receptacles must be located within 7 feet of the site.
- A temperature of between 5°C (41°F) and 40°C (104°F) must be maintained at the installation site with fluctuations of less than 10°C (18°F) per hour.

⚠ Caution
To ensure proper ventilation and prevent overheating, leave a minimum clearance space of 5.1 cm (2.0 in.) at the front and rear of the device.

PRECAUCIÓN
Para asegurar una buena ventilación y evitar que el sistema se sobrecaliente, deje un espacio mínimo de 5.1 cm (2 pulgadas) con respecto el anverso y reverso del aparato.

Unpacking the PV-FC-180 Application Sensor

Unpack the PV-FC-180 application sensor as follows:

1. Open the box and remove the packing material protecting the PV-FC-180 application sensor.

   Save the shipping box and materials in the event the unit must be reshipped.
2. Remove and set aside the RJ45-to-DB9 converter, anti-static wrist strap, adhesive feet (for flat surface placement), and power cord retention clips.

   The PV-FC-180 appliance does not include screws for attaching the PV-FC-180 application sensor to rack posts.
3. Verify the contents of the carton as listed in the the following table.

Table 3: Contents of PV-FC-180 Application Sensor

Item	Quantity
PV-FC-180 chassis	1
RJ45 management cable	1
RJ45-to-DB9 converter	1
Anti-static wrist strap	1
Adhesive rubber feet	4
Power cord retention clips	2
PV-FC-180 Quick Reference	1

4 Inspect the PV-FC-180 application sensor for any signs of physical damage.

If there are any signs of damage, DO NOT install the PV-FC-180 application sensor instead, contact Extreme Networks. Refer to Getting Help on page 7 for details.

Mounting the PV-FC-180 Application Sensor

Note
The PV-FC-180 switch comes with integrated mounting ears that are adequate for most installations. For slide-in mounting, high vibration, or high shock installations, an optional rack mount kit (SSA-FB-MOUNTKIT) is available.

To install the PV-FC-180 application sensor in a rack using the SSA-FB-MOUNTKIT optional rack mount kit, follow the pre-installation discussion here including: Power Supply Air Flow and Switch Fan Module Air Flow on page 14 and Reversing the Fan Module Air Flow on page 15, before proceeding to Optional Rack Mount Rail Kit Installation on page 52.

You can install a PV-FC-180 application sensor on a flat surface or in a rack. For more information about flat surface installation, see Flat Surface Installation on page 24.

There are four possible rack mounting configurations as shown in Figure 2: PV-FC-180 Rack Configurations on page 14, based upon whether:

- The switch I/O ports side or the power supply side of the device face front, or
- The device is mounted flush with the rack posts or mid-mounted.

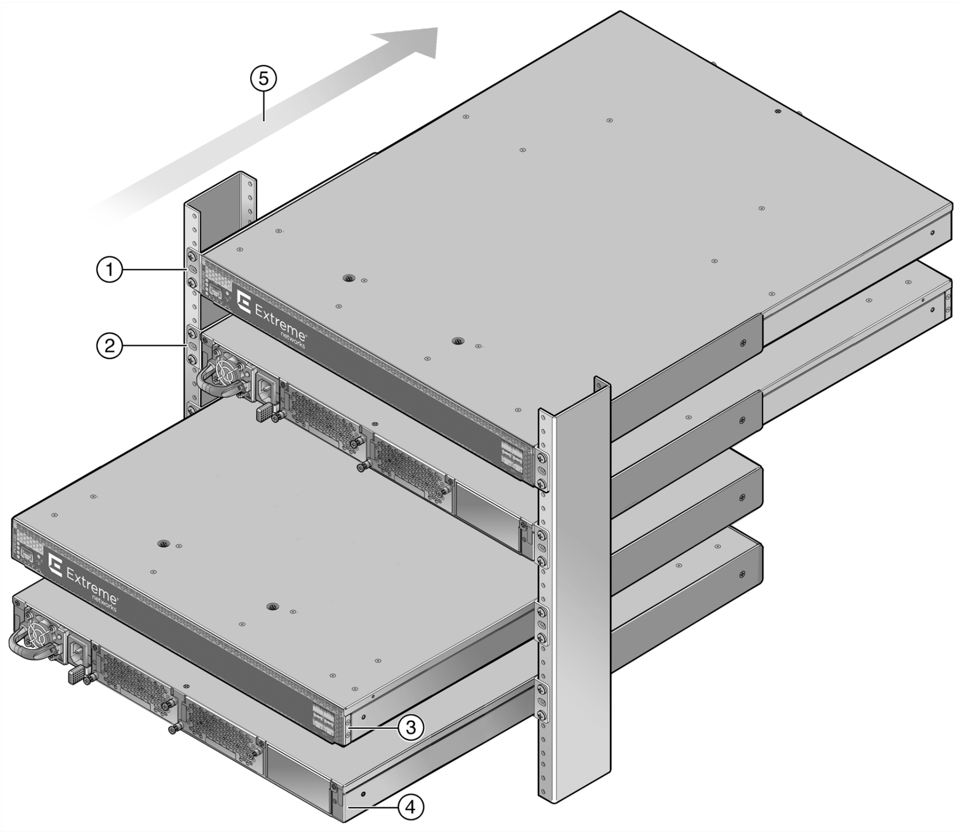


Figure 2: PV-FC-180 Rack Configurations

1	Flush mounted with the switch I/O ports facing front (cool air side)	4	Mid-mounting with the power supply facing front
2	Flush mounted with the power supply facing front (cool air side	5	Air flow direction
3	Mid-mounted with the switch I/O ports facing front		

Power Supply Air Flow and Switch Fan Module Air Flow

The power supply module has its own fan for cooling the power supply, and the two switch fan modules have two fans (each) for cooling the switch circuitry. The air flow direction of all three modules must agree in order to properly cool the installed PV-FC-180 application sensor. In rack mount configurations it is best practice to mount all devices with a common cool air side and a common exhaust (hot air) side.

On the PV-FC-180 application sensor, two air flow directions are supported:

- The I/O port side to the power supply side.

- The power supply side to the I/O port side.

Note
The power suppl(ies) must be ordered separately from the switch unit, and air flow direction must be specified when ordering them. Power supply air flow direction is fixed and cannot be manually changed. If the ordered power supply has an air flow direction that does not work for your rack configuration, you must re-order the power supply that has the correct air flow direction (see Table 5: Power Supply Air Flow Based on Model Number on page 15).

The PV-FC-180 application sensor is shipped from the factory set up for air flow direction from the I/O port side to the power supply side device. If your installation requires that air flow direction be from the power supply side to the I/O port side, you must reverse the air flow of the switch fan module fans (see Reversing the Fan Module Air Flow on page 15). Also, you must reverse the rack mount flanges (ears) (see Rack Mount Ear Positioning on page 17).

You can determine air flow direction of the switch fan modules by visually inspecting them for whether a white label or a fan blade is visible through the fan screen. Before securing the PV-FC-180 application sensor to the rack or installing the power supply into the PV-FC-180 application sensor, perform a visual verification that both power supply module and switch fan module air flow agree with the intended configuration as defined in Table 4: Fan Module Air Flow Direction on page 15 and Table 5: Power Supply Air Flow Based on Model Number on page 15.

Unpack each power supply you ordered for the PV-FC-180 application sensor (see Unpacking the Power Supplies on page 24).

Table 4: Fan Module Air Flow Direction

Air Flow Direction	Visual Indication
From I/O port side to power supply side	White label is visible on fan unit
From power supply side to I/O port side	Fan blade is visible on fan unit

The power supply air flow direction can also be verified based upon the power supply manufacturer's part number located on the power supply bottom label.

Table 5: Power Supply Air Flow Based on Model Number

Model Number	Mfg. Part Number	Air Flow Direction
SSA-FB-AC-PS-A	DS460S-3-003	From power supply side to I/O port side
SSA-FB-AC-PS-B	DS460S-3-002	From I/O port side to power supply side

Reversing the Fan Module Air Flow

Note
If the PV-FC-180 application sensor rack configuration requires the air flow to be from the power supply side to the I/O port side, you must reverse the air flow in the switch fan modules for both switch fan module 1 and switch fan module 2.

Removing the Fan Module

To remove the switch fan module:

1. Unscrew the two fan module captive screws as shown in the figure below.
2. Slide the fan module forward until it is unplugged from the device.

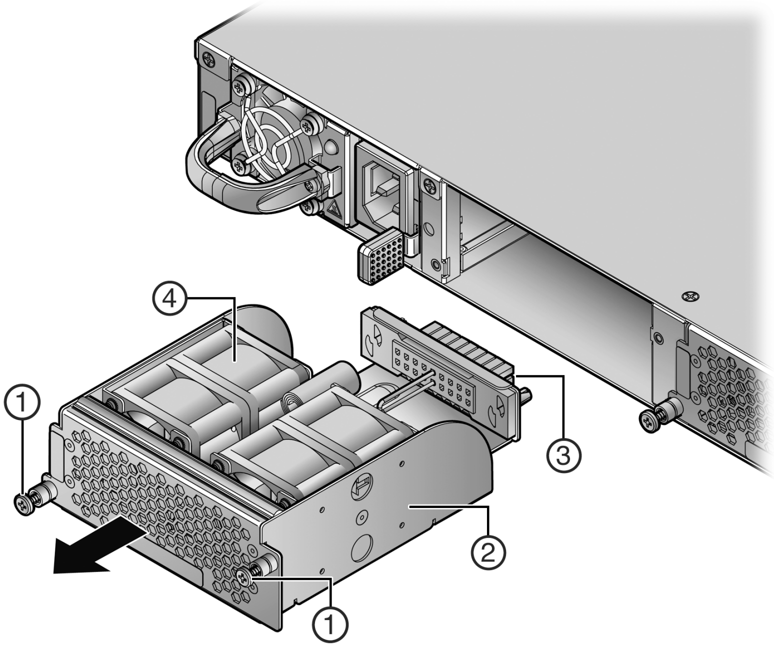


Figure 3: Removing the Fan Module

1	Fan module captive screws	3	Fan module connector
2	Fan module	4	Fan units

Reversing the Fan Unit

The fan module has a single reversible dual fan unit. When the fan unit is properly seated, the air flow indicator arrow is completely visible as shown in callout 1, Figure 4: Reversing the Fan Module Air Flow on page 17. The air flow indicator arrow points in the direction the fan unit flows air through the fan module.

In the I/O port to power supply module (default) air flow configuration, the fan unit is visible (as shown in Figure 3: Removing the Fan Module on page 16, callout 4)

When the fan unit is reversed, a metal plate covers the fan unit (as shown in Figure 4: Reversing the Fan Module Air Flow on page 17). To reverse the fan module air flow:

1. Hold the module in your hand.
2. Apply pressure to the edges of the fan units closer to the fan module connector to rotate the fan unit (thick black arrows in Figure 4: Reversing the Fan Module Air Flow on page 17).

3 Flip the fan unit 180 degrees until the air flow indicator is again completely visible and pointing away the fan module screen, as shown in callout 4, the figure below.

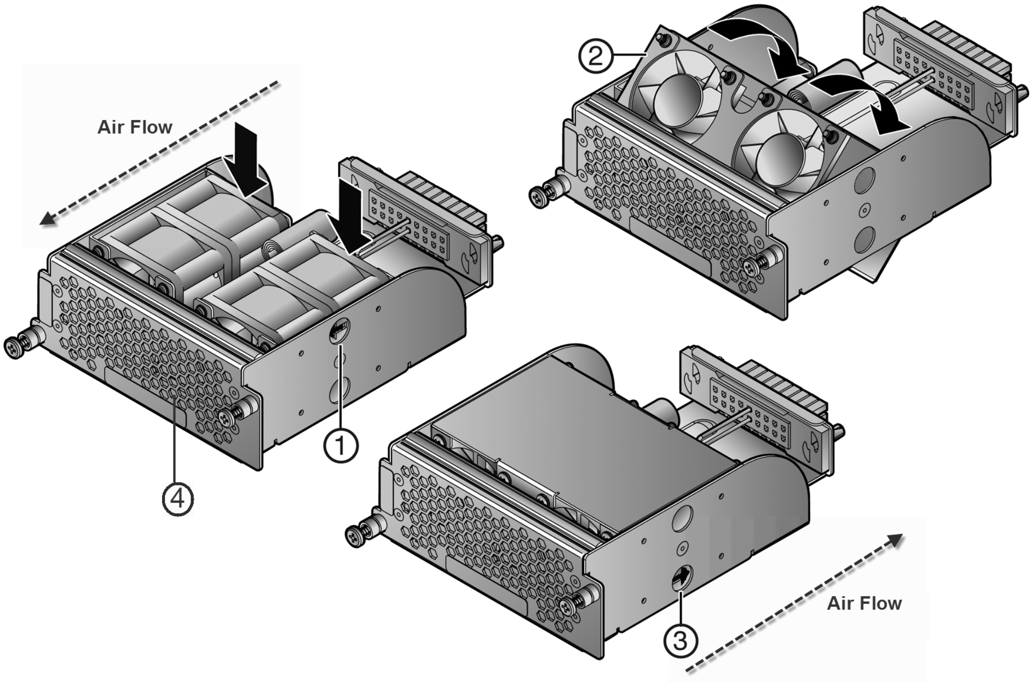


Figure 4: Reversing the Fan Module Air Flow

1	Air flow indicator arrow	3	Air flow indicator arrow
2	Fan unit in mid-reversal	4	Fan screen

Callout 1 shows air flow from the I/O port side to the power supply side of the module.

Callout 3 shows air flow from the power supply side to the I/O port side of the module.

Reinstalling the Fan Module

To reinstall the fan module:

1 Align the fan module with the fan module opening.
2 Insert the module into the fan module opening, applying enough pressure that the fan module is flush with the device.
3 Secure the two fan module captive screws.

Rack Mount Ear Positioning

If you are installing the PV-FC-180 application sensor using the SSA-FB-MOUNTKIT optional rack mount kit, proceed to Optional Rack Mount Rail Kit Installation on page 52.

When shipped from the factory, the PV-FC-180 application sensor has rack mount ears attached to the edge of the side of the appliance containing the I/O ports in a flush mount configuration, as shown in callout 1 of Figure 2: PV-FC-180 Rack Configurations on page 14. If you are mounting the appliance using the factory positioning of the rack mount ears, go to Securing the PV-FC-180 Application Sensor to the Rack on page 22.

You can reposition the rack mount ears for three alternative mounting options:

- Flush-Mount Power Supply Facing Front Configuration on page 18
- Mid-Mount I/O Ports Facing Front Configuration on page 19
- Mid-Mount Power Supply Facing Front Configuration on page 20

Flush-Mount Power Supply Facing Front Configuration

The flush-mount, power supply facing front configuration is depicted in callout 2 of Figure 2: PV-FC-180 Rack Configurations on page 14. This PV-FC-180 application sensor rack mount configuration requires the repositioning of the rack mount ears on both sides of the device.

To reposition the rack mount ears for this configuration:

1. Remove the screw by the three holed ear, as shown in Figure 5: Flush Mount Power Supply Front Configuration on page 19 callout 1, and loosen the opposite screw, shown in callout 2.
2. Pivot the rack mount ear at the loosened screw, shown by callout 3, repositioning the rack mount ear so that the three-holed ear is flush with the switch I/O port side of the device.
3. Reinsert the front screw, shown by callout 4, and retighten the middle screw, shown by callout 5.
4. Repeat steps 1–3 on the other side of the chassis.

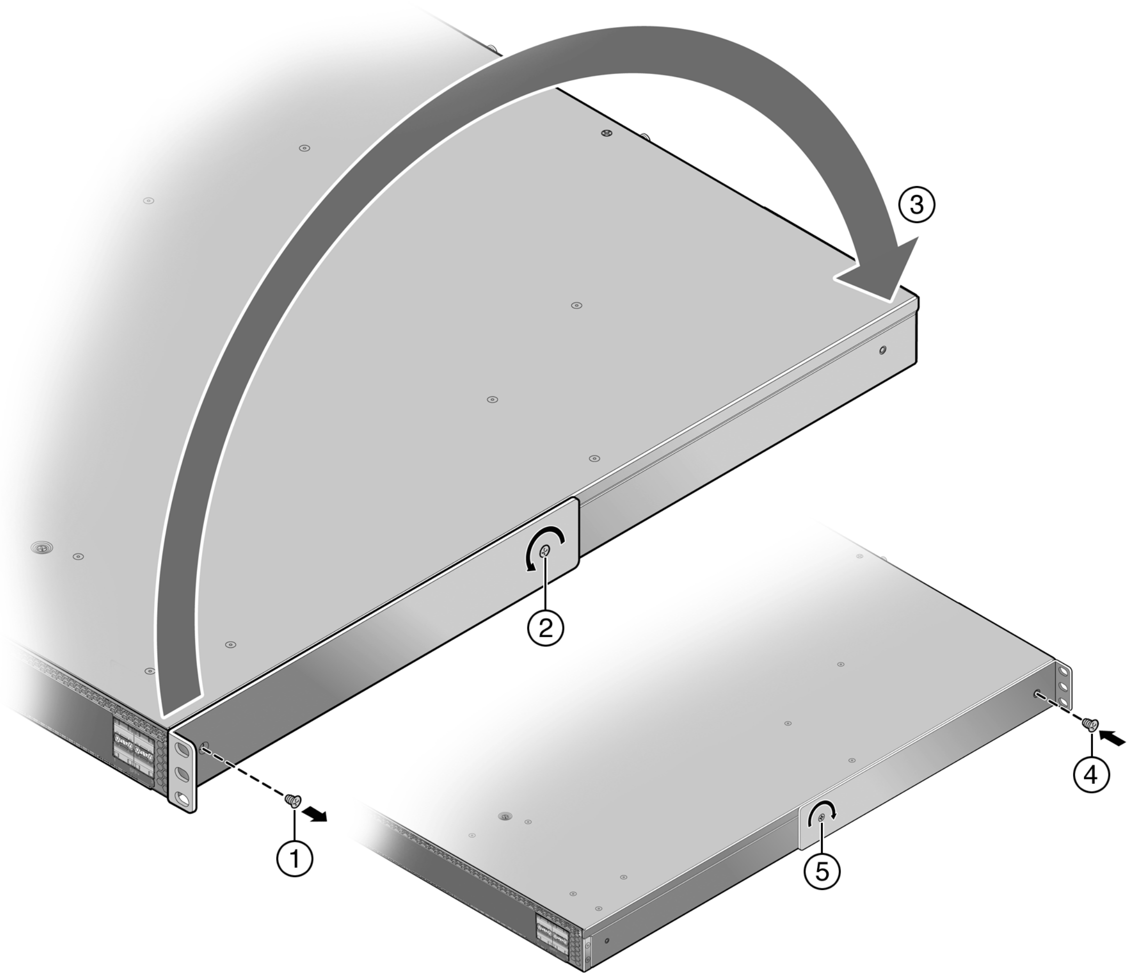


Figure 5: Flush Mount Power Supply Front Configuration

1	Ear mount screw removal	4	Ear mount screw insertion
2	Rack mount ear pivot screw	5	Pivot screw retightened
3	Reposition of rack mount ear		

Mid-Mount I/O Ports Facing Front Configuration

The mid-mount, I/O ports facing front configuration is depicted in callout 3 of Figure 2: PV-FC-180 Rack Configurations on page 14. This rack mount configuration requires repositioning the rack mount ears on both sides of the device.

To reposition the rack mount ears for this configuration:

1. Unscrew the two rack mount ear screws as shown by callout 1 in Figure 6: Mid-Mount I/O Ports Facing Front Configuration on page 20.
2. Reposition the rack mount ear, shown by callout 2, with the middle and power supply side screw holes.

3 Reinsert the two rack mount ear screws, shown by callout 3.
4 Repeat steps 1–3 on the other side of the chassis.

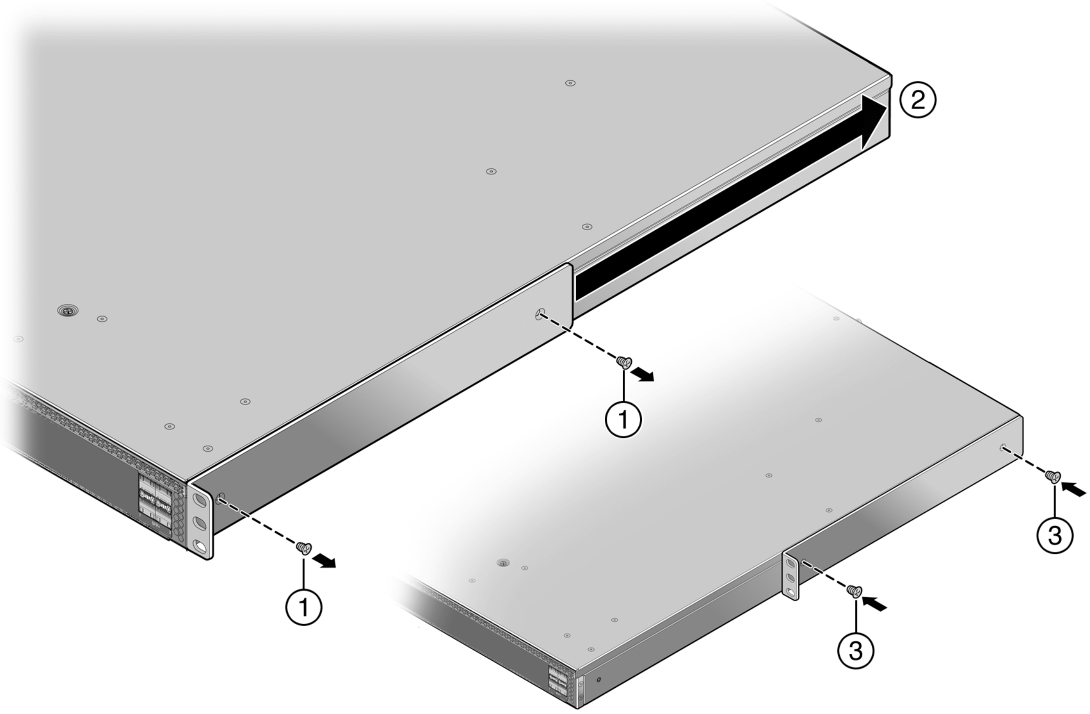


Figure 6: Mid-Mount I/O Ports Facing Front Configuration

1	Ear mount screw removal	3	Ear mount screw insertion
2	Reposition of rack mount ear		

Mid-Mount Power Supply Facing Front Configuration

The mid-mount, power supply facing front configuration is depicted in callout 4 of Figure 2: PV-FC-180 Rack Configurations on page 14. This rack mount configuration requires repositioning the rack mount ears on both sides of the device.

To reposition the rack mount ears for this configuration:

1 Unscrew the two rack mount ear screws as shown by callout 1 in Figure 7: Mid-Mount Power Supply Front Configuration on page 21.
2 Reposition the rack mount ear towards the power supply end of the device, shown by callout 2 and the thick black arrow. The three-holed ear is now located in the middle of the device, facing the power supply side.
3 Reinsert the two rack mount ear screws, shown by callout 3.
4 Repeat steps 1–3 on the other side of the chassis.

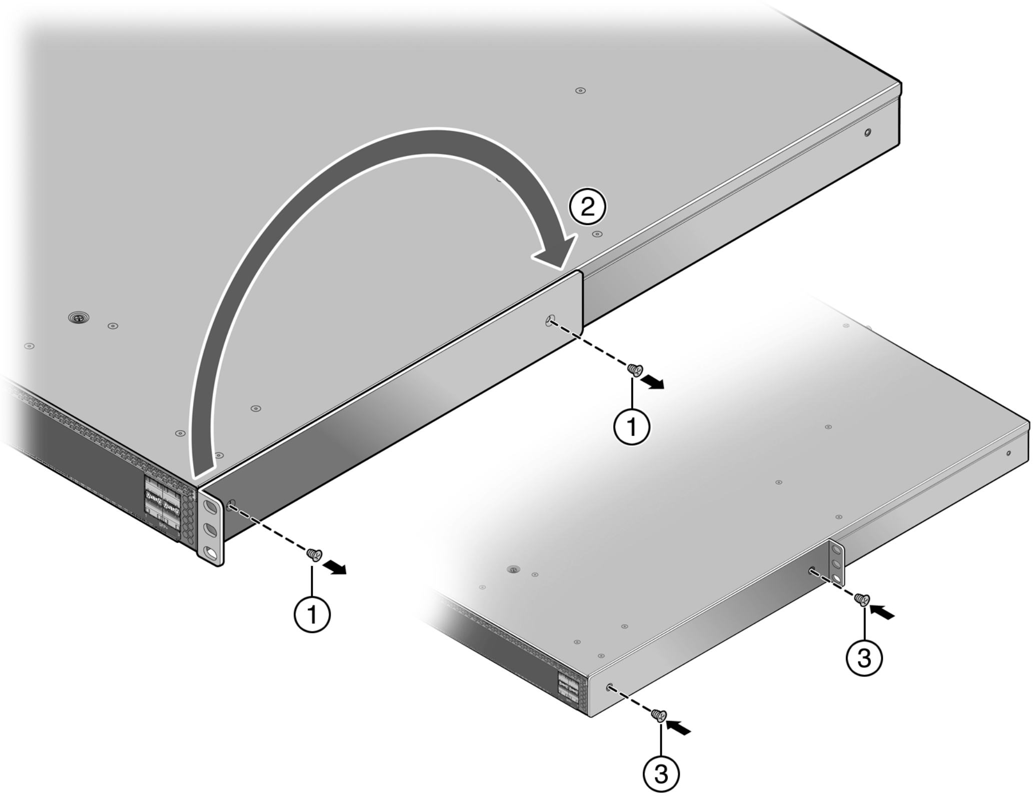


Figure 7: Mid-Mount Power Supply Front Configuration

1	Ear mount screw removal	3	Ear mount screw insertion
2	Reposition of rack mount ear		

Securing the PV-FC-180 Application Sensor to the Rack

Warning

Before rack-mounting the device, ensure that the rack can support it without compromising stability. Otherwise, personal injury and/or equipment damage may result.

ADVERTENCIA

Antes de montar el equipo en el rack, asegurarse que el rack puede soportar su peso sin comprometer su propia estabilidad, de otra forma, daño personal o del equipo puede ocurrir.

WARNHINWEIS

Überzeugen Sie sich vor dem Einbau des Gerätes in das Rack von dessen Stabilität, ansonsten könnten Personenschäden oder Schäden am Gerät die Folge sein.

AVERTISSEMENTS

Avant de monter l'appareil sur le bâti, assurez-vous que l'étagère peut en supporter le poids sans en compromettre la stabilité. Cela pourrait, dans le cas contraire, entraîner des blessures ou des dommages au matériel.

Note

The rack mounting ear provides three holes for securing the PV-FC-180 application sensor to the rack. Use at least two screws or fasteners appropriate to your rack on each side when securing the PV-FC-180 application sensor to the rack.

It is recommended that power supplies be installed after the PV-FC-180 application sensor has been secured to the rack to minimize weight that must be supported when installing rack screws.

To secure the PV-FC-180 application sensor to the rack:

1 Ensure that the rack mount ears are properly installed based upon the discussion in section Rack Mount Ear Positioning on page 17.

2 Align the rack mount ear holes with the front rack post holes in either a flush or mid-mount) configuration.

3 Secure the PV-FC-180 application sensor to each rack post with at least two screws or fasteners appropriate to the rack as shown in callout 1 of the appropriate figure (Figure 8: Securing the PV-

FC-180 Application Sensor to the Rack in a Flush Mount Configuration on page 23 or Figure 9: Securing the PV-FC-180 Application Sensor to the Rack in a Mid-Mount Configuration on page 24).

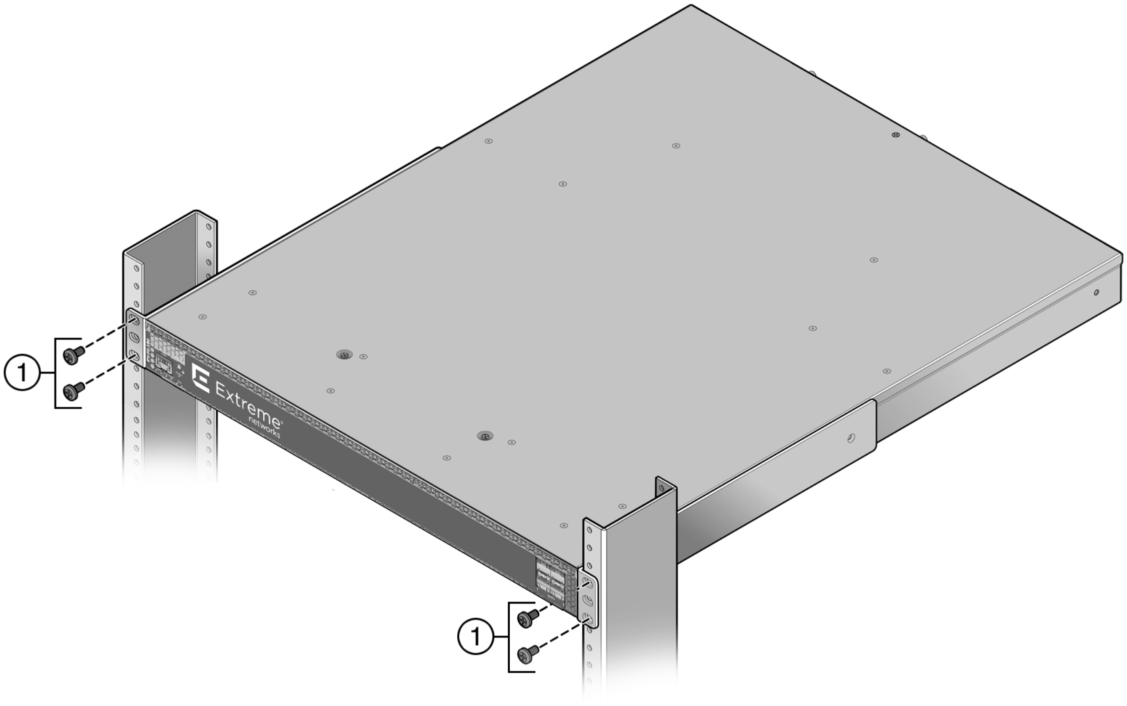


Figure 8: Securing the PV-FC-180 Application Sensor to the Rack in a Flush Mount Configuration

1	4–6 screws or fasteners appropriate to the rack

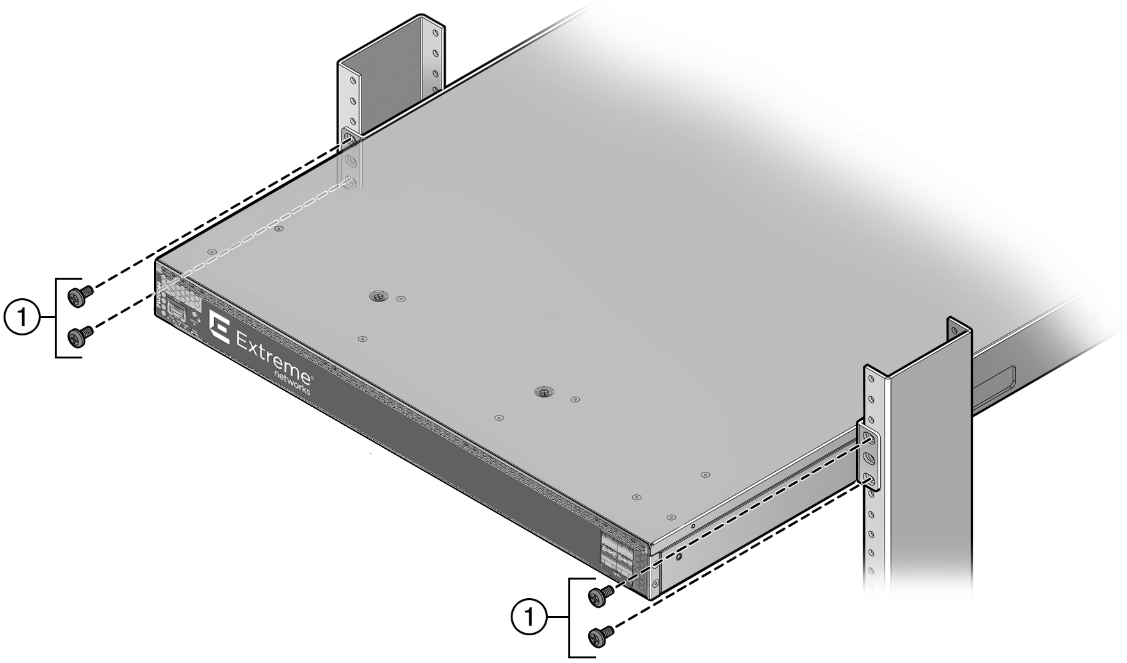


Figure 9: Securing the PV-FC-180 Application Sensor to the Rack in a Mid-Mount Configuration

1	4–6 screws or fasteners appropriate to the rack

You can now install the power supplies. See Installing the Power Supplies on page 25.

Flat Surface Installation

For flat surface installation, optionally attach the adhesive rubber feet to the bottom of the PV-FC-180 application sensor.

To attach the rubber feet to the bottom of the PV-FC-180 application sensor:

1. Place the PV-FC-180 application sensor upside down on a sturdy, flat surface.
2. Remove the adhesive backing from the four rubber feet.
3. Adhere the rubber feet to the round, recessed areas on the bottom of the PV-FC-180 application sensor.

You can now install the power supplies. See Installing the Power Supplies on page 25.

Unpacking the Power Supplies

The SSA-FB-AC-PS-A and SSA-FB-AC-PS-B power supply modules are shipped in boxes separate from the PV-FC-180 application sensor. To unpack a power supply:

1. Remove the power supply from the shipping box and slide the two foam end caps off the unit.

   Save the shipping box and materials in the event the unit must be reshipped.

2 Verify the contents of the box using Table 6: Contents of PV-FC-180 Power Supply Carton on page 25.

3 Remove the power supply from its protective plastic bag.

4 Examine the power supply carefully, checking for damage.

If there are any signs of damage, DO NOT install the power supply; instead, contact Extreme Networks. Refer to Getting Help on page 7 for details.

Table 6: Contents of PV-FC-180 Power Supply Carton

Item	Quantity
Power supply (SSA-FB-AC-PS-A or SSA-FB-AC-PS-B)	1

Note
You must purchase the appropriate power cord separately.

Installing the Power Supplies

If you are installing only one power supply, you must put the power supply in the left power supply bay (labeled PS1). The PV-FC-180 application sensor ships without a coverplate for the PS1 bay.

Note
For proper operation, the PV-FC-180 application sensor must have a power supply in PS1 at all times while the PV-FC-180 application sensor is powered up.

To install the power supplies in the PV-FC-180 application sensor:

1 Use appropriate antistatic protection when handling power supplies.

2 Perform a visual verification of the power supply air flow direction, verifying that the power supply air flow direction agrees with the installed fan module air flow direction. For details, see Power Supply Air Flow and Switch Fan Module Air Flow on page 14.

3 Holding the power supply by the handle and bottom, align the power supply with the left power supply bay (labeled PS1).

4 Slide the power supply forward until it is plugged into the chassis connector and the lock tab clicks to the right. Pull on the power supply handle to ensure that the power supply is firmly in place. See the following figure.

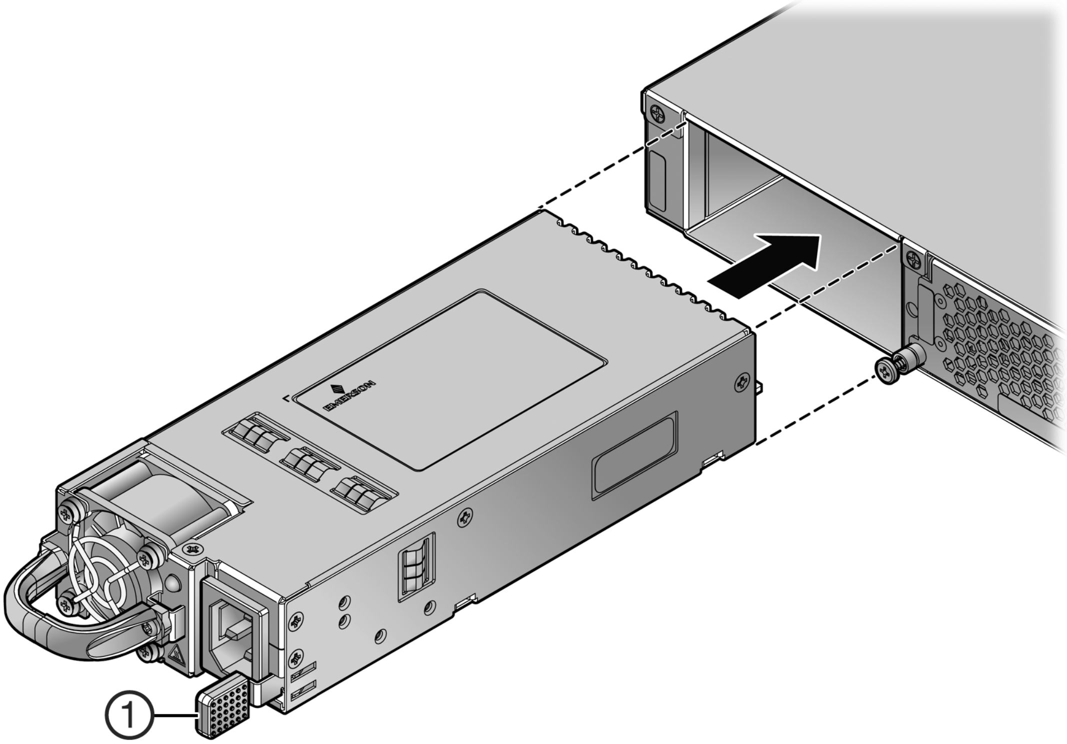


Figure 10: Installing a Power Supply

1	Lock Tab

5 If you are installing a second power supply, remove the coverplate from the right power supply bay by unscrewing the screw that attaches the coverplate to the PV-FC-180 application sensor and

rotating the coverplate out of its position from right to left before disengaging it from the chassis (see the following figure). Reinstall the screw once the cover plate is removed.

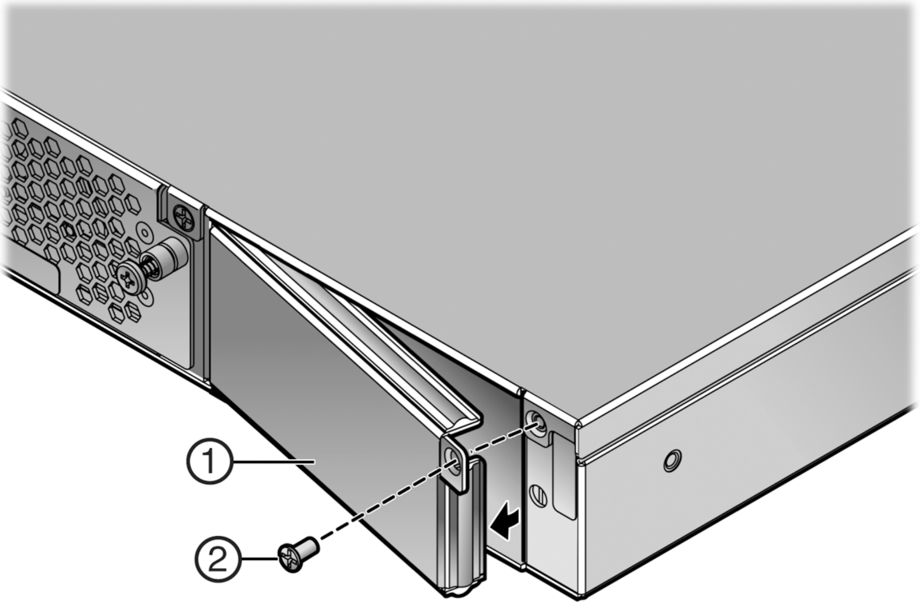


Figure 11: Removing the Power Supply Bay Coverplate

1	Coverplate	2	Coverplate Screw

Keep the coverplate in the event you need to revert to a single power supply configuration. If a power supply is not installed, the coverplate must be in place for proper air flow.

6 Repeat steps 2–3 to install the power supply in the right power supply bay.

Powering Up the PV-FC-180 Application Sensor

To connect the PV-FC-180 application sensor to the power sources:

1 Plug a power cord into each power supply's AC power receptacle.

2 Plug the cord into a dedicated grounded AC outlet.

In the case of a two power supply configuration, to take advantage of redundancy capabilities, plug each power cord into a separate dedicated AC outlet.

The system PWR LED, located on the application sensor I/O port panel, turns ON (green) and the CPU LED turns red until the PV-FC-180 application sensor completes its initialization.

See Figure 15: PV-FC-180 System LEDs on page 37 for the PWR and CPU LED locations. It takes under 30 seconds for the PV-FC-180 application sensor to boot up.

Note
If the power-up sequence is interrupted on the PV-FC-180 application sensor, it may run an extended diagnostics sequence that may take up to two minutes to complete.

When the initialization process is successful, the CPU LED turns green. If the CPU LED does not turn green, refer to Troubleshooting on page 36 for troubleshooting information.

Installing the Power Cord Retention Clip Assembly

The PV-FC-180 application sensor comes with two optional power cord retention clip assemblies. Power cord retention clips provide added security against the inadvertent removal of the power cord from the power supply AC receptacle.

To install the power cord retention clip assembly:

1. Holding the strap piece with the rough side facing away from the power supply, shown by callout 2 of Figure 12: Installing the Power Cord Clip Assembly in the Power Supply on page 28, insert the strap piece into the hole to the right of the power cord receptacle, shown by callout 1.
2. Slide the power cable clamp, shown by callout 3, onto the strap piece with the tab on the clamp piece facing out.
3. Insert the power cord in the open clamp.
4. Close the clamp piece.

   To open the clamp piece, push down the clamp release tab, shown by callout 4.

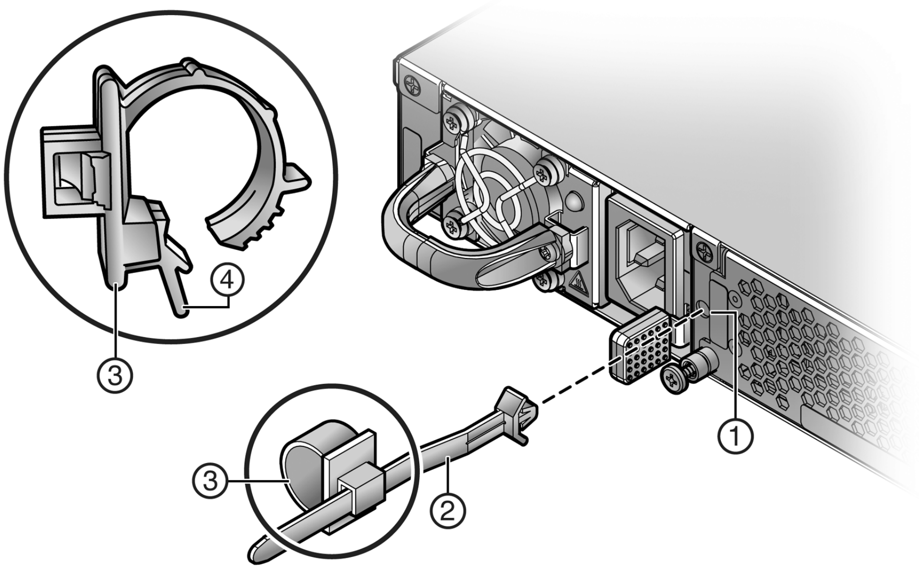


Figure 12: Installing the Power Cord Clip Assembly in the Power Supply

1	Retention clip receptacle	3	Power cable clamp
2	Retention clip strap piece, smooth side facing power supply	4	Clamp release tab

Connecting to the Network

This section provides the procedures for connecting SFP+ pluggable transceivers from the network or other devices to the PV-FC-180 application sensor.

Note
If the PV-FC-180 application sensor is being installed in a network using Link Aggregation, there are rules concerning the network cable and port configurations that must be followed for Link Aggregation to operate properly. Before connecting the cables, refer to the *S-, K-, and 7100 Series Configuration Guide* for configuration information.

Connecting Pluggable Transceivers to the SFP+ Ports

This section describes how to install an SFP+ pluggable transceiver in appropriate PV-FC-180 application sensor ports. See Figure 1: PV-FC-180 I/O Port Panel on page 9 for the location of the pluggable transceiver ports.

For a list of supported SFP+ pluggable transceivers and their specifications, refer to the *S-Series firmware Release Notes* (www.extremenetworks.com/support/release-notes) for the latest compatibility matrix for pluggable transceivers. You can also refer to the datasheet located at the following URL: http://learn.extremenetworks.com/rs/extreme/images/Pluggable-Transceivers-DS.pdf

Warning

Fiber-optic pluggable transceivers use Class 1 lasers. Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, power must be removed from the network adapter.

ADVERTENCIA

Los transmisores receptores de fibra óptica SFP+ conectables utilizan sistemas de láser clase 1. No emplee instrumentos ópticos para ver la salida del láser. Hacerlo podría incrementar el riesgo de daño en los ojos. Cuando se revise el puerto óptico de salida, deberá cortarse la energía del adaptador de red.

WARNHINWEIS

Faseroptische, steckbare Transceiver der Typen SFP+ verwenden Laser der Klasse 1. Zur Ansicht der Laserausgabe dürfen keine optischen Geräte verwendet werden, da hierdurch die Wahrscheinlichkeit einer Gefährdung der Augen erhöht wird. Vor der Inspektion des optischen Ausgangsanschlusses muss das Stromkabel des Netzwerkadapters herausgezogen werden.

AVERTISSEMENTS

Les émetteurs-récepteurs en fibre optique enfichables ne fonctionnent qu'avec des lasers de classe 1. N'utilisez aucun instrument d'optique pour observer la sortie du laser. L'utilisation d'instruments d'optique augmente les risques de blessure aux yeux. L'alimentation de l'adaptateur de réseau doit être coupée lorsque vous inspectez le port optique de sortie.

Caution

Carefully follow the instructions in this manual to avoid damaging the pluggable transceivers and PV-FC-180 chassis.

The pluggable transceivers and PV-FC-180 chassis are sensitive to static discharges. Use an antistatic wrist strap and observe all static precautions during this procedure. Failure to do so could result in damage to the SFP+ and PV-FC-180. Always leave the SFP+ in the antistatic bag or an equivalent antistatic container when not installed.

PRECAUCIÓN

Siga las instrucciones del manual para no dañar el SFP+ ni el PV-FC-180, puesto que son muy sensible a las descargas de electricidad estática.

Utilice la pulsera antiestática y tome todas las precauciones necesarias durante este procedimiento. Si no lo hace, podría dañar el SFP+ o el PV-FC-180. Mientras no esté instalado, mantenga el SFP+ en su bolsa antiestática o en cualquier otro recipiente antiestático.

Preparation

Before installing the pluggable transceiver, proceed as follows:

1 Put on the ESD wrist strap, shipped with the application sensor, and attach it to the ground receptacle on the switch I/O port side of the PV-FC-180 application sensor before removing the pluggable transceiver from the anti-static packaging. Refer to the instructions in the anti-static wrist strap package. See the figure below for the location of the ground receptacle.

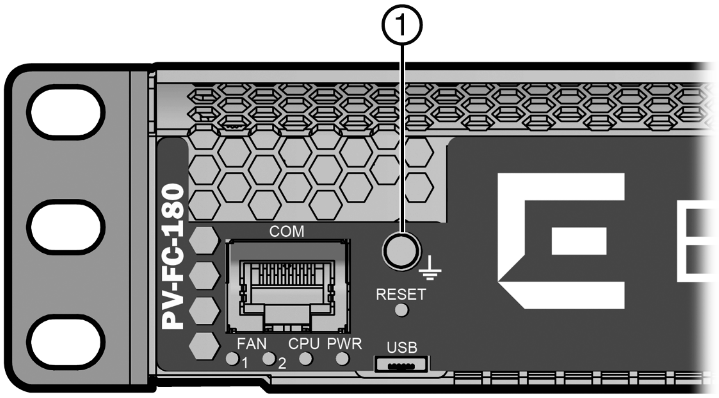


Figure 13: PV-FC-180 Application Sensor Ground Receptacle

1	Ground receptacle

2 Remove the pluggable transceiver from the packaging.

3 If there is a protective dust cover on the pluggable transceiver, do not remove it at this time.

Installing the Pluggable Transceiver

To install an SFP+ pluggable transceiver in the PV-FC-180 application sensor:

1 Hold the pluggable transceiver so that the connector will seat properly.

2 Carefully align the pluggable transceiver with the port.

3 Push the pluggable transceiver into the port until the pluggable transceiver clicks and locks into place.

Removing the Pluggable Transceiver

To remove a pluggable transceiver from a port:

Caution

Do NOT remove an SFP+ pluggable transceiver from a slot without releasing the locking tab located under the front bottom end of the SFP+. This can damage the SFP+.

The SFP+ and PV-FC-180 are sensitive to static discharges. Use an antistatic wrist strap and observe all static precautions during this procedure. Failure to do so could result in damage to the SFP+ and PV-FC-180. Always leave the SFP+ in the antistatic bag or an equivalent antistatic container when not installed.

PRECAUCIÓN

NO quite el SFP+ de la ranura sin antes abrir la traba ubicada en la parte frontal del el SFP+.

Utilice la pulsera antiestática y tome todas las precauciones necesarias durante este procedimiento. Si no lo hace, podría dañar el SFP+ o el PV-FC-180. Mientras no esté instalado, mantenga el SFP+ en su bolsa antiestática o en cualquier otro recipiente antiestático.

1 Put on the ESD wrist strap and attach it to the ground receptacle on the I/O port side of the PV-FC-180 application sensor before removing the pluggable transceiver. Refer to the instructions in the anti-static wrist strap package. See Figure 10: Installing a Power Supply on page 26 for the location of the ground receptacle.

2 Remove the cables connected to the pluggable transceiver.
3 Release the pluggable transceiver from the port.
4 Grasp the sides of the pluggable transceiver and pull it straight out of the port.

If storing or shipping the pluggable transceiver, insert its dust protector to protect its fiber-optic ports.

Connecting to the COM Port for Local Management

This section describes how to install a UTP cable with RJ45 connectors and adapters to connect a PC or VT series terminal to an PV-FC-180 application sensor to access Local Management. This section also details adapter pinout assignments.

What Is Needed

The following is a list of the parts that may be needed depending on the connection:

- UTP cable with RJ45 connectors (supplied with the PV-FC-180 application sensor)
- RJ45-to-DB9 female adapter (supplied with the PV-FC-180 application sensor)
- RJ45-to-DB25 female adapter (customer-supplied)

Using the UTP cable with RJ45 connectors and RJ45-to-DB9 adapter, you can connect from the PV-FC-180 RJ45 COM port to a PC running a VT series emulation software package.

Using the UTP cable with RJ45 connectors and an optional RJ45-to-DB25 female adapter, you can connect from the PV-FC-180 RJ45 COM port to a VT series terminal or VT type terminals running emulation programs for the VT series.

Connecting to a PC or Laptop

To connect a PC or laptop running the VT terminal emulation to the PV-FC-180 COM port:

1 Connect the RJ45 connector at one end of the cable to the COM port on the PV-FC-180 application sensor.
2 Plug the RJ45 connector at the other end of the cable into an RJ45-to-DB9 adapter.
3 Connect the RJ45-to-DB9 adapter to the communications port on the PC.
4 Configure the VT emulation package on your PC or laptop as follows:

Parameter	Setting
Mode	7 Bit Control
Transmit	Transmit = 57600
Bits Parity	8 Bits, No Parity
Stop Bit	1 Stop Bit

When these parameters are set, the Local Management password screen will display. Refer to Completing the Installation on page 34 for further information.

Connecting to a VT Series Terminal

To connect a VT Series terminal to the PV-FC-180 COM port, use a UTP cable with RJ45 connectors and an optional RJ45-to-DB25 female adapter.

1 Connect the RJ45 connector at one end of the cable to the COM port on the PV-FC-180 application sensor.
2 Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB25 female adapter.
3 Connect the RJ45-to-DB25 adapter to the port labeled COMM on the VT terminal.
4 Turn on the VT terminal and access the Setup Directory.
5 Set the following parameters:

Parameter	Setting
Mode	7 Bit Control
Transmit	Transmit = 57600
Bits Parity	8 Bits, No Parity
Stop Bit	1 Stop Bit

When these parameters are set, the Local Management password screen will display. Refer to Completing the Installation on page 34 for further information.

Adapter Wiring and Signal Assignments

Table 7: COM Port Adapter Wiring and Signal Diagram

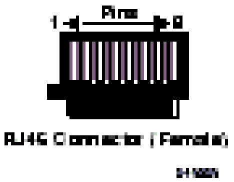
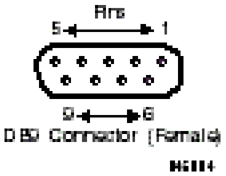
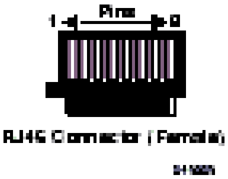
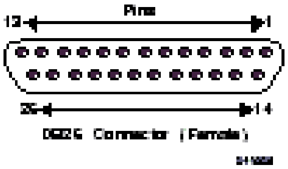
RJ45		DB9	
Pin	Conductor	Pin	Signal
1	Blue	2	Receive (RX)
4	Red	3	Transmit (TX)
5	Green	5	Ground (GRD)
2	Orange	7	Request to Send (RTS)
6	Yellow	8	Clear to Send (CTS)
			

Table 8: VT Series Port Adapter Wiring and Signal Diagram

RJ45		DB25	
Pin	Conductor	Pin	Signal
4	Red	2	Transmit (TX)

Table 8: VT Series Port Adapter Wiring and Signal Diagram (continued)

RJ45		DB25	
1	Blue	3	Receive (RX)
6	Yellow	5	Clear to Send (CTS)
5	Green	7	Ground (GRD)
2	Orange	20	Data Terminal Ready
			

Completing the Installation

After installing the PV-FC-180 application sensor and making the connections to the network, access the device management startup screen from your PC or terminal connection as described below.

Note

This procedure applies only to initial log-in and to logging in to a device not yet configured with administratively-supplied user and password settings.

By default, the PV-FC-180 application sensor is configured with three user login accounts: 'ro' for Read-Only access; 'rw' for Read-Write access; and 'admin' for super-user access to all modifiable parameters. The default password is blank (null). For information on changing these default passwords, refer to the *S-, K-, and 7100 Series Configuration Guide*.

Start the Command Line Interface (CLI) from the device's local console port as follows:

1 Connect a terminal to the local console port as described in Connecting to the COM Port for Local Management on page 32. The startup screen displays.

```
login: admin
Password:

PURVIEW FLOW COLLECTOR
Command Line Interface

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134
Phone: +1 408 579-2800
E-mail: support@extremenetworks.com
WWW: http://www.extremenetworks.com(

c) Copyright Extreme Networks, Inc. 2014

Chassis Serial Number: xxxxxxxxxxxx
Chassis Firmware Revision: xx.xx.xx.xxxx

User admin last logged in WED OCT 08 16:12:42 2014
```

```
There have been 0 failed login attempts since then

PV-FC(su)->
```

2. At the login prompt, enter one of the following default user names:
   - `ro` for Read-Only access
   - `rw` for Read-Write access
   - `admin` for Super User access. (This access level allows Read-Write access to all modifiable parameters, including user accounts.)
3. Press **[ENTER]**.

   The Password prompt displays.
4. Leave the password string blank and press **[ENTER]**.

   The device information and PV-FC-180 application sensor prompt appear as shown above.

The PV-FC-180 application sensor is now ready to be configured.

For information about setting the IP address and configuring Telnet settings for remote access to PV-FC-180 application sensor management, refer to the *S-, K-, and 7100 Series Configuration Guide*.

The CLI commands enable you to initially set up and perform more involved management configurations. The *Extreme Networks S-Series Configuration Guide* is available online at: http://documentation.extremenetworks.com

3 Troubleshooting

LEDs

The PV-FC-180 application sensor has port, system, and power supply LEDs.

Port LEDs

On the PV-FC-180 application sensor, you can view the receive and transmit activity on the RX and TX LEDs for the SFP+ ports. See the following figure.

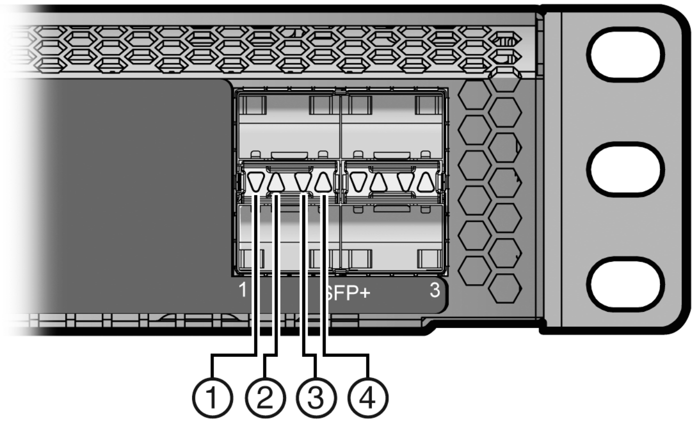


Figure 14: SFP+ Port LEDS

1	RX LED for bottom port	3	TX LED for bottom port
2	RX LED for top port	4	TX LED for top port

The table below describes the LED indications for the RX and TX LEDs for the SFP+ ports and provides recommended actions.

Table 9: Port LEDs

LED	Color	State	Recommended Action
RX (Receive)	None	No link. No activity. Port enabled or disabled.	None.
	Green (solid)	Link present, port enabled, no traffic is being received by the interface.	None.
	Yellow (blinking)	Link present, port enabled, traffic is being received by the interface.	None.
TX (Transmit)	None	Port enabled, but no activity.	If you know the port should be active and is not, contact Extreme Networks Technical Support.
	Green (blinking)	Indicates data transmission activity. Flashing frequency indicates the data rate.	None.
	Yellow (solid)	Fault or error (collision).	None, unless activity is high; in which case, check for network configuration problems or a defective device.

System LEDs

The following figure shows the PV-FC-180 system LEDs. The two left LEDs are separately labeled for fan modules 1 and 2.

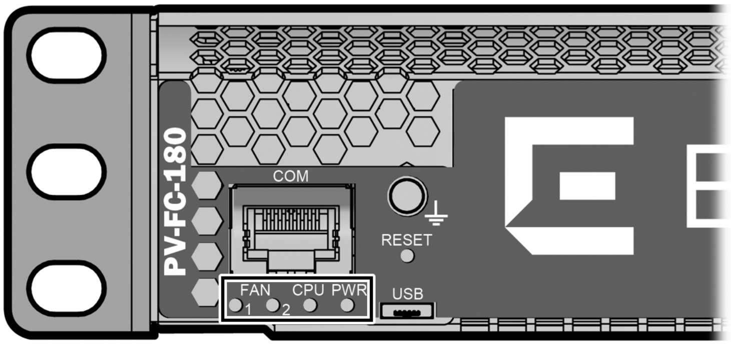


Figure 15: PV-FC-180 System LEDs

The following table describes the LED indications for the system LEDs and provides recommended actions.

Table 10: System LEDs

LED	Color	State	Recommended Action
FAN 1 and 2	Off	Fans are off or booting up.	None.
	Green	All fans are operating normally.	None.

Table 10: System LEDs (continued)

LED	Color	State	Recommended Action
	Amber	One fan has failed.	Replace the failed fan. See Replacing the Fan Module on page 41.
	Red	One or more of the following conditions has occurred: • Temperature is out of range. • The fan controller has failed. • Both fans have failed.	Use the show system CLI command to check the exact condition of the fans. If fans have failed, replace the fan module. See Replacing the Fan Module on page 41.
CPU	Off	Power off.	Ensure chassis has adequate power.
	Amber	Blinking. Device in bootup process.	None.
		Solid. Testing.	If the LED remains amber for several minutes, contact Extreme Networks for technical support.
	Green	Blinking. Image starts running.	None.
		Solid. Functional.	None.
	Red	Solid. Processor in reset.	None.
	Green and Amber	Blinking. Indicates that the PV-FC-180 application sensor is in the process of shutting down.	None. This state is activated when the RESET button is pressed for less than one second to start an orderly shutdown.
	Amber and off	Alternating (67% on, 33% off). Indicates a shutdown is complete. The indication will hold for 60 seconds then automatically restart.	While in this state, you have 60 seconds before the PV-FC-180 application sensor will reboot.
	Blue	Blinking. Virtual Switch Bonding is enabled, but the devices are not bonded	None.
		Solid. Virtual Switch Bonding is enabled, and the devices are bonded.	None.
PWR	Off	The PV-FC-180 application sensor is not receiving power from the power supplies.	Ensure the power cords are plugged in and power is available at the source. Contact Extreme Networks for technical support.

Table 10: System LEDs (continued)

LED	Color	State	Recommended Action
	Green	Functional. Indicates one of the following conditions: • A single power supply is present and operating normally. • Two power supplies are present and operating normally.	None.
	Amber	One of the following conditions has occurred: • Two power supplies are present but only one is operating normally while the other is not connected. • Two power supplies are present but only one is operating normally while the other indicates a fault. • Both power supplies are faulty but the PV-FC-180 application sensor is still receiving power. • Power supplies are operating in additive (non-redundant) mode. • Other internal fault.	Ensure the power cords are plugged in and power is available at the source. Contact Extreme Networks for technical support.

Note

The PWR LED status indication is based on power supplies being powered on.

The following table describes the CPU LED when the PV-FC-180 application sensor is in a virtual switch bonding configuration.

Table 11: CPU LED in Virtual Switch Bonding (VSB) Configuration

Color	State
Green and Blue	Blinking. Image has started and found chassis bonding enabled.
Blue	Solid. Functional (binding is operational and ready to switch)
Blue	Blinking. Binding is not functional (non-operational).

Power Supply LED

The SSA-FB-AC-PS-A and SSA-FB-AC-PS-B power supplies have a single LED. The following table describes the different states of the power supply LEDs.

Table 12: Power Supply LED Status Definitions

LED Color	Status
Green	Sufficient power is available to the system.
Off	No AC power to the power supply or power supply malfunctioning.

Troubleshooting Checklist

If the PV-FC-180 application sensor is not working properly, refer to the following table for a checklist of problems, possible causes, and recommended actions to resolve the problem.

Table 13: Troubleshooting Checklist

Problem	Possible Cause	Recommended Action
All LEDs are OFF.	Loss of power.	Ensure the PV-FC-180 application sensor was installed properly accord installation instructions in Installation on page 11, and that the chassis h
No Local Management Password screen.	Incorrect terminal setup.	Refer to the *S-, K-, and 7100 Series Configuration Guide* for proper setu
	Improper console cable pinouts.	Refer to Specifications on page 45 for proper COM port pinouts.
	Corrupt firmware image or hardware fault.	If possible, attempt to download the image to the PV-FC-180 applicatio Refer to Clearing the Persistent Storage or System Password on page 4 to clear NVRAM.
Cannot navigate beyond Password screen.	Improper username/ password combination entered.	If the username/password combination has been forgotten, refer to Cle Storage or System Password on page 47 for instructions on how to clea resetting it to the default value of null (blank), using either the boot loa command or set mode switch method.
Cannot contact the PV-FC-180 application sensor through in-band management.	IP address not assigned.	See the *S-, K-, and 7100 Series Configuration Guide* for instructions to a
	Port is disabled.	Enable port. See the *S-, K-, and 7100 Series Configuration Guide* for ins disable ports.
	Host Port policy and/or management VLAN is incorrectly configured, or not configured.	Verify that a management VLAN exists and that it is associated with th Refer to the *S-, K-, and 7100 Series Configuration Guide* for information and management VLAN configuration.
	No link to device.	Verify that all network connections between the network management FC-180 application sensor are valid and operating. If the problem continues, contact Extreme Networks for technical supp
Port goes into standby for no apparent reason.	Loop condition detected.	Verify that Spanning Tree is enabled. Refer to the *S-, K-, and 7100 Serie Guide* for the instructions to set the type of STP. Review the network design and delete loops. If the problem continues, contact Extreme Networks for technical supp
User parameters (IP address, device and device name, etc.) were lost when the IdentiFi Wireless power was cycled or the OFFLINE/ RESET button was pressed.	Position of Mode switch (7), Persistent Data Reset, was changed sometime before either cycling power or pressing the RESET button, causing the user-entered parameters to reset to factory default settings. Clear Persistent Data that was set through Local Management.	Reenter the lost parameters as necessary. Refer to the *S-, K-, and 7100 Configuration Guide* for the instructions to configure the device. If the problem persists, contact Extreme Networks for technical suppor

Replacing the Fan Module

The PV-FC-180 application sensor is cooled by two fan modules accessible from the power supply side of the unit. If the FAN LED and the output of the CLI show system command indicate that a fan module has failed, you must replace the failed fan module.

Note
Fan modules are hot-swappable. Do not uninstall a failed fan module until its replacement is available. All PV-FC-180 application sensor components and cover plates must be installed to ensure proper air flow.

The replacement fan kit, SSA-FB-FAN, which you must order separately, contains one replacement fan.

To replace the failed fan module:

1. Determine the location of the failed module using the label shown in Figure 16: Removing the Fan Module on page 42.
2. Unscrew the two captive screws of the failed fan module as shown in Figure 16: Removing the Fan Module on page 42.
3. Following the discussion in Power Supply Air Flow and Switch Fan Module Air Flow on page 14, ensure that the new fan module air flow direction agrees with the installed PV-FC-180 application sensor configuration.
4. If a non-default air flow is required, see Reversing the Fan Module Air Flow on page 15 for directions on how to reverse the fan unit direction.

5 Once you have ensured that the fan module air flow is appropriate to your system configuration, slide the currently installed fan module forward until it is unplugged from the device as shown below.

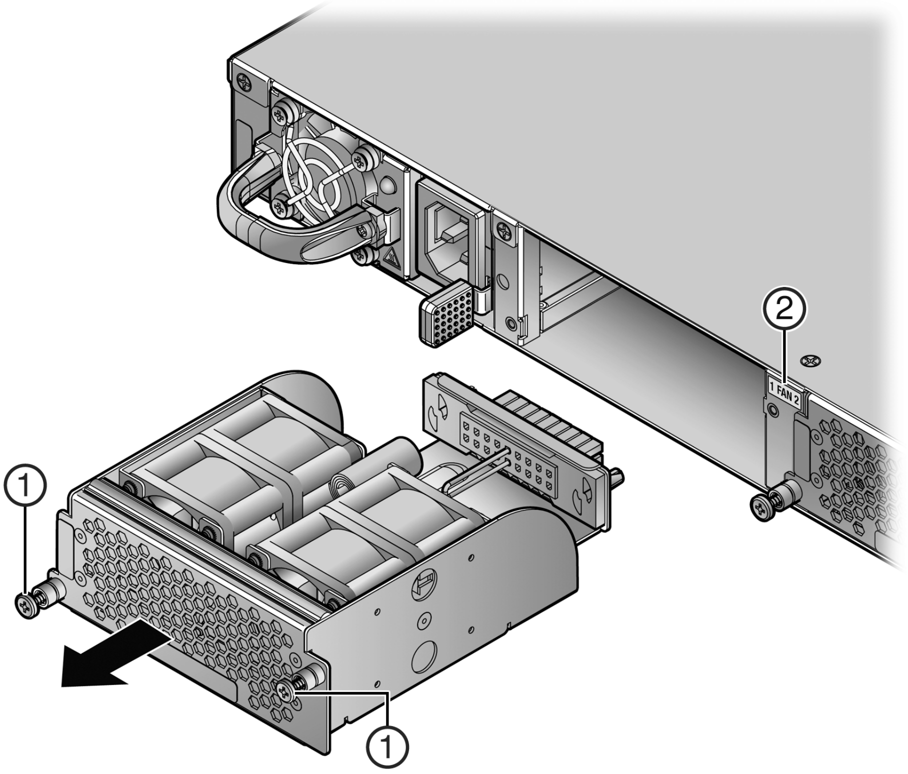


Figure 16: Removing the Fan Module

1	Fan module screws	2	Fan module location label

6 Align the new fan module with the fan module opening.

7 Insert the module into the fan module opening, applying enough pressure that the fan module is flush with the device.

8 Secure the two fan module captive screws.

Removing a Power Supply

To remove a power supply from the PV-FC-180 application sensor:

1 Use appropriate antistatic protection when handling power supplies.

2 If a power cord retention clip is securing the power cord, push down on the retention clip clamp tab to open the clamp and disengage the power cord from the clamp.

3 Unplug the associated power cord from the AC inlet.

4 Do not remove the power supply in power supply bay PS1 until a replacement power supply is available.

5 Remove the power supply by simultaneously pressing the power supply lock tab to the left, grasping the handle, and pulling the power supply straight out of the PV-FC-180 application sensor.

6 If you are removing the power supply from power supply bay PS2, and you are not immediately installing another power supply, reinstall the coverplate that comes with the PV-FC-180 application sensor over the empty PS2 power supply bay.

> ⚠ Caution
>
> If you plan to operate the chassis with only one power supply, the power supply must be installed in the left power slot labeled PS1 and the coverplate must be in place in the right power slot to contain EMI radiation and ensure proper air circulation.
>
> PRECAUCIÓN
>
> Si desea trabajar sólo con una fuente de poder, no olvide colocar la tapa en el compartimiento de la fuente de poder que haya eliminado, para reducir la interferencia electromagnética y para asegurar una buena ventilación.

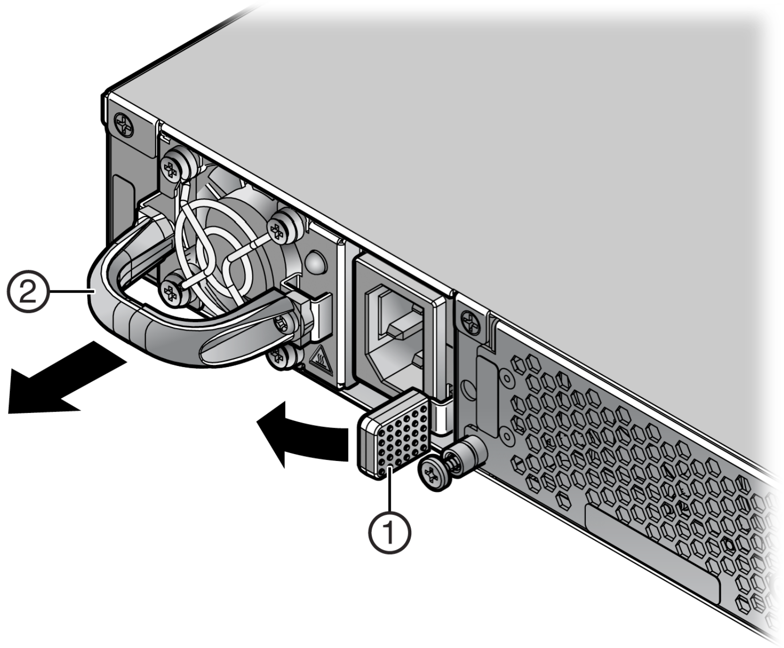


Figure 17: Removing the Power Supply

1	Lock tab	2	Power supply handle

Using the OFFLINE/RESET Button

You can shut down a PV-FC-180 application sensor using the OFFLINE/RESET button, shown in Figure 18: OFFLINE/RESET Button on page 44, which is slightly recessed behind the PV-FC-180 application sensor faceplate. There are two procedures to shut down a PV-FC-180 application sensor:

- Recommended Shutdown Procedure Using OFFLINE/RESET Button on page 44
- Last Resort Shutdown Procedure Using OFFLINE/RESET Button on page 44 (this procedure is not recommended)

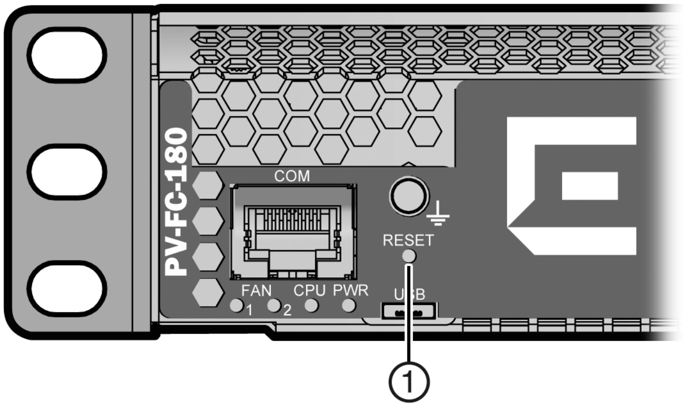


Figure 18: OFFLINE/RESET Button

1	OFFLINE/RESET button

Recommended Shutdown Procedure Using OFFLINE/RESET Button

Before shutting off power to a PV-FC-180 application sensor, press or tap on its OFFLINE/RESET button for less than one second.

The PV-FC-180 system CPU LED changes from solid green to blinking between green and amber, indicating that the PV-FC-180 application sensor is shutting down. At the end of the shutdown routine, the CPU LED changes to a 67% / 33% sequence of amber / off, respectively, indicating the system is in a halt state. At this time it is safe to restart the PV-FC-180 application sensor.

When you initiate a controlled shutdown with the OFFLINE/RESET button, you have 60 seconds from the time the CPU LED starts flashing amber/off until the device automatically restarts.

Last Resort Shutdown Procedure Using OFFLINE/RESET Button

⚠

Caution

This method of shutting down a PV-FC-180 application sensor is not recommended except as a last resort, because all processes currently running on the PV-FC-180 application sensor will be interrupted, resulting in loss of frames.

PRECAUCIÓN

No se recomienda utilizar este método para apagar los módulos PV-FC-180. Recurra a él sólo como último recurso, puesto que interrumpe todos los procesos del módulo en funcionamiento, lo que podría resultar pérdidas de frames.

To reset an PV-FC-180 application sensor without it performing an orderly shutdown routine, press and hold the OFFLINE/RESET button for approximately six seconds.

A Specifications

Extreme Networks reserves the right to change specifications at any time without notice.

PV-FC-180 Application Sensor Specifications

The following table describes I/O ports for the PV-FC-180 application sensor.

Table 14: PV-FC-180 Application Sensor Ports

Item	Port Description
Uplink Ports 1 through 4	Four 10Gb SFP+ ports

The following table describes physical, electrical, and environmental specifications for the PV-FC-180 application sensor.

Table 15: Specifications

Item	Specification
Physical (PV-FC-180 Chassis)	
Dimensions	4.37 cm H x 44.73cm W x 57.30 cm D 1.72” H x 17.61” W x 22.55” D
Approximate Weight	Gross: 14.6 kg (32.2 lb)
Mean Time Between Failure (MTBF)	Refer to the MTBF web site at URL www.extremenetworks.com/support/policies/mean-time-between-failures/
SSA-FB-AC-PS-A and SSA-FB-AC-PS-B (Power Supplies)	
Input Frequency	50 to 60 Hz
Input (Voltage/Current) at Output Power	100 to 240 V AC: 5.29 to 2.2A at 450 watts
Approximate Weight	0.86 kg (1.90 lb)
Environmental	
Operating Temperature	5°C to 40°C (41°F to 104°F)
Storage Temperature	-30°C to 73°C (-22°F to 164°F)
Operating Relative Humidity	5% to 95% (non-condensing)

Pluggable Transceiver Specifications

For SFP+ transceiver specifications, refer to the datasheet at the following URL: http://learn.extremenetworks.com/rs/extreme/images/Pluggable-Transceivers-DS.pdf

COM Port Pinout Assignments

The COM port is an RJ45 communications port for local access to local management. Refer to the table below for the COM port pin assignments.

Table 16: COM Port Pin Assignments

Pin	Signal Name	Input/Output
1	Transmit Data (XMT)	Output
2	Data Carrier Detect (DCD)	Output
3	Data Set Ready (DSR)	Input
4	Receive Data (RCV)	Input
5	Signal Ground (GND)	NA
6	Data Terminal Ready (DTR)	Output
7	Request to Send (RTS)	Input
8	Clear to Send (CTS)	NA

Regulatory Compliance

The PV-FC-180 application sensor meets the safety, electromagnetic compatibility (EMC), and environmental requirements listed below:

Table 17: Compliance Standards

Regulatory Compliance	Standard
Safety	UL 60950-1, FDA 21 CFR 1040.10 and 1040.11, CAN/CSA C22.2 No. 60950-1, EN 60950-1, EN 60825-1, EN 60825-2, IEC 60950-1, 2006/95/EC (Low Voltage Directive)
Electromagnetic Compatibility (EMC)	FCC 47 CFR Part 15 (Class A), ICES-003 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZS CISPR-22 (Class A). VCCI V-3. CNS 13438 (BSMI), 2004/108/EC (EMC Directive)
Environmental	2011/65/EU (RoHS Directive), 2002/96/EC (WEEE Directive), Ministry of Information Order #39 (China RoHS)

B Clearing the Persistent Storage or System Password

When troubleshooting the PV-FC-180 application sensor, it may become necessary to clear the persistent storage in NVRAM or the system password. There are two methods available:

- Enter boot loader mode during the bootup process.
- Manually set a dip switch internal to the device.

This appendix details the two methods available for clearing persistent storage or system password on the PV-FC-180 application sensor.

Clearing Persistent Storage or Password Using the Boot Loader Method

Persistent storage can be cleared or the system password reset to factory default using the boot loader by connecting a terminal application to the serial (console) port. Serial console access to the boot loader has been successfully tested with the following applications:

- HyperTerminal
- TeraTerm

Any other terminal applications may work but are not explicitly supported.

To either clear the PV-FC-180 appliance persistent storage or only the system password, proceed as follows:

1 With the console port connected, power up the device.
The following message displays:

```
Boot ROM Initialization, Version 01.02.02

Copyright (c) 2014 Extreme Networks, Inc.
SDRAM size: 1024 MB
Testing SDRAM....                  PASSED.
Loading Boot Image: 01.00.19...    DONE.
Uncompressing Boot Image...        DONE.
```

2 Once the boot image has finished uncompressing, you receive a message indicating you have three seconds to access the bootloader menu by pressing any key. Press a key and the system image loader prompt displays:

```
###You have 3 seconds to access the bootloader menu###
Press any key to enter System Image Loader menu
PressAnyKey
[System Image Loader]:
```

3. Enter the `clearnvram` command to clear all of persistent storage; enter `clearpw` to only clear the system password:

   ```
   [System Image Loader]:clearnvram or clearpw
   [System Image Loader]:
   ```

4. Power the system off and back on to reboot the system using the factory defaults.
5. Enter `admin` at the username prompt.
6. Press **[ENTER]** at the password prompt.

See the Image Configuration and File Management chapter of the *S-, K-, and 7100 Series Configuration Guide* for instructions on restoring a config if you cleared the NVRAM.

Clearing System Storage or Password Using the Dip Switch Method

⚠	ELECTRICAL HAZARD
	Only qualified personnel should install or service this unit.
	RIESGO ELECTRICO
	Nada mas personal capacitado debe de instalar o darle servicio a esta unida.
	ELEKTRISCHER GEFAHRENHINWEIS
	Installationen oder Servicearbeiten sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.
	RISQUES D'ÉLECTROCUTION
	Seul un personnel qualifié doit installer ou effectuer les opérations de maintenance sur cet élément.

⚠	ELECTRICAL HAZARD
	Do not remove any component from the PV-FC-180 while power is applied to the unit. Hazardous voltages are present and could cause personal injury and/or damage the unit. Do not power up the PV-FC-180 again until all components and screws are in place.
	RIESGO ELECTRICO
	No debe de remover cualquier componente durente que este coneltado a la corriente, una descarga electrica le puede causar y probocarle daños, al igual que al aparato. No enchufe a la corriente hasta que todo componente y los tornillos esten en su lugar.
	ELEKTRISCHER GEFAHRENHINWEIS
	Entfernen sie nicht beliebig komponenten des PV-FC-180, wenn dieser noch an die Stromzufuhr angeschossen ist, gefährliche Spannungen können Personen verletzten oder das Gerät beschädigen. Schalten Sie den PV-FC-180 nicht ein, bevor alle komponente das Gerät abdeckt und mit den Schrauben fixiert wurde.

RISQUES D'ÉLECTROCUTION

Ne retirez aucun composant du commutateur lorsque l'appareil est sous tension. Des tensions dangereuses pourraient entraîner des blessures ou endommager l'élément.

Warning

This unit may have more than one power supply cord. Disconnect two power supply cords before servicing to avoid electric shock.

ADVERTENCIA

Esta unida puede tener mas de un cable de fuente de poder. Desconectar dos cables de fuentes de poder antes de dar servicio para prevenir riesgo eléctrico.

WARNHINWEIS

Dieses Gerät hat mehrere Netzanschlüße, trennen Sie vor den Wartungsarbeiten beide Netzanschlüsse vom Versorgungsnetz. zum Schutz vor elektrischen Schlägen.

AVERTISSEMENTS

Cet élément pourrait avoir plus d'un câble d'alimentation. Déconnectez tous les câbles d'alimentation avant d'effectuer les opérations de maintenance sur l'appareil afin de réduire les risques d'électrocution.

Required Tools

Use the following tools to perform the procedure provided in this appendix:

- ESD wrist strap
- Phillips screwdriver capable of extending 6 or more inches into the unit
- Flash light (recommended)

Caution

An antistatic wrist strap is required to perform the procedures in this appendix. Use the antistatic wrist strap to minimize ESD damage to the devices involved.

PRECAUCIÓN

Para llevar a cabo los procedimientos especificados en el apéndice deberá utilizar una pulsera antiestática. Esta pulsera sirve para minimizar los efectos de las descargas de electricidad estática.

About the Mode Switches

Caution

Read the appropriate sections to be fully aware of the consequences when changing switch settings.

Only qualified personnel should change switch settings.

PRECAUCIÓN

Si desea modificar la configuración del interruptor, lea las secciones correspondientes para saber cuál será el resultado de hacerlo.

Estas modificaciones a la configuración sólo debe realizarlas personal calificado.

Figure 19: Mode Switch Location on page 50 shows the locations of the mode switches and the switch settings for normal operation. These switches are set at the factory and rarely need to be changed. Switches are numbered 1 through 8 from left to right.

Switch definitions and positions are as follows:

- Switches 1– 6: For Extreme Networks use only.
- Switch 7: Clear Persistent Data. Changing the position of this switch from the up position to the down position clears persistent data on the next power-up of the PV-FC-180 application sensor. All user-entered parameters, such as the IP address, system name, and so on, are reset to the factory default settings. Once the system resets, you can either use the factory default settings or reenter your own parameters.
- Switch 8: Clear Admin Password. Changing the position of this switch from the up position to the down position clears the admin password, and restores the factory default password on the next power-up of the system. Once the PV-FC-180 application sensor resets, you can either use the factory default setting or reenter your own password.

Note

Do not change the position of Switch 8 unless it is necessary to reset the admin password to its factory default setting.

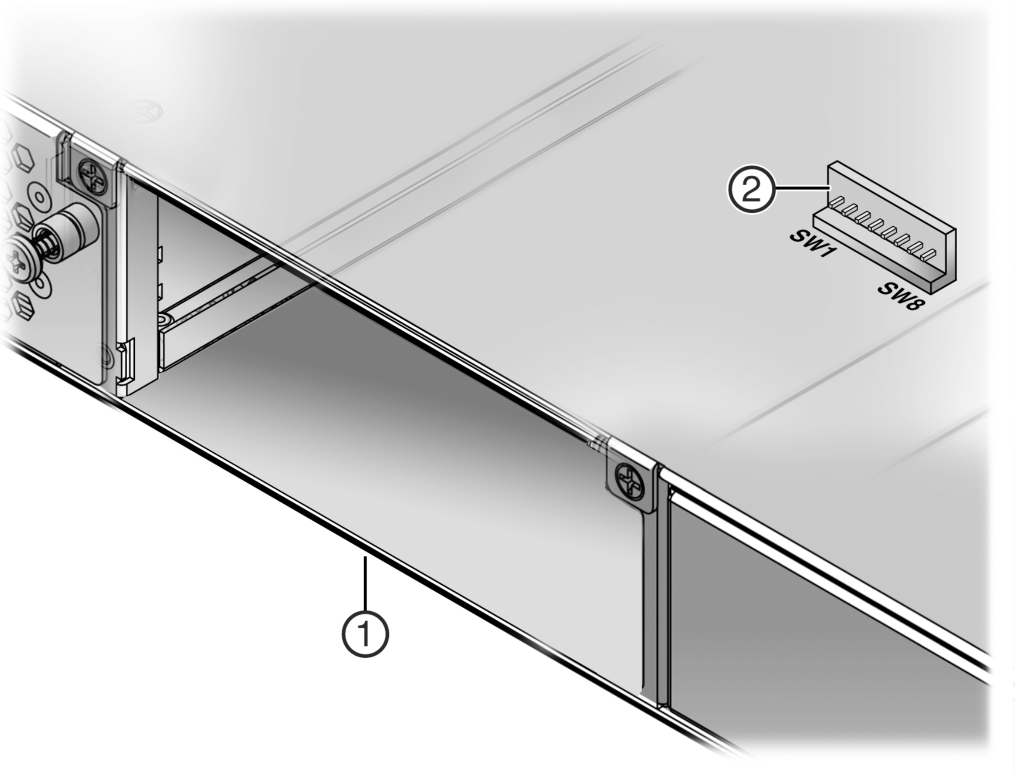


Figure 19: Mode Switch Location

1	Fan Module Bay 2	2	Mode Switches

Setting the Mode Switches

Before setting the mode switches, you must power down the PV-FC-180 application sensor.

1. Put on the ESD wrist strap and attach it to the ground receptacle on the switch I/O ports side of the PV-FC-180 application sensor.
2. Remove fan module 2 from the PV-FC-180 application sensor detailed in steps 1–5 of Replacing the Fan Module on page 41.
3. Toggle the appropriate switch to the opposite position relative to its current state.
4. Reinstall fan module 2 detailed in steps 6–8 of Replacing the Fan Module on page 41.

Note

Switches 7 and 8 are treated as one-time toggle switches. The system looks for a change in position since the last system reset. If the position of switch 7 has changed since the last reset, persistent storage will clear on this reboot. If the position of switch 8 has changed since the last reset, the system password will reset to the default password on this reboot.

C Optional Rack Mount Rail Kit Installation

This appendix describes the installation and use of the optional Universal Rack Mount Kit, model number SSA-FB-MOUNTKIT. This optional rack mounting kit provides for flexible mounting options in both 4-post and 2-post rack installations.

⚠	ELECTRICAL HAZARD
	Only qualified personnel should install or service this unit.
	RIESGO ELECTRICO
	Nada mas personal capacitado debe de instalar o darle servicio a esta unida.
	ELEKTRISCHER GEFAHRENHINWEIS
	Installationen oder Servicearbeiten sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.
	RISQUES D'ÉLECTROCUTION
	Seul un personnel qualifié doit installer ou effectuer les opérations de maintenance sur cet élément.

Required Tools

- ESD wrist strap (included with the PV-FC-180 chassis)
- Phillips screwdriver

Contents of Mounting Kit

The following table lists the contents of the SSA-FB-MOUNTKIT mounting kit.

Table 18: Contents of SSA-FB-MOUNTKIT

Item	Quantity
Left and right rails and extensions assemblies	2
Adapter plates	2
Mid-Brackets	2
6-32 flat head screws	6
10-32 pan head screws (black)	2
10-32 cage nuts	2

Note

The SSA-FB-MOUNTKIT mounting kit does not include rack screws. You must provide screws or fasteners appropriate to your rack for securing the rails and the PV-FC-180 chassis in the equipment rack. Each procedure in this guide specifies the number of rack screws that you must provide.

Installation Site Requirements

To cable your PV-FC-180 application sensor with SFP+ pluggable transceivers, you may need to have 3–4 inches of clearance on the switch I/O port side of the PV-FC-180 application sensor.

See Environmental Guidelines on page 79 for environmental guidelines relating to the PV-FC-180 application sensor installation.

The installation site must be within reach of the network cabling and meet the requirements listed below:

- Appropriate grounded power receptacles must be located within 7 feet of the site.

- A temperature of between 5°C (41°F) and 40°C (104°F) must be maintained at the installation site with fluctuations of less than 10°C (18°F) per hour.

Caution

To ensure proper ventilation and prevent overheating, leave a minimum clearance space of 5.1 cm (2.0 in.) at the front and rear of the device.

PRECAUCIÓN

Para asegurar una buena ventilación y evitar que el sistema se sobrecaliente, deje un espacio mínimo de 5.1 cm (2 pulgadas) con respecto el anverso y reverso del aparato.

Warning

Before rack-mounting the device, ensure that the rack can support it without compromising stability. Otherwise, personal injury and/or equipment damage may result.

ADVERTENCIA

Antes de montar el equipo en el rack, asegurarse que el rack puede soportar su peso sin comprometer su propia estabilidad, de otra forma, daño personal o del equipo puede ocurrir.

WARNHINWEIS

Überzeugen Sie sich vor dem Einbau des Gerätes in das Rack von dessen Stabilität, ansonsten könnten Personenschäden oder Schäden am Gerät die Folge sein.

AVERTISSEMENTS

Avant de monter l'appareil sur le bâti, assurez-vous que l'étagère peut en supporter le poids sans en compromettre la stabilité. Cela pourrait, dans le cas contraire, entraîner des blessures ou des dommages au matériel.

For more information about flat surface installation or rack installation using the mounting brackets installed on the PV-FC-180 application sensor, see Installation on page 11.

Required Order of Installation

1. Remove the rack mount ears from the chassis.
2. Attach the adapter plates to the chassis.
3. Install the rail assemblies in either a four post rack (see Four-Post Rack Mount Installation on page 56) or a two post rack (see Two-Post Rack Mount Installation on page 60).
4. Install the chassis in the rack.

Removing the Rack Mount Ears from the PV-FC-180 Application Sensor

Remove the rack mount ears from both sides of the PV-FC-180 application sensor before continuing with the mounting kit installation. See the following figure.

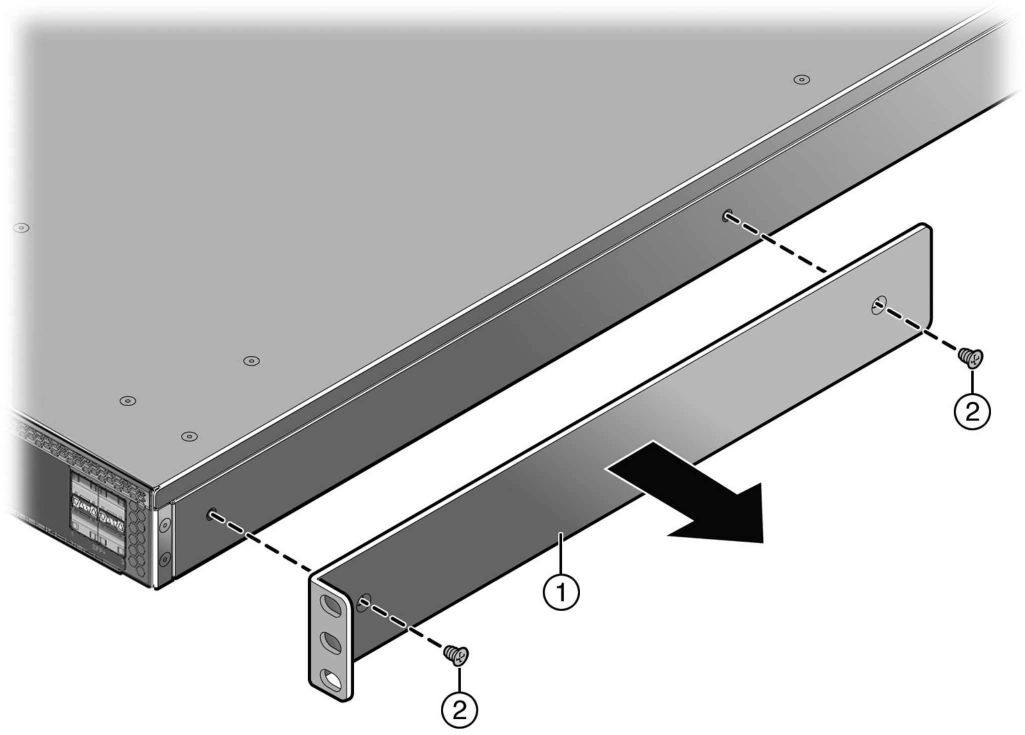


Figure 20: Removing the PV-FC-180 Application Sensor Rack Mount Ears

1	Rack mount ear	2	Rack mount ear screws

The removed rack mount ears and screws are not used in any mounting kit installation procedures.

Installing the Adapter Plates

Two adapter plates come with the mounting kit. Adapter plates are used to secure the chassis to:

- The rail and extension assemblies used in the 4-post rack configuration (see Rack Mount Rail with Attached Extension Assembly Installation on page 58)
- The rail and mid-bracket assemblies used in the 2-post rack configuration (see Pre-Installation Tasks on page 61)

The adapter plates can be installed in either a flush or a recessed configuration of up to 1.5 inches.

The PV-FC-180 application sensor can be configured for air intake on either the I /O port side or the power supply side. Adapter plate installation must align the adapter plate ears with the air intake side of the chassis.

If you have not verified the power supply and fan module air flow for the chassis you are installing, see Power Supply Air Flow and Switch Fan Module Air Flow on page 14 for information on determining air flow direction for your chassis before installing the adapter plates.

See Reversing the Fan Module Air Flow on page 15 if the current fan module air flow direction does not match the intended chassis air flow direction.

To install the adapter plates:

1 Place the adapter plates on each side of the chassis with the ear end toward the air intake side of the chassis, ear flange pointing away from the chassis. Figure 21: Installing the Adapter Plates on page 56 shows the correct orientation for a chassis with air flow from switch I/O port side to power supply side.

2 Align either the flush mount adapter plate screw holes (Callout 2) or the appropriate recess mount adapter plate screw holes with the three chassis screw holes on each side of the chassis. Callout 3 identifies the screw holes used to recess the chassis by .5, 1.0, or 1.5 inches.

Note

When recess mounting, use care that the installation does not result in openings above and below the chassis face at the inlet side that allow for hot air recirculation from the exhaust side of the rack or cabinet. This is especially the case for a cabinet with enclosed sides where the cold and hot aisles are meant to be isolated.

3 Insert and tighten three of the six 6-32 flat head screws that come with the mounting kit in three places on each side of the chassis.

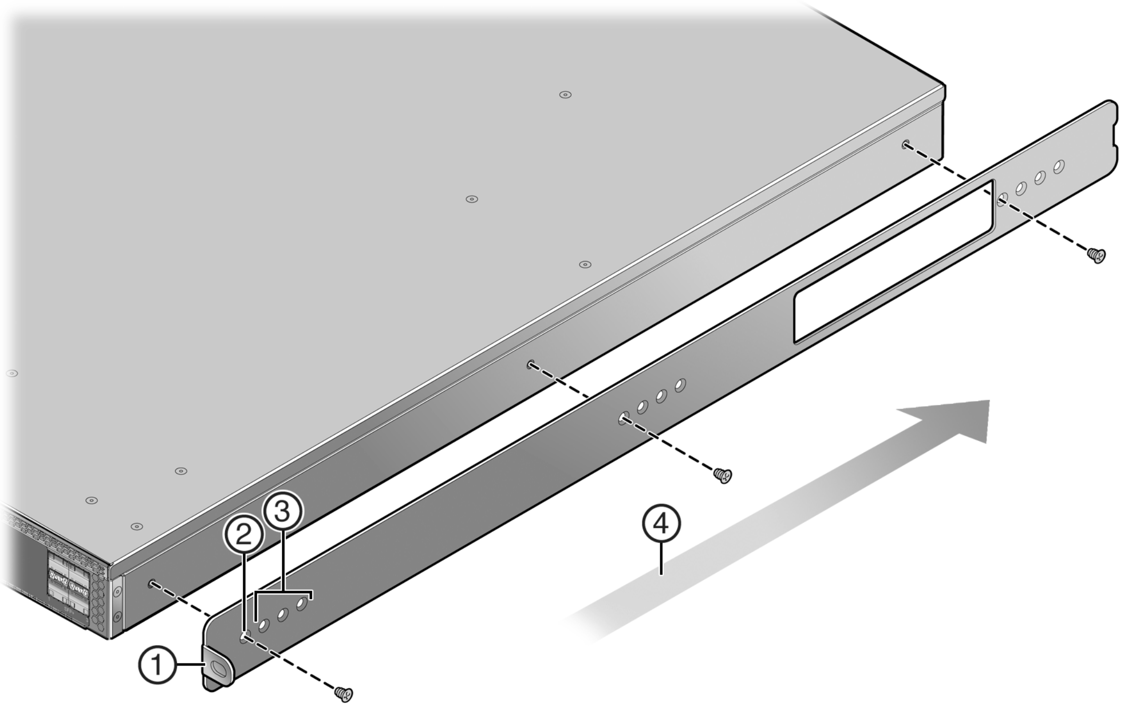


Figure 21: Installing the Adapter Plates

1	Adapter plate (ear side)	3	Recess mount adapter plate screw holes (1.5 in.)
2	Flush mount adapter plate screw hole	4	Air flow direction

Four-Post Rack Mount Installation

The rack mount option kit supports the flush mount configuration for a four-post rack installation, with the option of recessing the chassis a maximum of 1.5 inches. Both air flow directions are supported.

Figure 22: Four-Post Rack Supported Configurations on page 57 displays the four-post rack flush mount configuration for both air flow directions. The recessed chassis configurations (configured when installing the adapter plates, see Figure 21: Installing the Adapter Plates on page 56) are not displayed.

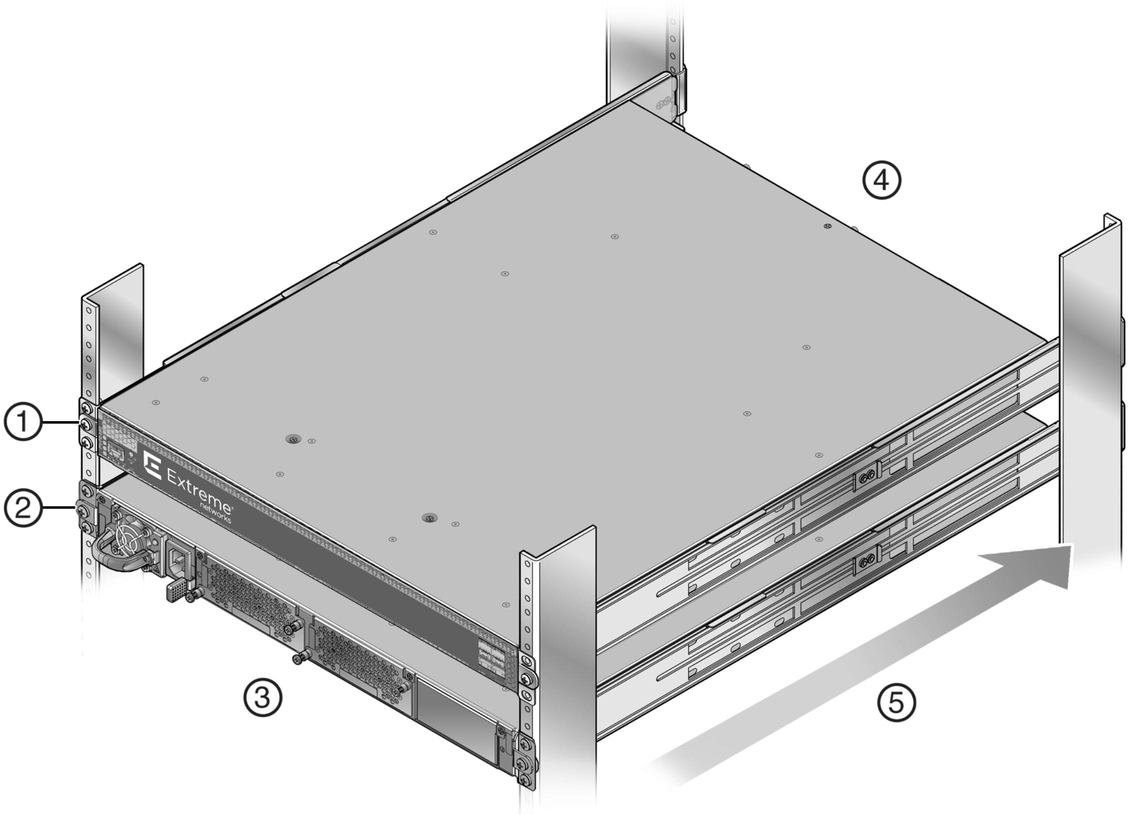


Figure 22: Four-Post Rack Supported Configurations

1	Flush mount, switch I/O port side to power supply side air flow	4	Hot air exhaust side
2	Flush mount, power supply side to switch I/O port side air flow	5	Air flow direction
3	Cool air intake side		

This section details the installation of the optional rack mount kit for a four-post rack and covers installing:

- The rack mount rail and extension assembly to the rack
- The PV-FC-180 chassis to the rack mount rail and extension assembly

  The optional rack mount kit contains two pre-assembled rack mount rails with attached extensions. The length of each assembly is adjustable from 22 inches to 30 inches. Each assembly is labeled either "right front" or "left front". The front of the rack is always the cool air intake side. The rear of the rack is always the hot air exhaust side.

Rack Mount Rail with Attached Extension Assembly Installation

Refer to Figure 23: Installing the Rack Mount Rail with Extension Assemblies on page 58 as you perform the following procedure. You must supply eight rack screws to install the rack mount rails in the equipment rack.

To install the rack mount rail with extension assembly:

1 Adjust the length of the two assemblies (callout 1) to agree with the distance between the outer face of the vertical rack posts. The screws (callout 5) holding the assembly together may need to be loosened slightly to allow for the adjustment. Retighten any loosened screws once the adjustment has been made.

2 Install the side of the assembly labeled "right front" (callout 2) on the front (cool air inlet) right rack post. Secure the assembly to both the front and rear posts, using rack appropriate screws or fasteners that you supply.

Do not use the middle hole when securing the assembly to the rack post. The middle hole is used to secure the adapter plate (previously installed on the chassis) to the assembly.

3 Repeat Step 2 for the assembly labeled "left front".

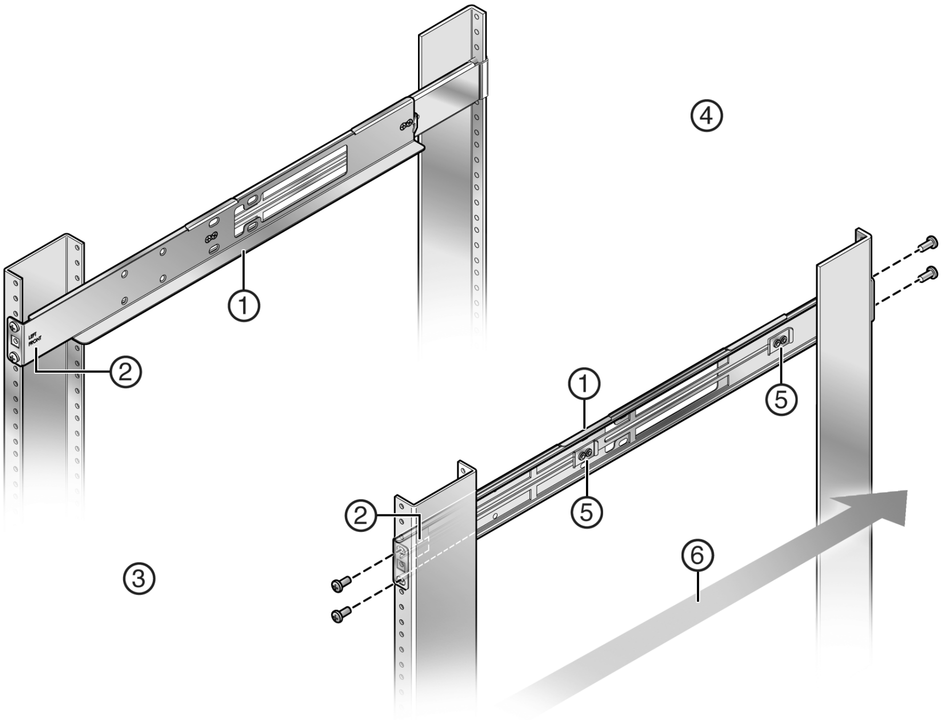


Figure 23: Installing the Rack Mount Rail with Extension Assemblies

1	Rack mount rail with extension assembly	4	Rack rear (hot air outlet)
2	Right/left front assembly label location	5	Rail assembly adjustment screws
3	Rack front (cool air inlet)	6	Air flow direction

Chassis to Rail Assembly Installation

Refer to Figure 24: Installing the Chassis on to the Rack Mount Rail Assembly on page 59 as you perform the following procedure.

To install the chassis into the rail assembly:

1. Face the front (cool air) side of the rack (callout 1) with the air intake side of the chassis (callout 2) facing you.
2. Slide the chassis with the installed adapter plates onto the rack mount rails until the adapter plate ear (callout 3) meets the middle screw hole (callout 4) of the rack mount rail.
3. Secure the chassis with one screw or fastener appropriate to your rack in each of two adapter plate ear screw holes.

   A flange (callout 6), towards the back of each rail assembly secures the back side of the chassis adapter plate in place. If needed, loosen the two screws (callout 8) that secure the rear of the rail assembly to the rack and adjust the rail assembly position for best fit or alignment. Retighten the two screws.

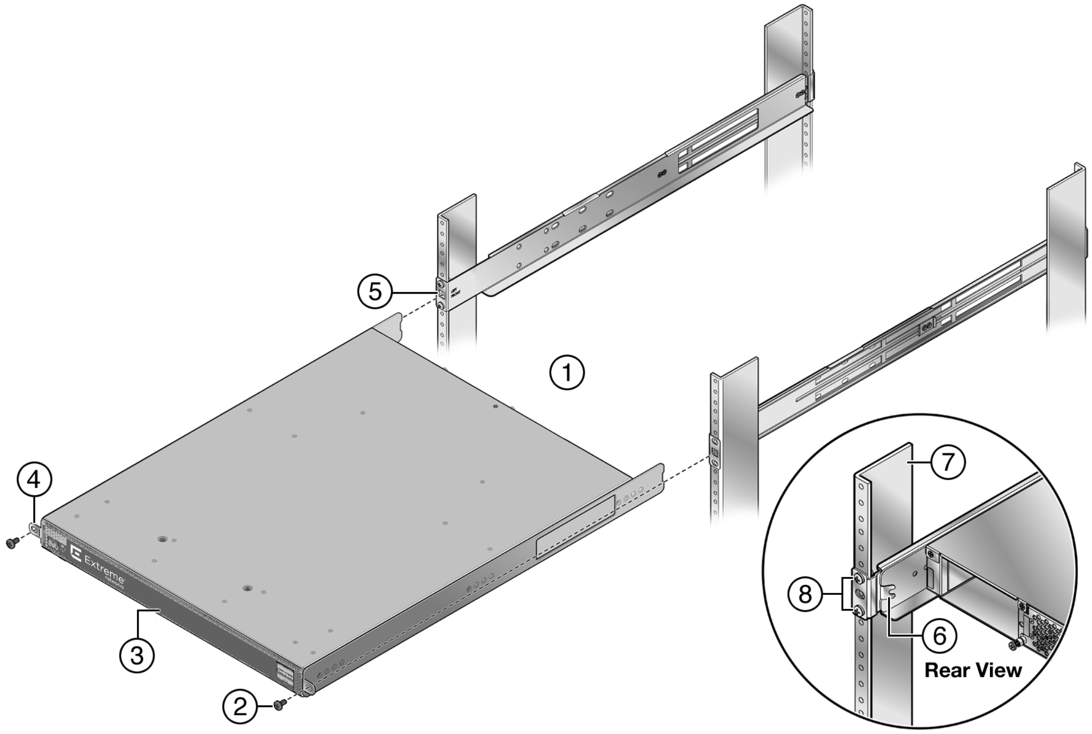


Figure 24: Installing the Chassis on to the Rack Mount Rail Assembly

1	Rack front (cool air inlet)	5	Rail assembly middle screw hole
2	Rack specific screw (2)	6	Rail assembly flange
3	Chassis air intake side	7	Rear rack post
4	Adapter plate ear	8	Rail assembly to rack screws

Two-Post Rack Mount Installation

The rack mount option kit supports two configurations for a two-post rack installation:

- A 3 inch or 7.25 inch post flush mount configuration
- A mid-mount configuration

The option of recessing the chassis up to 1.5 inches is also supported for each configuration (see Installing the Adapter Plates on page 55). Both air flow directions are supported.

The figure below displays the two-post rack flush mount and mid-mount configurations for supported air flow directions for a 3 inch post installation. The same configurations apply to a 7.25 inch post installation. The recessed chassis configurations are not displayed.

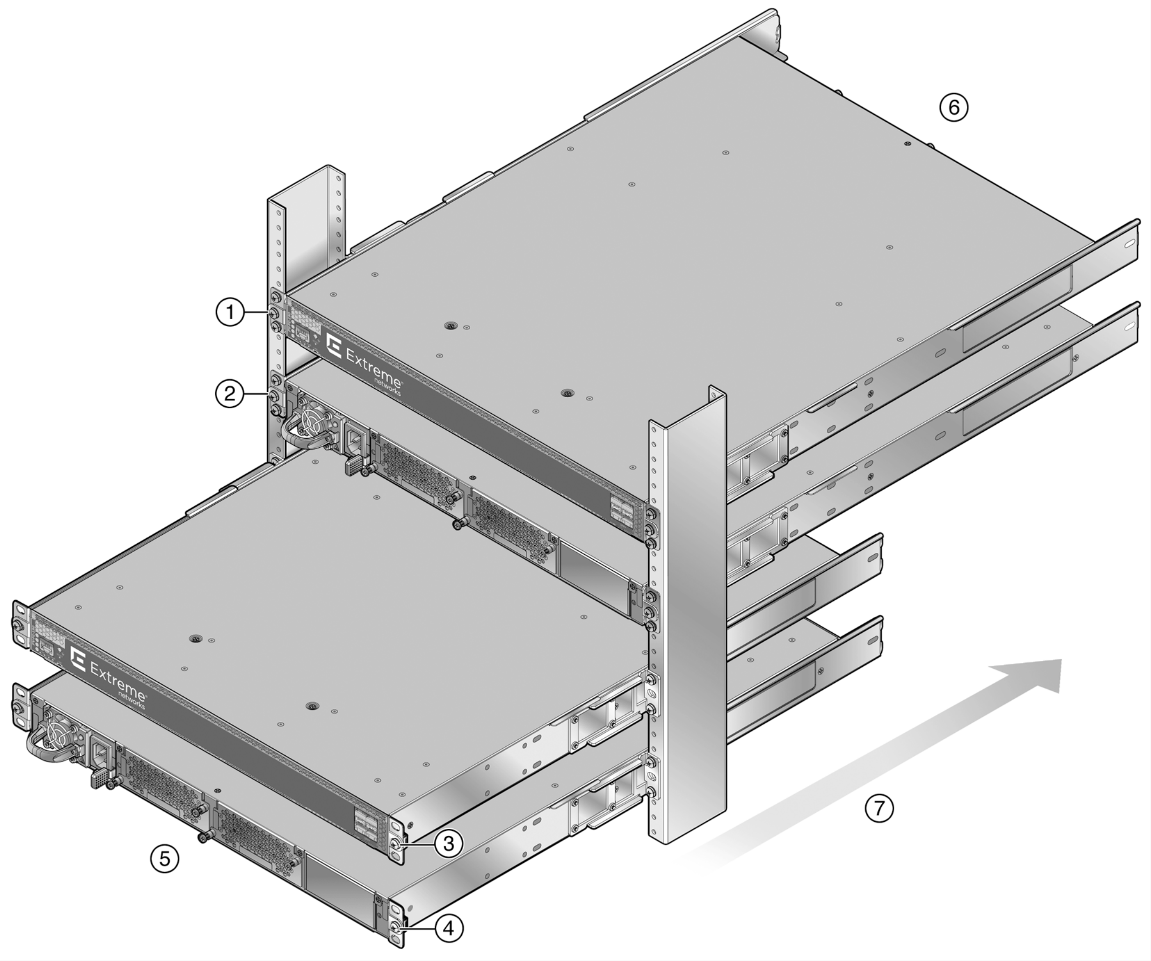


Figure 25: Two-Post Rack Supported Configurations

1	Flush mount, I/O port side to power supply side air flow	5	Cool air intake side
2	Flush mount, power supply side to I/O port side air flow	6	Hot air exhaust side
3	Mid-mount, I/O port side to power supply side air flow	7	Air flow direction
4	Mid-mount, power supply to I/O port side air flow		

This section details the installation of the optional rack mount kit for a two-post rack, including:

- Preparing the rack mount rail assembly for a two-post rack installation, by removing the extension from the rail assembly and adding a mid-bracket to the rail
- Securing the rack mount rail and mid-bracket assembly to the rack post

Pre-Installation Tasks

The rack mount kit rail assembly is pre-assembled for a four-post rack installation. Before installing the rail to a two-post rack:

- Remove the extension from each rack mount kit rail with extension assembly as described in Rack Mount Rail Assembly Extension Removal on page 61.
- Install a mid-bracket in either a flush or mid-mount configuration to each rail as described in Mid-Bracket to Rail Assembly on page 62.

Rack Mount Rail Assembly Extension Removal

To remove the extension (callout 1) from the rack mount rail assembly, unscrew two screws from each of two assembly clips (callout 4) as shown below.

Retain the four screws (callout 3) from both mount rail assemblies for securing the mid-bracket to the rail (callout 2). Both the extensions and the assembly clips are not used for a two-post rack installation.

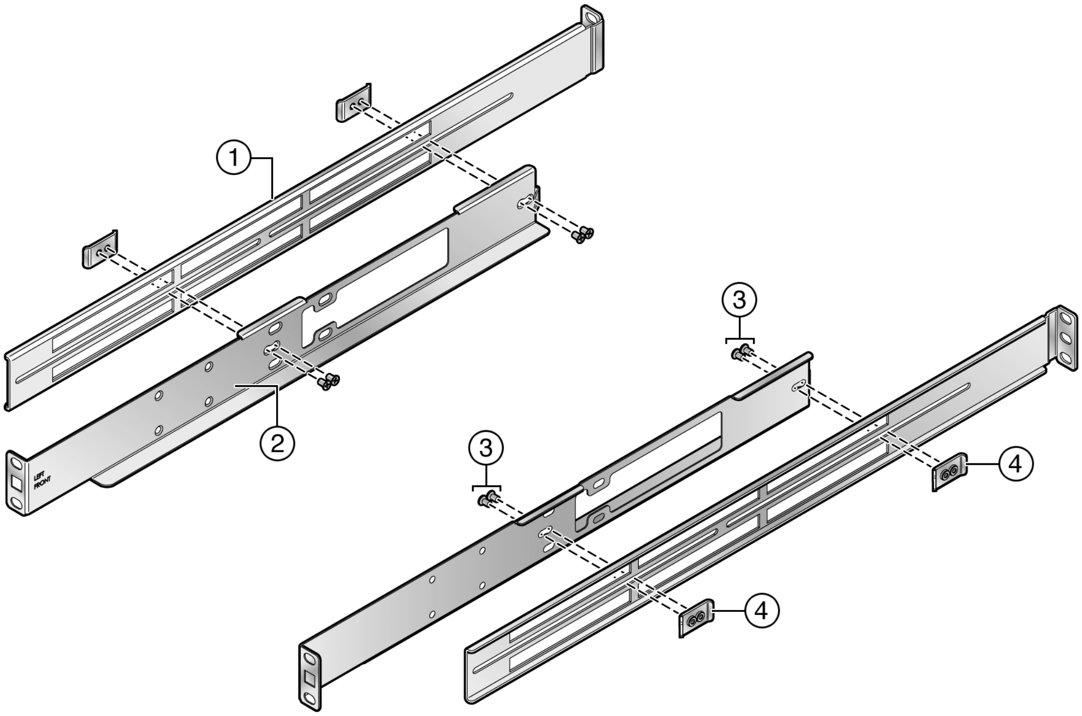


Figure 26: Removing the Extension from the Rack Mount Rail Assembly

1	Rack mount rail assembly extension	3	Rail assembly clip screws (4 per assembly)
2	Rack mount rail	4	Rail assembly clips (2 per assembly

Mid-Bracket to Rail Assembly

Note
The rack post must have holes on both the front and rear flanges to properly secure the rack mount rail in either a 3-inch or 7.25-inch flush two-post rack configuration. The rack post must have holes on the front flange to secure the rack mount rail in a mid-mount two-post rack configuration.

The mid-bracket is used to secure the rack mount rail to the rear flange of the rack post in a flush mount configuration or to the front flange of the rack post in a mid-mount configuration.

You can position the mid-bracket on to the rail in the following configurations:

- 3inches in from the rack mount rail ear for securing to the rear rack post flange in a 3-inch rack post flush mount configuration. See Figure 27: Securing Mid-Bracket to Rail 3-inch Flush Mount on page 63.
- 7.25 inches in from the rack mount rail ear for securing to the rear rack post flange in a 7.25-inch rack post flush mount configuration. See Figure 28: Securing Mid-Bracket to Rail 7.25-inch Flush Mount on page 64.
- 7.25 inches in from the rack mount rail ear for securing to the front rack post flange for a mid-mount configuration (the rear rack post flange is not used in a mid-mount configuration). See Figure 29: Securing Mid-Bracket to Rail 7.25-inch Mid Mount on page 65.

  The two-post rack mount rail can be installed in both a flush mount or mid-mount configuration. In a flush mount configuration, the rack mount rail is secured to both the front and rear flange of either a 3-inch or 7.25-inch rack post.

Mid-Bracket to Rail 3-inch Flush Mount Assembly

Note
If you are installing the rack mount rail in a flush mount 7.25-inch rack post or a mid-mount configuration, proceed to Mid-Bracket to Rail 7.25-inch Flush Mount or Mid-Mount Assembly on page 63, otherwise continue here.

To secure the mid-bracket to the rail for a 3-inch post flush mount assembly:

1. Align the mid-bracket (callout 2) with the four rail holes closest to the rail ear (callout 3) as shown in Figure 27: Securing Mid-Bracket to Rail 3-inch Flush Mount on page 63 for both rails.
2. Insert and secure the four screws (callout 1) from the rack mount extension assembly for both rails.

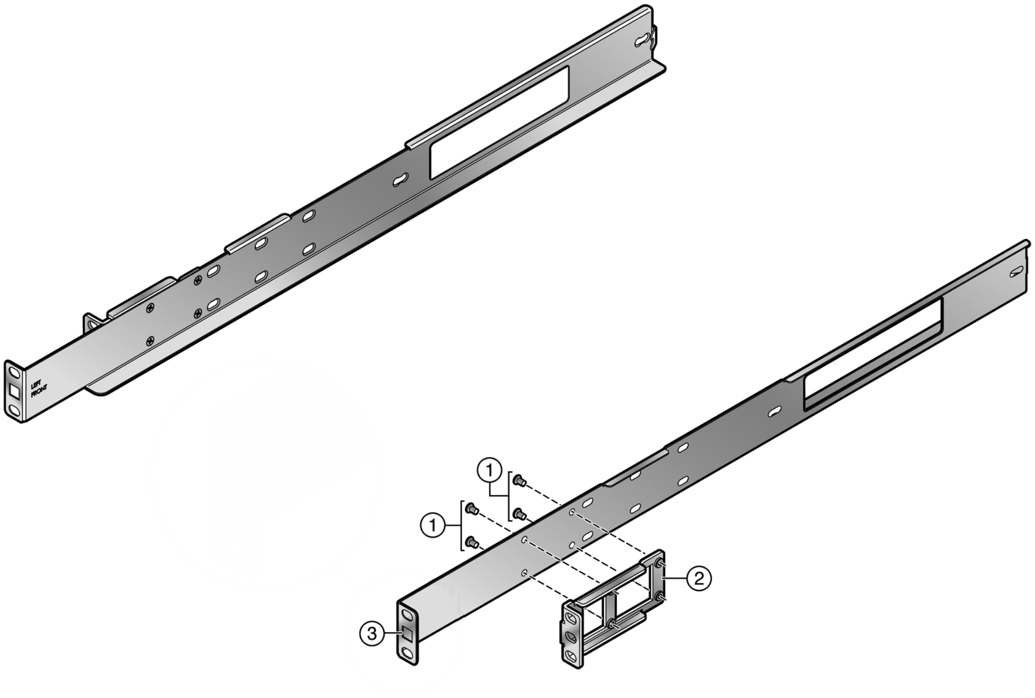


Figure 27: Securing Mid-Bracket to Rail 3-inch Flush Mount

1	Four screws from extension rack assembly	3	Rail ear
2	Mid-bracket		

Mid-Bracket to Rail 7.25-inch Flush Mount or Mid-Mount Assembly

To secure the mid-bracket to the rail for a 7.25-inch post flush mount or mid-mount assembly:

1 Align the mid-bracket (callout 2) with the four rail slots as shown in Figure 28: Securing Mid-Bracket to Rail 7.25-inch Flush Mount on page 64 for flush mount or Figure 29: Securing Mid-Bracket to Rail 7.25-inch Mid Mount on page 65 for mid-mount assembly.

2 Insert and secure the four screws (callout 1) from the rack mount extension assembly, allowing some play to adjust the mid-bracket position within the slot space when securing the assembly to the rack post

3 If the assembly will be used in a mid-mount configuration, insert a cage nut (callout 4, Figure 29: Securing Mid-Bracket to Rail 7.25-inch Mid Mount on page 65) that comes with the kit in the rail ear square opening (callout 3, Figure 29: Securing Mid-Bracket to Rail 7.25-inch Mid Mount on page 65).

4 Repeat steps 1–4 for the other rail.

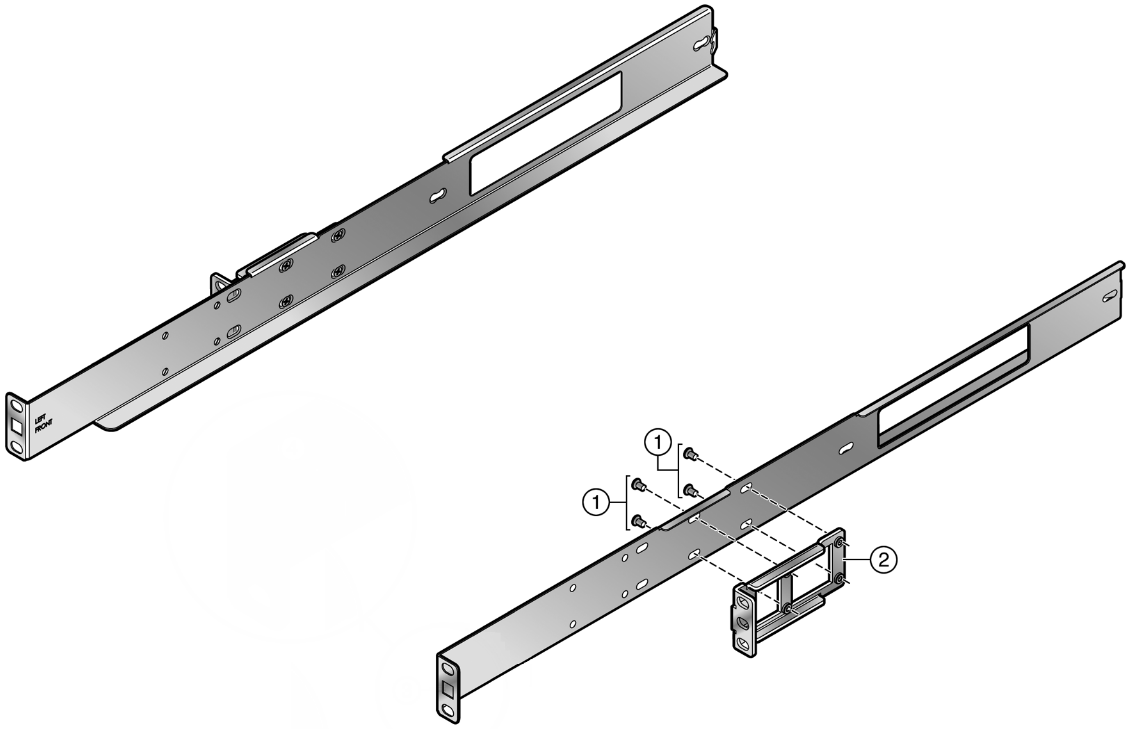


Figure 28: Securing Mid-Bracket to Rail 7.25-inch Flush Mount

1	Four screws from extension rack assembly	2	Mid-bracket

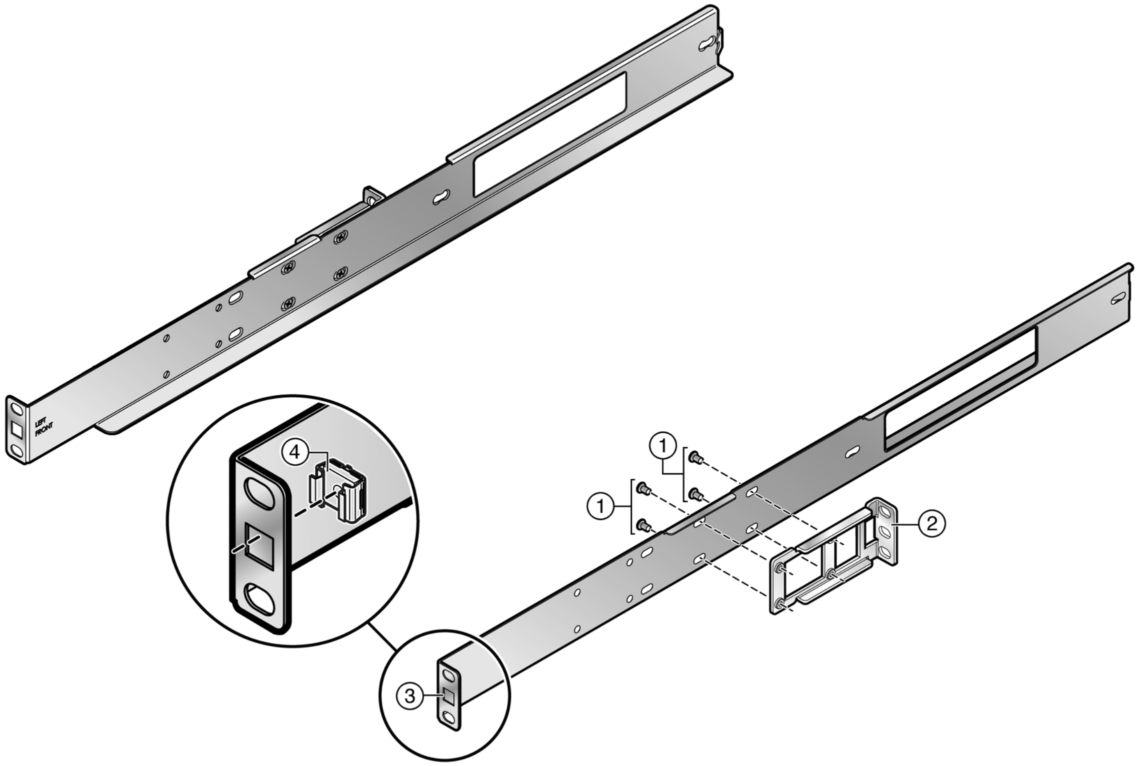


Figure 29: Securing Mid-Bracket to Rail 7.25-inch Mid Mount

1	Four screws from extension rack assembly	3	Rail ear square opening
2	Mid-bracket	4	Cage nut

Securing the Rail Assembly for a 2-Post Flush Mount Configuration

When securing the rail and mid-bracket assembly in a flush mount configuration:

1. Align the rail ear circular openings with outer front flange rack post openings and the mid-bracket ear openings with outer rear flange rack post openings as shown in Figure 30: Securing a Flush Mount Rail Assembly on page 66.

2 Secure each rail assembly with two screws or fasteners appropriate to the rack at both the rail ear and mid-bracket ear.

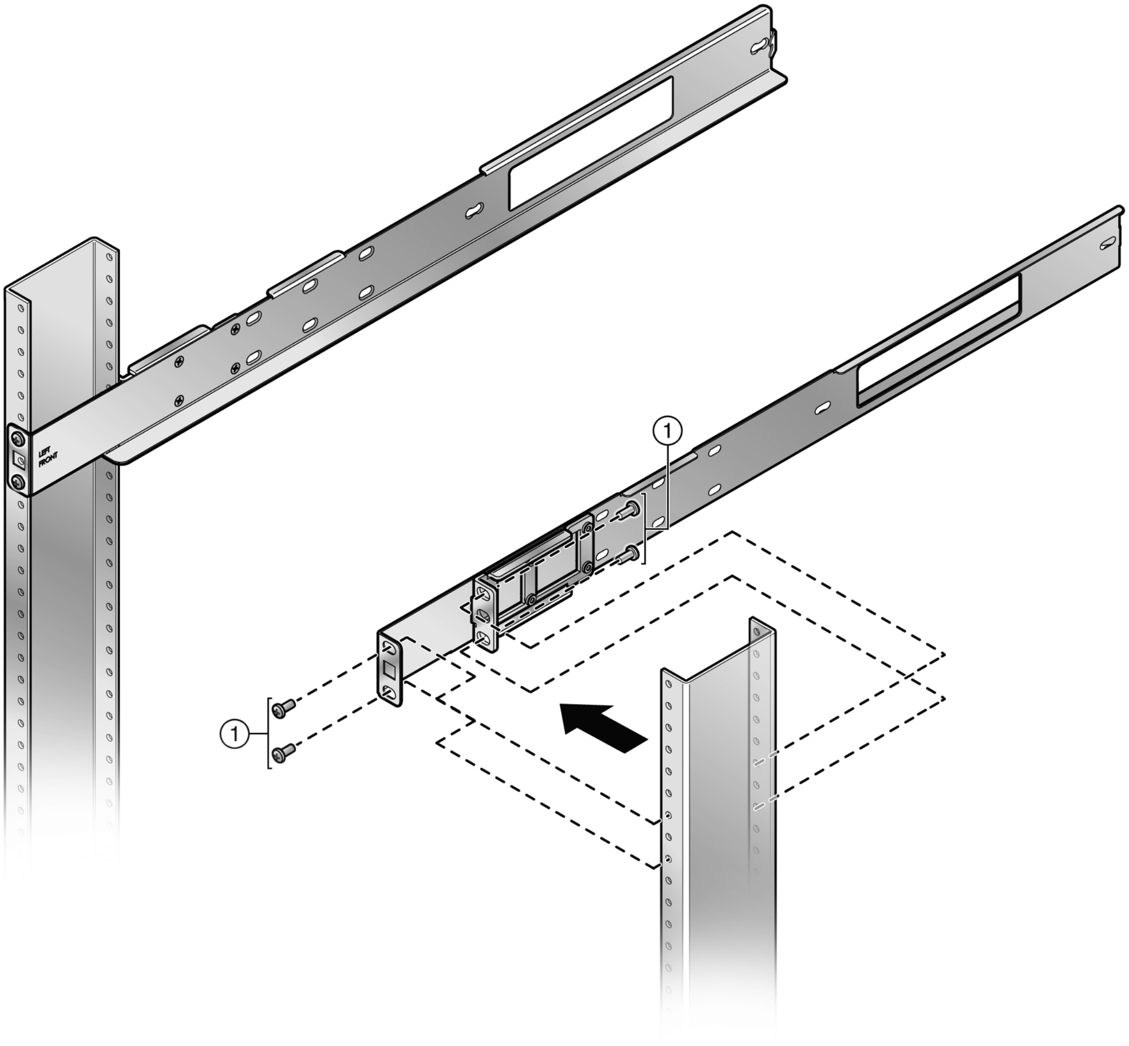


Figure 30: Securing a Flush Mount Rail Assembly

1	Rack appropriate screws of fasteners (8)

Securing the Rail Assembly for a 2-Post Mid-Mount Configuration

When securing the rail and mid-bracket assembly in a mid-mount configuration:

1 Ensure that a cage nut is installed in the rail ear square opening as described in Mid-Bracket to Rail 7.25-inch Flush Mount or Mid-Mount Assembly on page 63.

2 Align the mid-bracket ear openings with the outer front flange rack post openings as shown in Figure 31: Securing Mid-Mount Rail Assembly on page 67.

3 Secure the rail assembly with two screws or fasteners appropriate to the rack at both the rail ear and mid-bracket ear.

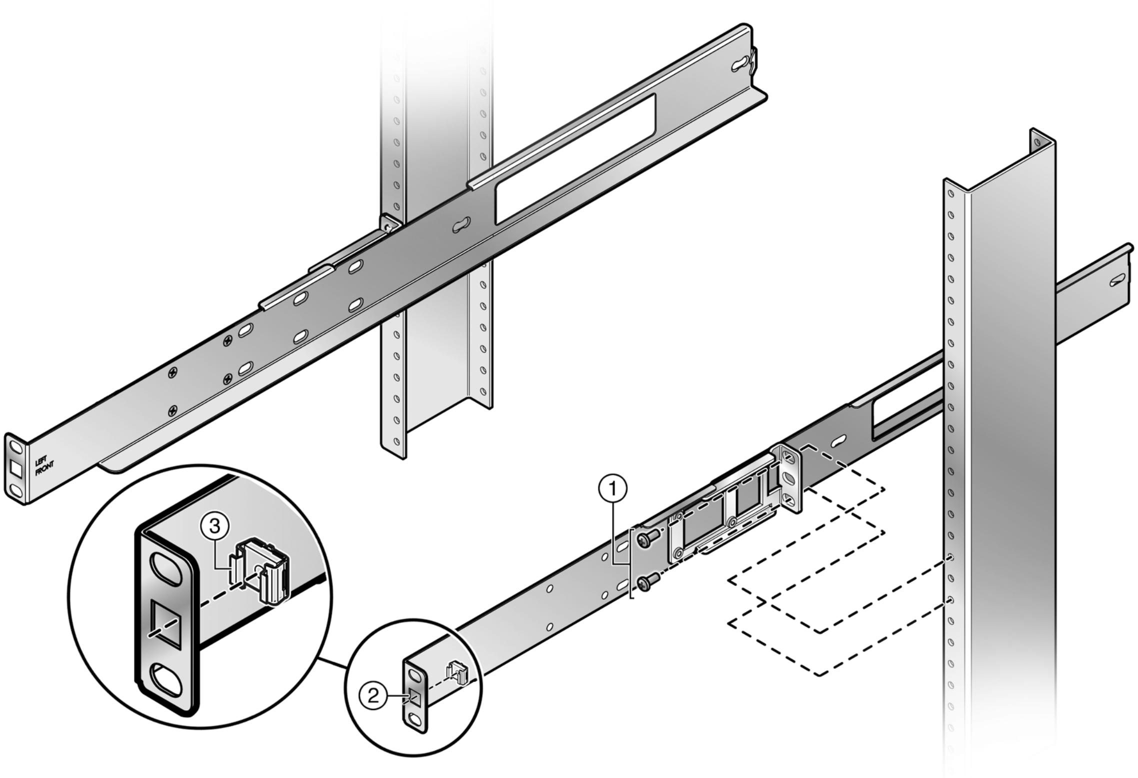


Figure 31: Securing Mid-Mount Rail Assembly

1	Rack appropriate screws or fasteners (4)	3	Cage nuts (2)
2	Rail ear square opening		

Securing the PV-FC-180 Application Sensor to the Rack

To secure the PV-FC-180 application sensor to the rack:

1 Slide the chassis onto the rail assembly until the chassis adapter plate ears meet the rail assembly ears. See Figure 32: Securing the PV-FC-180 Application Sensor to the Rack on page 68.

2 For a flush mount rail assembly configuration, secure each side of the chassis using a screw or fastener appropriate to your rack that you provide.

3 For a mid-mount rail assembly configuration, secure each side of the chassis using a black, 10-32 screw that comes with the rack mount kit. These screws are screwed into the cage nut installed in

the square rail ear opening as described in Step 3 of section Mid-Bracket to Rail 7.25-inch Flush Mount or Mid-Mount Assembly on page 63.

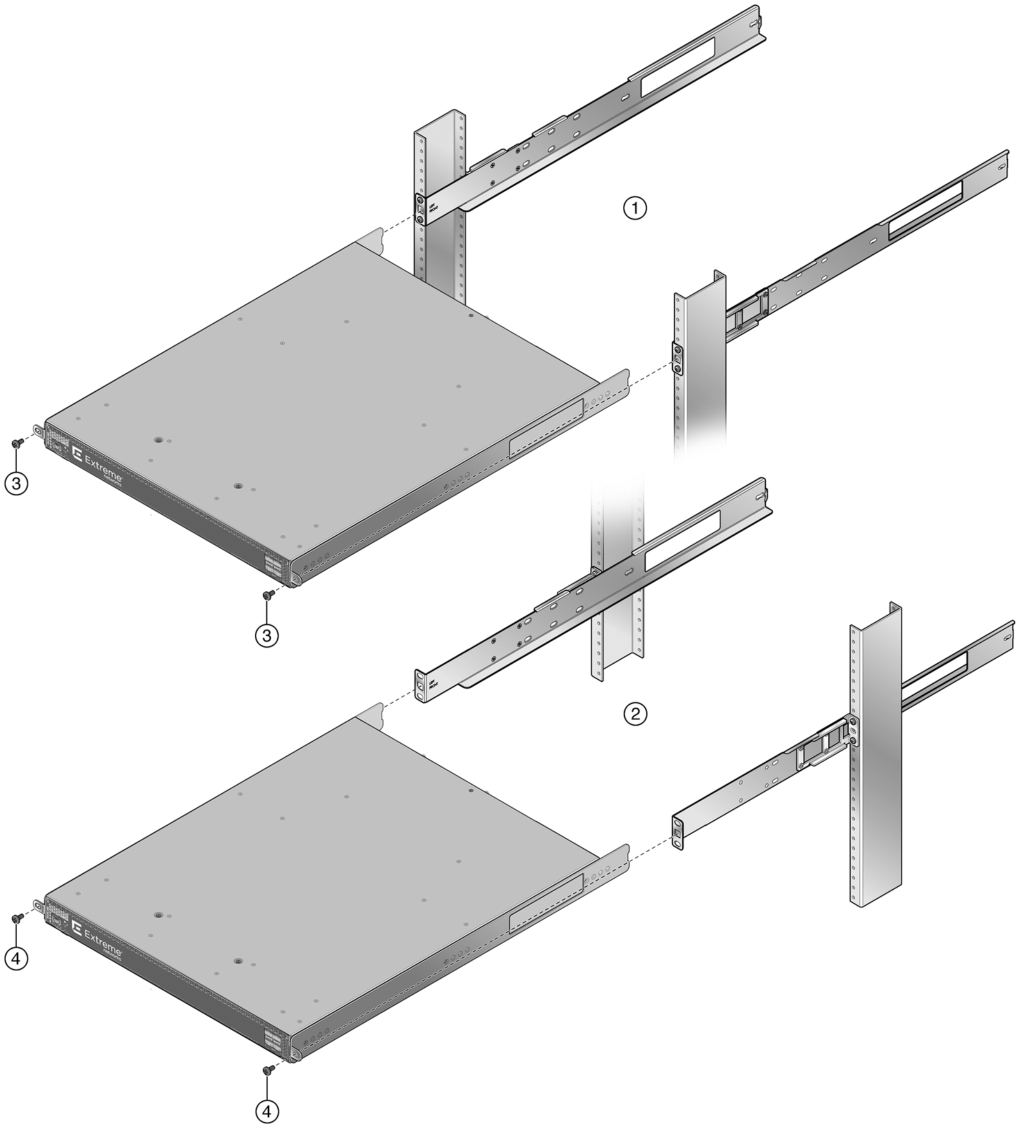


Figure 32: Securing the PV-FC-180 Application Sensor to the Rack

1	Flush mount configuration	3	Rack appropriate screws or fasteners (2)
2	Mid-mount configuration	4	Black 10-32 screws (2)

D Installing the SSA-WALL-MOUNT Kit

This appendix provides instructions for installing the PV-FC-180 application sensor on a wall using the optional SSA-WALL-MOUNT kit.

⚠	ELECTRICAL HAZARD
	Only qualified personnel should install or service this unit.
	RIESGO ELECTRICO
	Nada mas personal capacitado debe de instalar o darle servicio a esta unida.
	ELEKTRISCHER GEFAHRENHINWEIS
	Installationen oder Servicearbeiten sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.
	RISQUES D'ÉLECTROCUTION
	Seul un personnel qualifié doit installer ou effectuer les opérations de maintenance sur cet élément.

Required Tools

- ESD wrist strap (included with the PV-FC-180 application sensor)
- Phillips screwdriver

Contents of SSA-WALL-MOUNT Kit

The table below lists the contents of the SSA-WALL-MOUNT kit.

Table 19: Contents of SSA-WALL-MOUNT Kit

Item	Quantity
Mounting bracket	1
10-32 x .5 inch pan head screws	2

Note
The SSA-WALL-MOUNT kit does not include hardware for installing the mounting bracket on a wall.

You must provide screws and wall anchors that are appropriate for the wall on which you are installing the mounting bracket. The screws and wall anchors that you provide must be capable of supporting at least four times the combined weight of the PV-FC-180 chassis and two power supplies. For example, the combined weight of an PV-FC-180 chassis and two power supplies is 32.2 lb (14.6 kg). The screws and wall anchors must be able to support at least 128.8 lb (58.42 kg).

Preparing the Installation Site

The SSA-WALL-MOUNT mounting bracket may be attached to various types of wall construction.

- Hollow Wall Construction on page 70
- Concrete or Masonry Wall Construction on page 71

Note
Ensure that walls are clear of plumbing and electrical lines prior to drilling any mounting holes.

Use the SSA-WALL-MOUNT mounting bracket as a template to mark locations on wall prior to drilling.

Hollow Wall Construction

For hollow walls studded with metal or wood framing and sheathed with drywall, plaster, or plywood, use appropriate hollow wall fasteners in all four mounting locations through the hollow wall.

- Toggle Bolts on page 70
- Reusable Anchors on page 71
- Pan Head Steel Machine Screws on page 71

  The four mounting locations on the SSA-WALL-MOUNT mounting bracket, which are located side to side on 18.576” centers, do not coincide with typical wall stud centers. Position the mounting bracket to avoid studs at the four mounting locations.

Toggle Bolts

Toggle bolts must be at least 3/16". Each of the four toggle bolts used must be rated for 32.2 lb (14.6 kg) minimum.

Typical drill size is ½" for the 3/16" toggle bolt. Follow the manufacturer's instructions.

Reusable Anchors

The minimum recommended size for reusable anchors is #10 size. Each of the four reusable anchors must be rated for 32.2 lb (14.6 kg) minimum and be the appropriate size for the wall thickness.

Typical drill size is 3/8" for the #10 reusable anchor. Follow the manufacturer's instructions.

Pan Head Steel Machine Screws

If the rear side of the wall is accessible, you can bolt the wall mount bracket using four #10-#12 pan head steel machine screws with fender washers and lock nuts behind the sheathing. The screws must be long enough to fully engage all threads on the nuts.

Concrete or Masonry Wall Construction

For concrete or masonry walls, use appropriate wall fasteners in all four mounting points.

- Concrete Screws on page 71
- Concrete Inserts on page 72

Concrete Screws

Concrete screws must be at least 3/16". Each of the four screws must be rated for 32.2 lb (14.6 kg) minimum.

Typical drill size is 5/32" for the 3/16" concrete screw. Follow the manufacturer's instructions, including the recommendation for drill depth.

Concrete Inserts

You can use concrete inserts, such as conical lead or flanged polypropylene, for installing the rack mount bracket in concrete. Each insert must be individually rated to support 32.2 lb (14.6 kg) minimum.

Use sizes that support a #10 screw minimum.

Typical drill size is 5/16" for the #10 conical lead anchor for concrete.

Typical drill size is 1/4" for the #10 flanged polypropylene anchor for concrete.

Follow the manufacturer"s instructions, including the recommendation for drill depth for the insert that you are using.

Mounting the PV-FC-180 Chassis on a Wall

To mount the PV-FC-180 chassis on a wall:

1 Using four customer-supplied screws and wall anchors, secure the mounting bracket to the wall. See Figure 33: Securing the Wall Mounting Bracket to a Wall on page 73.

The screws and wall anchors that you provide must be capable of supporting at least four times the combined weight of the PV-FC-180 chassis and two power supplies.

Note

You must secure the mounting bracket to the wall in the orientation shown in Figure 33: Securing the Wall Mounting Bracket to a Wall on page 73. No other orientation is supported.

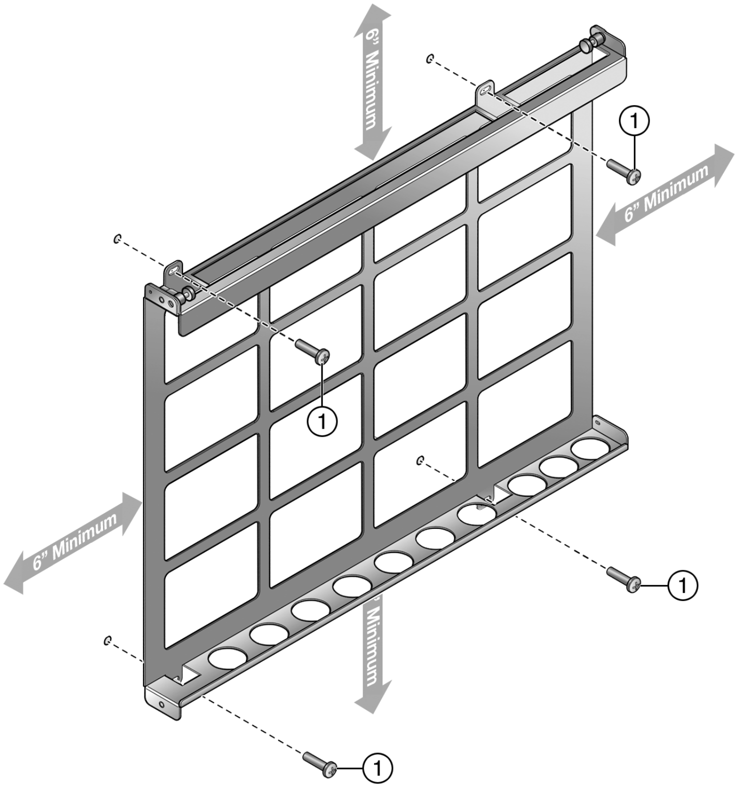


Figure 33: Securing the Wall Mounting Bracket to a Wall

1	Customer-supplied screws

2 Open the gate on the top side of the mounting bracket. See Figure 34: Opening the Gate on page 74.

a Pull the right and left plungers simultaneously to unlock the gate.

To lock the plungers in the open position, rotate the opened plungers counter-clockwise.

b Swing the gate into the open position.

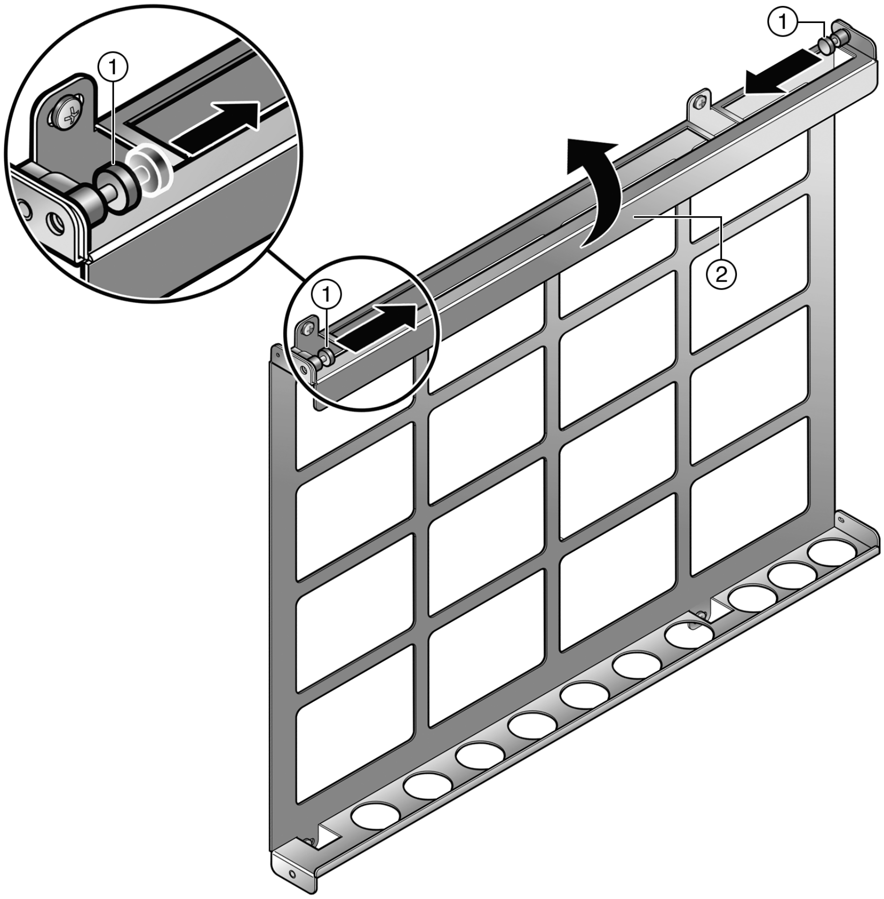


Figure 34: Opening the Gate

1	Right and left plungers	2	Gate

The following figure shows the gate in the open position.

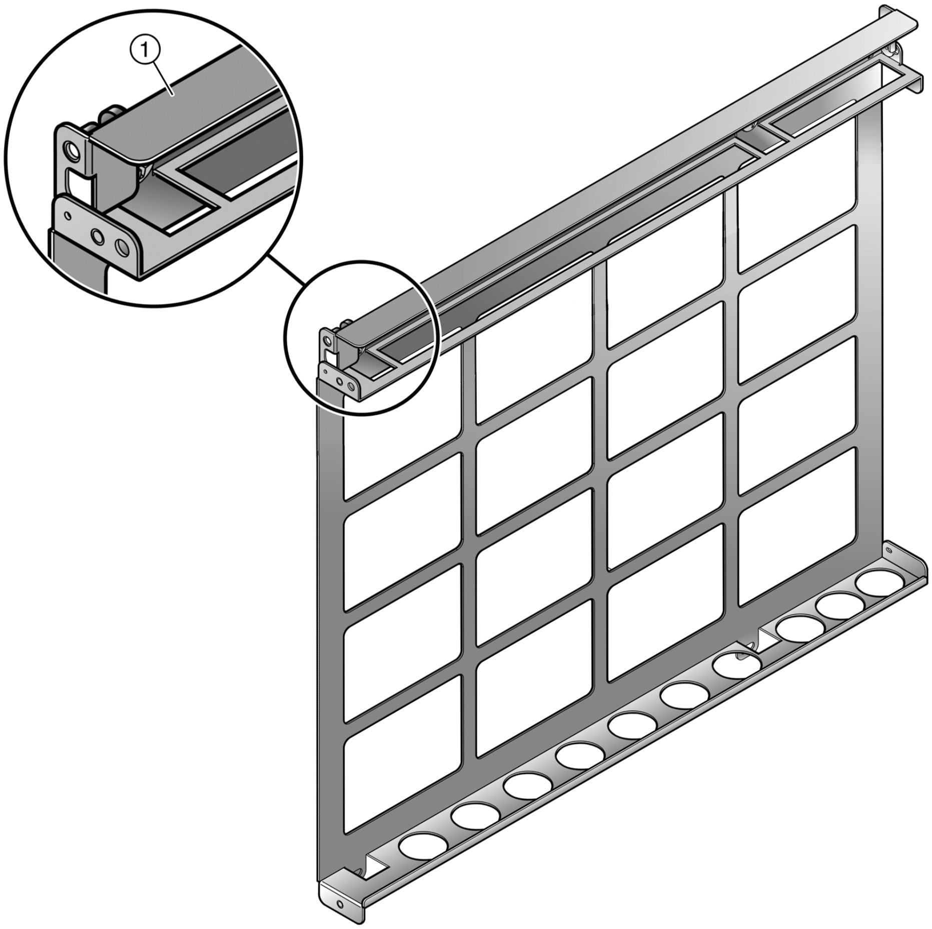


Figure 35: Mounting Bracket Gate in the Open Position

1	Gate in the open position

3 Holding the PV-FC-180 with the I/O connectors facing left, slide the bottom side of the PV-FC-180 chassis under the lip on the bottom side of the mounting bracket. See Figure 36: Installing the PV-FC-180 in the Mounting Bracket on page 76.

Note
You must install the PV-FC-180 chassis in the orientation shown in Figure 36: Installing the PV-FC-180 in the Mounting Bracket on page 76 (I/O connectors facing left, top of PV-FC-180 facing out). No other orientation of the PV-FC-180 chassis is supported.

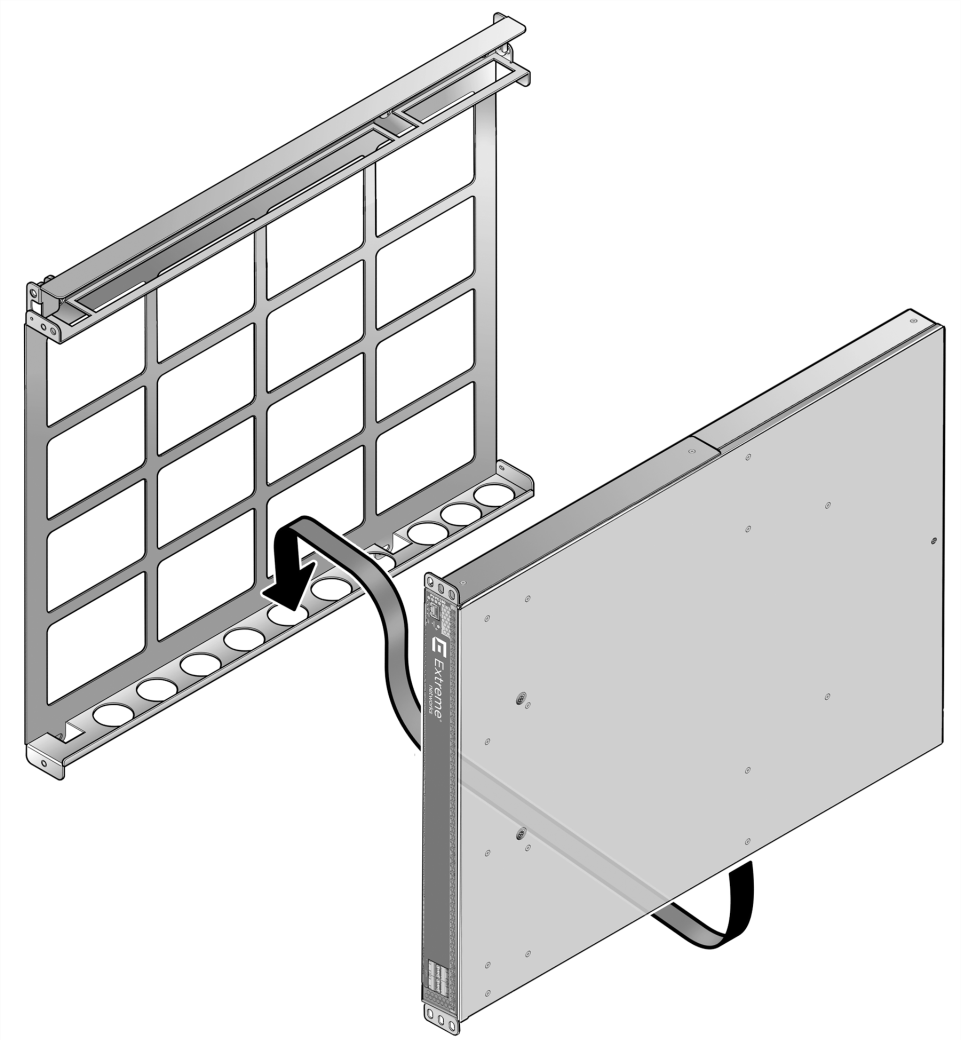


Figure 36: Installing the PV-FC-180 in the Mounting Bracket

4 Insert the top side of the PV-FC-180 chassis in the mounting bracket.

5 Close the gate to hold the PV-FC-180 chassis in place. See Figure 37: Closing the Gate on page 77.

Ensure that the plungers lock into place when you close the gate. If the plungers are in the open locked position, rotate the plungers clockwise until they unlock.

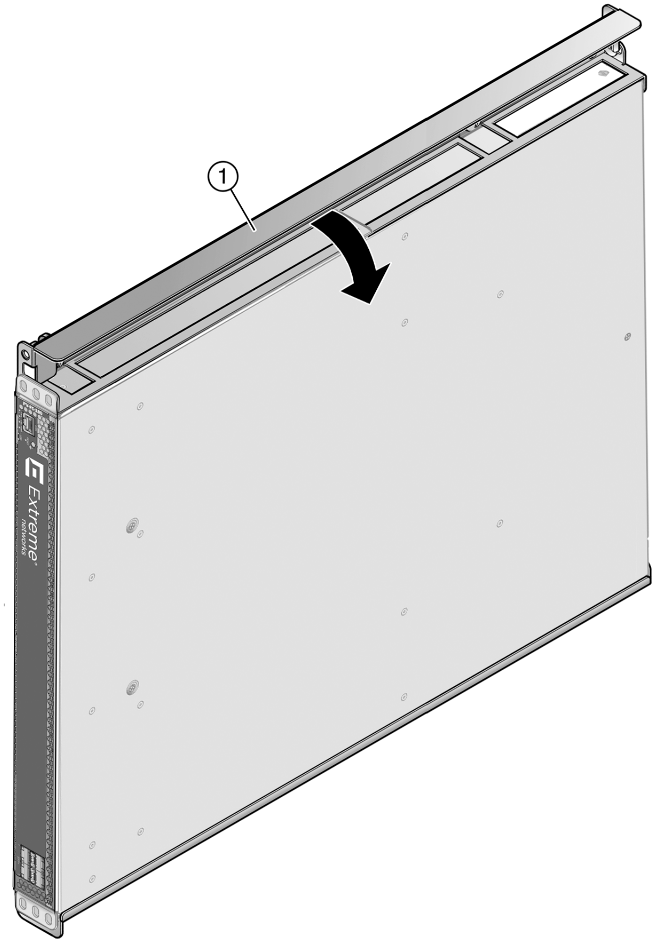


Figure 37: Closing the Gate

1	Gate

6 Using the 10-32 screws included with the mounting bracket, secure the front of the PV-FC-180 chassis to the left of the mounting bracket. See the following figure.

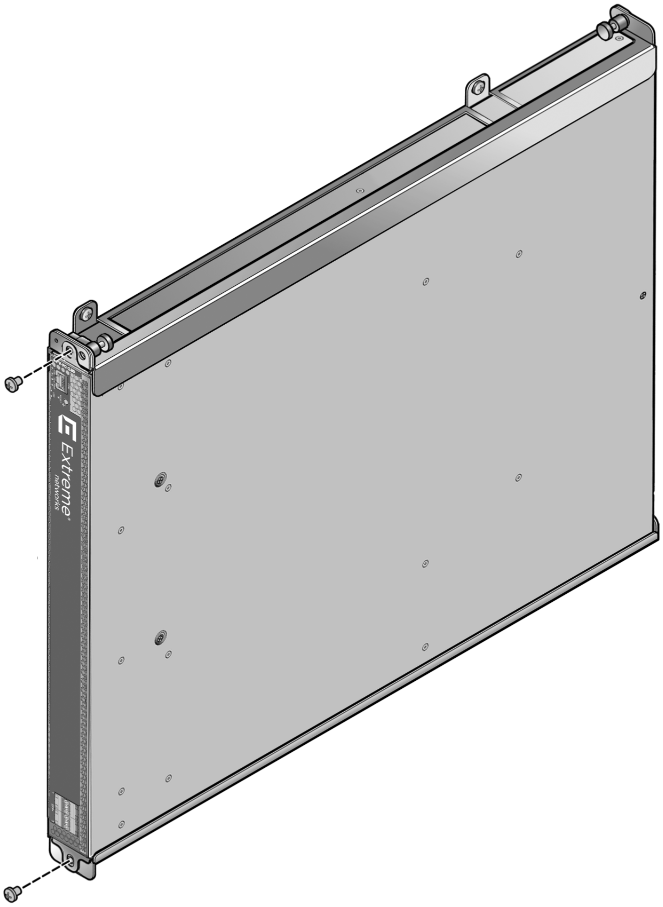


Figure 38: Securing the PV-FC-180 Chassis to the Mounting Bracket

You can now cable the I/O ports and power up the PV-FC-180 chassis as described in Installation on page 11.

E Environmental Guidelines

To ensure customer satisfaction and the continued reliable operation of our products, installation and operation must comply with the environmental guidelines as described in our product documentation. This document references limits on operating temperature and humidity. Failure to operate the equipment in these prescribed ranges can result in reduced performance and damaged equipment. Failure to comply with these limits and guidelines may void the product warranty and it may also exclude the equipment from support entitlements of any applicable maintenance contract agreements. The following information describes these limits and recommendations in further detail.

Temperature and Humidity Guidelines

Operating Temperatures

All equipment must operate within the prescribed temperature and humidity ranges specified in Extreme Networks documentation. Operation of the equipment outside these limits may result in damaged equipment and/or reduced performance and reliability. This may require reliable, monitored and 24x7 operation of climate control systems (heating and air conditioning).

Inlet Air Temperature Measurement

Operating temperature maximums and minimums are limits on the ambient air temperature entering the switching equipment. This area is located within one inch (1") of the main equipment inlet. This is not necessarily the same air temperature throughout the room.

Cooling Air

Many Extreme Networks switches utilize a side-to-side airflow method for cooling. Careful consideration is needed when mounting this equipment. Proper inlet and exit spaces must be allowed to get fresh, cool air into the equipment and to allow hot exhaust air to exit away from the equipment. Blocked venting can result in an overheating condition that can damage the equipment. Pay close attention to cable ingress and egress routing to verify that cabling is not blocking venting.

Power Conditioning

Extreme products are rated to be used with internationally accepted AC input parameters. It is important that these parameters are monitored and verified to operate as expected for the ratings that apply to the equipment installed. Surges and excessive noise outside of these prescribed ranges in the power circuits feeding this equipment may cause permanent damage to the equipment installed and must be monitored and prevented.

Airflow Concerns for Closed Racks

When placing Extreme switches into enclosed racks, rack exhaust fans must be considered if the rack does not contain adequate inlet and exit venting. These fans may be needed to help exhaust hot air from the rack. They must be sized properly to exhaust the collective volumetric flow from all equipment within the rack.

Figure 39: Closed Rack Ideal Configuration on page 80 illustrates the ideal configuration for a fully vented closed rack. All panels are vented, and side-to-side cooled sub-systems are flowing in the same direction.

Cool air ingress through the bottom of the rack must be carefully allowed to enhance overall system airflow and prevent stagnant air recirculation. This may need to be confirmed through thermal testing at the installation site.

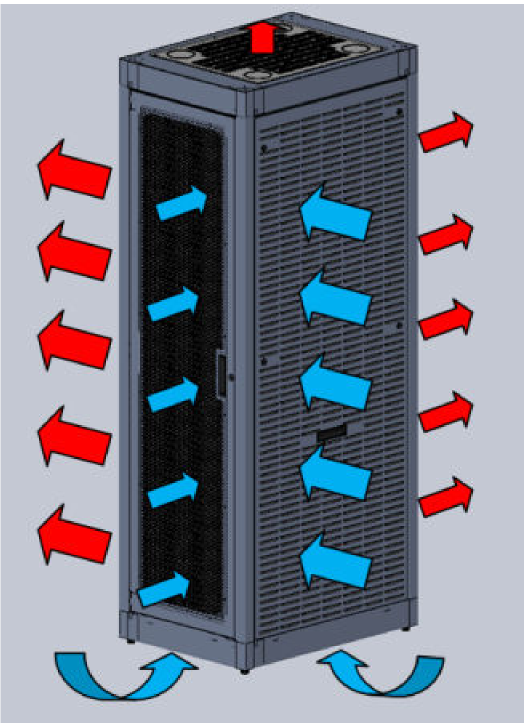


Figure 39: Closed Rack Ideal Configuration

Figure Key	
🟦	Blue arrows indicate cool air ingress
🟥	Red arrows indicate hot air egress
⇨	White arrows indicate airflow through the system

Airflow Concerns for Open Racks

Equipment with different air flow cooling patterns, such as front-to-back or side-to-side, can present special concerns. Recirculation of heated air through equipment is unwanted because it increases the inlet temperature, which causes the equipment components to operate at elevated temperatures. Likewise, equipment in neighboring racks must be planned to prevent hot air exhaust from one system being pulled into the inlet of an adjacent system.

The following figure illustrates the ideal configuration for an open rack. All sub-systems flow in the same direction, as shown by the white arrows.

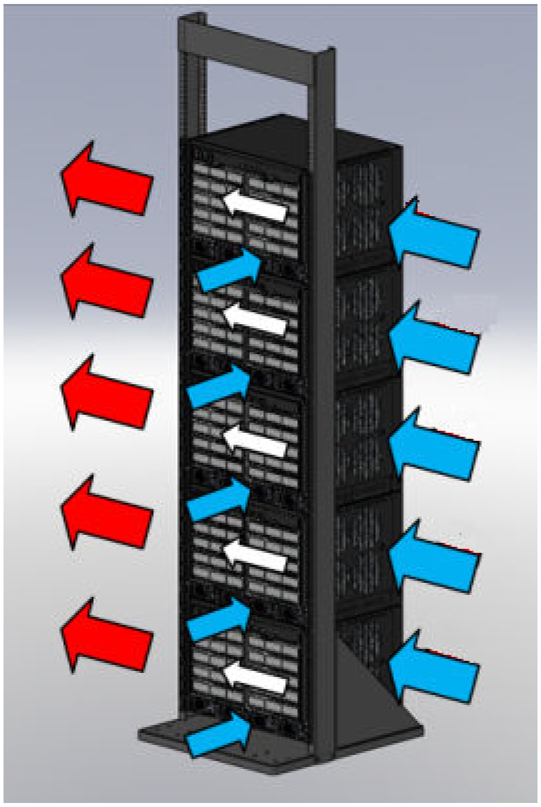


Figure 40: Open Rack Ideal Configuration

The figure below shows a non-ideal configuration for an open rack, where sub-systems with mixed flow directions (white arrows) are combined in one rack. Circular red arrows show potential for hot air recirculation.

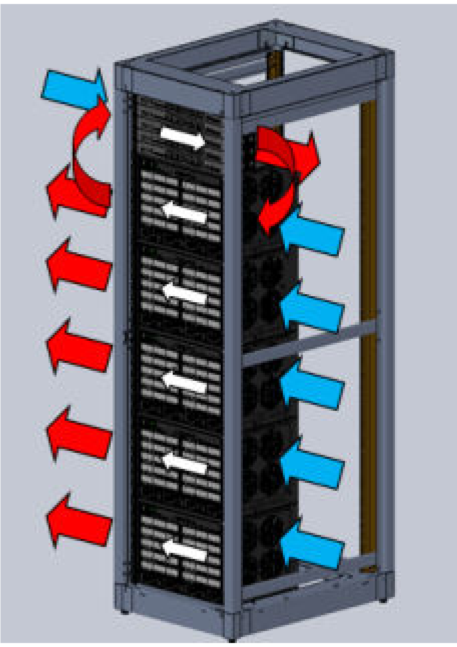


Figure 41: Non-ideal Open Rack Configuration

Non-ideal flows should be avoided or mitigated and confirmed through thermal testing.

The figure below shows a non-ideal open rack configuration containing sub-systems with mixed flow directions (white arrows). This configuration shows mitigation of potential hot air recirculation by leaving a gap in the rack population.

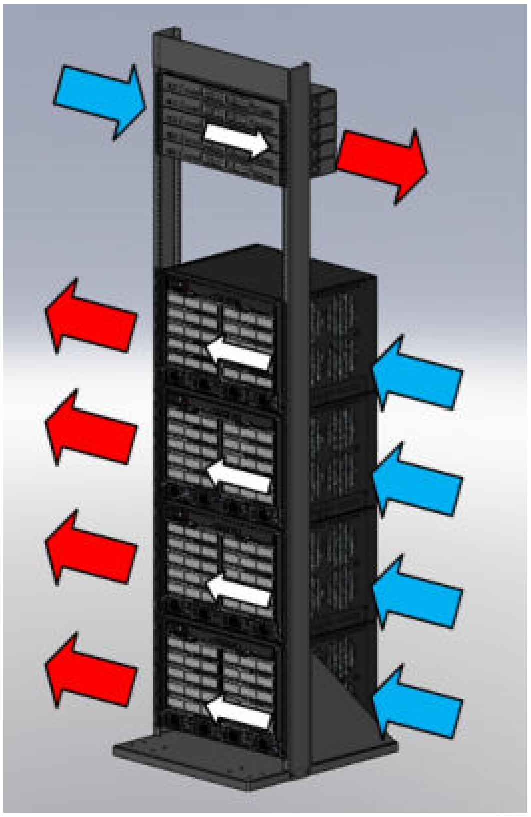


Figure 42: Mitigated Non-ideal Open Rack Configuration

The following figure shows another mitigation strategy for open racks containing sub-systems with mixed flow direction. Mitigation of potential hot air recirculation is achieved by separating unlike systems with products having front- to-back airflow patterns.

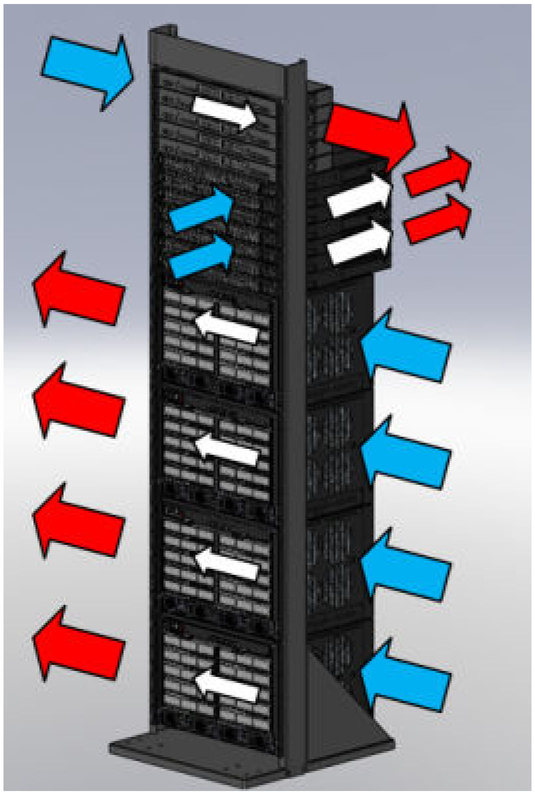


Figure 43: Another Mitigated Non-ideal Open Rack Configuration

Dust Mitigation and Prevention

Dust accumulation on inlet and exit venting is not uncommon after prolonged use. In dustier environments this accumulation can be much quicker.

We strongly recommend routine maintenance to check for clean inlet and exit vents on this equipment. Over time, dust accumulation can create vent blockages, thereby decreasing airflow and increasing component temperatures, resulting in reduced reliability. Recommended maintenance should start with monthly inspections and be adjusted based on dust accumulation levels.

The following table notes the maximum dust and debris accumulation limits for room environments as a reference.

Table 20: Airborne Dust Specification for Extreme Networks Equipment — Airborne Dust Maximum Values

Dust	Guidelines
All/Total Airborne Particles (TSP-Dichot 15): (see note 1)	20 µg/m^3 (see note 3)
PM10/Coarse Particles (2.5 to 15 microns): (see notes 2 & 3)	Preferred: <10 µg/m^3 (see note 2) Maximum: 20 µg/m3 (see note 3)
PM2.5/Fine particles (< 2.5 microns) (see note 2):	10 µg/m^3
1 TSP-Dichot 15 = Total Suspended Particulates as determined using a Dichotomous sampler with a 15 micron inlet	

Table 20: Airborne Dust Specification for Extreme Networks Equipment — Airborne Dust Maximum Values (continued)

Dust	Guidelines
2 Recommended value by WHO (World Health Organization) for 2005 air quality.	
3 Value from NEBs GR-63-CORE issue #3 table 4-12.	

Note
The equipment will operate at higher levels than listed above. However, the higher levels can decrease the products' service life.

Dust removal from the equipment is a required part of maintenance. When removing dust:

- Use proper ESD precautions.
- Use a vacuum that is properly grounded through a cord having an equipment-grounding conductor and grounding plug.
- Carefully vacuum the dust particles from the inlet and exit venting of the equipment to allow for proper air flow and ventilation.

Please contact Extreme Networks Technical Support for additional information about external filter options.

Airborne Chemicals and Prevention

Various airborne chemicals and contaminants can cause corrosion and thus decrease the service life of most vendors' equipment. To reduce the risk of such corrosion, locate the equipment only in areas that are safe for human occupation.

For more product information and documentation, go to: http://support.extremenetworks.com/

F Regulatory Compliance Information

Safety Information

Federal Communications Commission (FCC) Notice

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note
This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

Warning
Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada Notice

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Class A ITE Notice

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

Clase A. Aviso de ITE

ADVERTENCIA: Este es un producto de Clase A. En un ambiente doméstico este producto puede causar interferencia de radio en cuyo caso puede ser requerido tomar medidas adecuadas

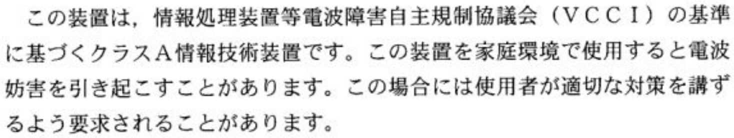
.

Klasse A ITE Anmerkung

WARNHINWEIS: Dieses Produkt zählt zur Klasse A (Industriebereich). In Wohnbereichen kann es hierdurch zu Funkstörungen kommen, daher sollten angemessene Vorkehrungen zum Schutz getroffen werden.

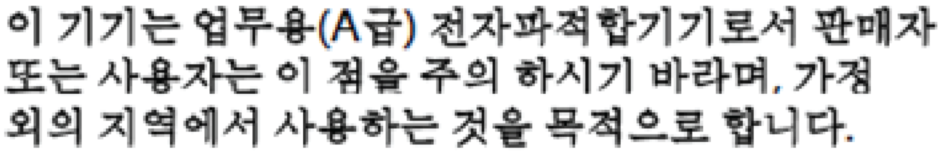
VCCI Notice

This is a class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.



この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

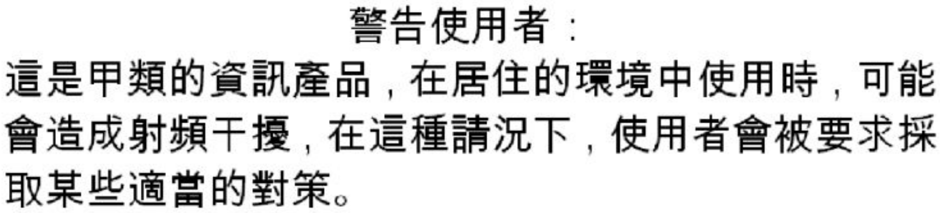
Korea EMC Statement



이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의 하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

BSMI EMC Statement — Taiwan

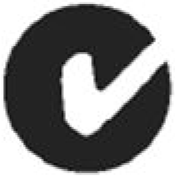
This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures



警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

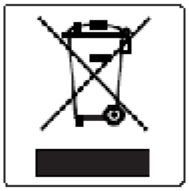
AS/NZS CISPR 22



Hazardous Substances

This product complies with the requirements of Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

European Waste Electrical and Electronic Equipment (WEEE) Notice



In accordance with Directive 2012/19/EU of the European Parliament on waste electrical and electronic equipment (WEEE):

1 The symbol above indicates that separate collection of electrical and electronic equipment is required.

2 When this product has reached the end of its serviceable life, it cannot be disposed of as unsorted municipal waste. It must be collected and treated separately.

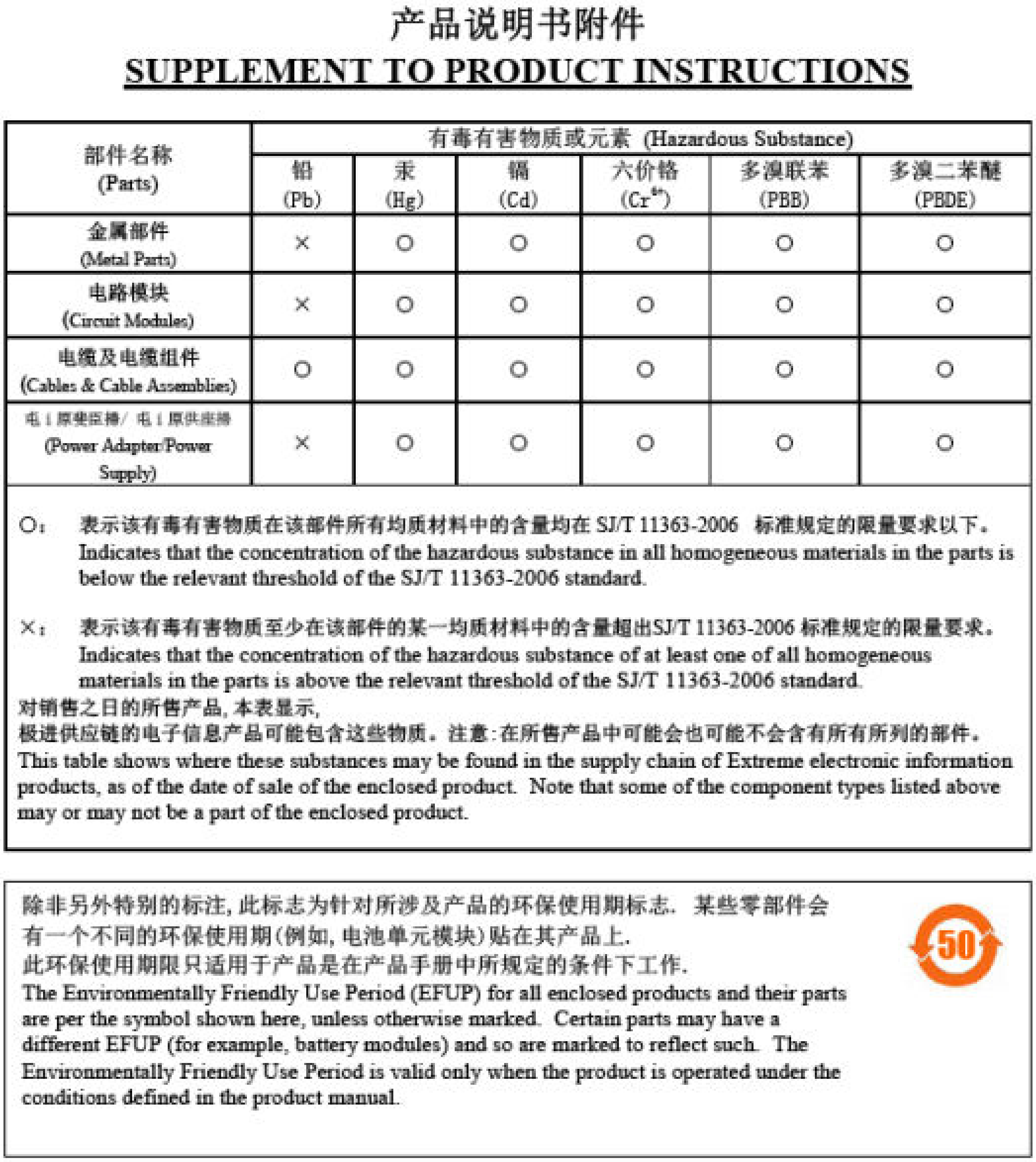
3 It has been determined by the European Parliament that there are potential negative effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment.

4 It is the users' responsibility to utilize the available collection system to ensure WEEE is properly treated. For information about the available collection system, please contact Extreme Customer Support at +353 61 705500 (Ireland).

Battery Notice

This product contains a battery used to maintain product information. If the battery should need replacement it must be replaced by Service Personnel. Please contact Technical Support for assistance.

⚠	CAUTION
	There is an explosion risk if you replace the battery with the incorrect type. Dispose of expended battery in accordance with local disposal regulations.
	PRECAUCIÓN
	Hay riesgo de explosion si la bateria se reemplaza con el typo incorrecto. Deshágase de las baterías gastadas de conformidad con las regulaciones de eliminación local.



产品说明书附件

SUPPLEMENT TO PRODUCT INSTRUCTIONS

部件名称 (Parts)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 (Metal Parts)	×	○	○	○	○	○
电路模块 (Circuit Modules)	×	○	○	○	○	○
电缆及电缆组件 (Cables & Cable Assemblies)	○	○	○	○	○	○
电源适配器/电源供应器 (Power Adapter/Power Supply)	×	○	○	○	○	○

○： 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。
Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T 11363-2006 standard.

×： 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006 标准规定的限量要求。
Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T 11363-2006 standard.

对销售之日的所售产品, 本表显示,
极进供应链的电子信息产品可能包含这些物质。注意:在所售产品中可能会也可能不会含有所有所列的部件。
This table shows where these substances may be found in the supply chain of Extreme electronic information products, as of the date of sale of the enclosed product. Note that some of the component types listed above may or may not be a part of the enclosed product.

除非另外特别的标注, 此标志为针对所涉及产品的环保使用期标志. 某些零部件会有一个不同的环保使用期(例如, 电池单元模块)贴在其产品上.
此环保使用期限只适用于产品是在产品手册中所规定的条件下工作.
The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain parts may have a different EFUP (for example, battery modules) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

Safety Information

⚠	ELECTRICAL HAZARD
	Only qualified personnel should install or service this unit.
	RIESGO ELECTRICO
	Nada mas personal capacitado debe de instalar o darle servicio a esta unida.
	ELEKTRISCHER GEFAHRENHINWEIS
	Installationen oder Servicearbeiten sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.
	RISQUES D'ÉLECTROCUTION
	Seul un personnel qualifié doit installer ou effectuer les opérations de maintenance sur cet élément.

Class 1 Laser Transceivers, Laser Radiation and Connectors

When the connector is in place, all laser radiation remains within the fiber. The maximum amount of radiant power exiting the fiber (under normal conditions) is -12.6 dBm or 55 x 10-6 watts. Removing the optical connector from the transceiver allows laser radiation to emit directly from the optical port. The maximum radiance from the optical port (under worst case conditions) is 0.8 W cm-2 or 8 x 103 W m2 sr-1.

Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, power must be removed from the network adapter.

Safety Compliance

Warning: Fiber Optic Port Safety	
CLASS I LASER DEVICE	When using a fiber optic media expansion module, never look at the transmit laser while it is powered on. Also, never look directly at the fiber TX port and fiber cable ends when they are powered on.
Avertissment: Ports pour fibres optiques - sécurité sur le plan optique	
DISPOSITIF LASER DE CLASSE I	Ne regardez jamais le laser tant qu'il est sous tension. Ne regardez jamais directement le port TX (Tramsmission) à fibres optiques et les embouts de câbles à fibres optiques tant qu'ils sont sous tension.
Warnhinweis: Faseroptikanschlüsse - Optische Sicherheit	
LASERGERÄT DER KLASSE I	Niemals ein Übertragungslaser betrachten, während dieses eingeschaltet ist. Niemals direkt auf den Faser-TX-Anschluß und auf die Faserkabelenden schauen, während diese eingeschaltet sind.

G Glossary

A
B
C
D
E
F
G
H
I
J
L
M
N
O
P
Q
R
S
T
U
V
W
X

A

AAA

Authentication, authorization, and accounting. A system in IP-based networking to control which computer resources specific users can access and to keep track of the activity of specific users over the network.

ABR

Area border router. In OSPF, an ABR has interfaces in multiple areas, and it is responsible for exchanging summary advertisements with other ABRs.

ACL

Access Control List. A mechanism for filtering packets at the hardware level. Packets can be classified by characteristics such as the source or destination MAC, IP addresses, IP type, or QoS queue. Once classified, the packets can be forwarded, counted, queued, or dropped.

ACMI

Asynchronous Chassis Management Interface.

ad-hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP).

AES

Advanced Encryption Standard. AES is an algorithm for encryption that works at multiple network layers simultaneously. As a block cipher, AES encrypts data in fixed-size blocks of 128 bits; AES is also a privacy transform for IPSec and Internet Key Exchange (IKE). Created by the National Institute of Standards and Technology (NIST), the standard has a variable key length—it can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

For the WPA2/802.11i implementation of AES, a 128-bit key length is used. AES encryption includes four stages that make up one round. Each round is then iterated 10, 12, or 14 times depending upon the bit-key size. For the WPA2/802.11i implementation of AES, each round is iterated 10 times.

AES-CCMP

Advanced Encryption Standard - Counter-Mode/CBC-MAC Protocol. CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include Counter mode (CTR) that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.

alternate port

In RSTP, the alternate port supplies an alternate path to the root bridge and the root port.

AP (access point)

In wireless technology, access points are LAN transceivers or "base stations" that can connect to the regular wired network and forward and receive the radio signals that transmit wireless data.

area

In OSPF, an area is a logical set of segments connected by routers. The topology within an area is hidden from the rest of the autonomous system (AS).

ARP

Address Resolution Protocol. ARP is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

AS

Autonomous system. In OSPF, an AS is a connected segment of a network topology that consists of a collection of subnetworks (with hosts attached) interconnected by a set of routes. The subnetworks and the routers are expected to be under the control of a single administration. Within an AS, routers may use one or more interior routing protocols and sometimes several sets of metrics. An AS is expected to present to other autonomous systems an appearance of a coherent interior routing plan and a consistent picture of the destinations reachable through the AS. An AS is identified by a unique 16-bit number.

ASBR

Autonomous system border router. In OSPF, an ASBR acts as a gateway between OSPF and other routing protocols or other autonomous systems.

association

A connection between a wireless device and an access point.

asynchronous

See ATM.

ATM

Asynchronous transmission mode. A start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

autobind

In STP, autobind (when enabled) automatically adds or removes ports from the STPD. If ports are added to the carrier VLAN, the member ports of the VLAN are automatically added to the STPD. If ports are removed from the carrier VLAN, those ports are also removed from the STPD.

autonegotiation

As set forth in IEEE 802.3u, autonegotation allows each port on the switch—in partnership with its link partner—to select the highest speed between 10 Mbps and 100 Mbps and the best duplex mode.

B

backbone area

In OSPF, a network that has more than one area must have a backbone area, configured as 0.0.0.0. All areas in an autonomous system (AS) must connect to the backbone area.

backup port

In RSTP, the backup port supports the designated port on the same attached LAN segment. Backup ports exist only when the bridge is connected as a self-loop or to a shared media segment.

backup router

In VRRP, the backup router is any VRRP router in the VRRP virtual router that is not elected as the master. The backup router is available to assume forwarding responsibility if the master becomes unavailable.

BDR

Backup designated router. In OSPF, the system elects a designated router (DR) and a BDR. The BDR smooths the transition to the DR, and each multi-access network has a BDR. The BDR is adjacent to all routers on the network and becomes the DR when the previous DR fails. The period of disruption in transit traffic lasts only as long as it takes to flood the new LSAs (which announce the new DR). The BDR is elected by the protocol; each hello packet has a field that specifies the BDR for the network.

BGP

Border Gateway Protocol. BGP is a router protocol in the IP suite designed to exchange network reachability information with BGP systems in other autonomous systems. You use a fully meshed configuration with BGP.

BGP provides routing updates that include a network number, a list of ASs that the routing information passed through, and a list of other path attributes. BGP works with cost metrics to choose the best available path; it sends updated router information only when one host has detected a change, and only the affected part of the routing table is sent.

BGP communicates within one AS using Interior BGP (IBGP) because BGP does not work well with IGP. Thus the routers inside the AS maintain two routing tables: one for the IGP and one for IBGP. BGP uses exterior BGP (EBGP) between different autonomous systems.

bi-directional rate shaping

A hardware-based technology that allows you to manage bandwidth on Layer 2 and Layer 3 traffic flowing to each port on the switch and to the backplane, per physical port on the I/O module. The parameters differ across platforms and modules.

blackhole

In the Extreme Networks implementation, you can configure the switch so that traffic is silently dropped. Although this traffic appears as received, it does not appear as transmitted (because it is dropped).

BOOTP

Bootstrap Protocol. BOOTP is an Internet protocol used by a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file that can be loaded into memory to boot the machine. Using BOOTP, a workstation can boot without a hard or floppy disk drive.

BPDU

Bridge protocol data unit. In STP, a BPDU is a packet that initiates communication between devices. BPDU packets contain information on ports, addresses, priorities, and costs and they ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

bridge

In conventional networking terms, bridging is a Layer 2 function that passes frames between two network segments; these segments have a common network layer address. The bridged frames pass only to those segments connected at a Layer 2 level, which is called a broadcast domain (or VLAN). You must use Layer 3 routing to pass frames between broadcast domains (VLANs).

In wireless technology, bridging refers to forwarding and receiving data between radio interfaces on APs or between clients on the same radio. So, bridged traffic can be forwarded from one AP to another AP without having to pass through the switch on the wired network.

broadcast

A broadcast message is forwarded to all devices within a VLAN, which is also known as a broadcast domain. The broadcast domain, or VLAN, exists at a Layer 2 level; you must use Layer 3 routing to communicate between broadcast domains, or VLANs. Thus, broadcast messages do not leave the VLAN. Broadcast messages are identified by a broadcast address.

BSS

Basic Service Set. A wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also IBSS.

C

captive portal

A browser-based authentication mechanism that forces unauthenticated users to a web page.

carrier VLAN

In STP, carrier VLANs define the scope of the STPD, including the physical and logical ports that belong to the STPD as well as the 802.1Q tags used to transport EMISTP- or PVST+-encapsulated BPDUs. Only one carrier VLAN can exist in any given STPD.

CCM

In CFM, connectivity check messages are CFM frames transmitted periodically by a MEP to ensure connectivity across the maintenance entities to which the transmitting MEP belongs. The CCM messages contain a unique ID for the specified domain. Because a failure to receive a CCM indicates a connectivity fault in the network, CCMs proactively check for network connectivity.

CDR

Call Data (Detail) Record

. In Internet telephony, a call detail record is a data record that contains information related to a telephone call, such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call, the time of day the call was made and any toll charges that were added through the network or charges for operator services, among other details of the call.

In essence, call accounting is a database application that processes call data from your switch (PBX, iPBX, or key system) via a CDR (call detail record) or SMDR (station message detail record) port. The call data record details your system's incoming and outgoing calls by thresholds, including time of call, duration of call, dialing extension, and number dialed. Call data is stored in a PC database.

CEP

Customer Edge Port. Also known as Selective Q-in-Q or C-tagged Service Interface. CEP is a role that is configured in software as a CEP VMAN port, and connects a VMAN to specific CVLANs based on the CVLAN CVID. The CNP role, which is configured as an untagged VMAN port, connects a VMAN to all other port traffic that is not already mapped to the port CEP role.

CA certificate

A certificate identifying a certificate authority. A CA certificate can be used to verify that a certificate issued by the certificate authority is legitimate.

certificate

A document that identifies a server or a client (user), containing a public key and signed by a certificate authority.

Certificate Authority (CA)

A trusted third-party that generates and signs certificates. A CA may be a commercial concern, such as GoDaddy or GeoTrust. A CA may also be an in-house server for certificates used within an enterprise.

certificate chain

An ordered set of certificates which can be used to verify the identity of a server or client. It begins with a client or server certificate, and ends with a certificate that is trusted.

certificate issuer

The certificate authority that generated the certificate.

Certificate Signing Request (CSR)

A document containing identifiers, options, and a public key, that is sent to a certificate authority in order to generate a certificate.

certificate subject

The server or client identified by the certificate.

client certificate

A certificate identifying a client (user). A client certificate can be used in conjunction with, or in lieu of, a username and password to authenticate a client.

CFM

Connectivity Fault Management allows an ISP to proactively detect faults in the network for each customer service instance individually and separately. CFM comprises capabilities for detecting, verifying, and isolating connectivity failures in virtual bridged LANs.

Chalet

A web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol. One of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure than because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

checkpointing

Checkpointing is the process of copying the active state configurations from the primary MSM to the backup MSM on modular switches.

CIDR

Classless Inter-Domain Routing. CIDR is a way to allocate and specify the Internet addresses used in interdomain routing more flexibly than with the original system of IP address classes. This address aggregation scheme uses supernet addresses to represent multiple IP destinations. Rather than advertise a separate route for each destination, a router uses a supernet address to advertise a single route representing all destinations. RIP does not support CIDR; BGP and OSPF support CIDR.

CIST

Common and Internal Spanning Tree. In an MSTP environment, the CIST is a single spanning tree domain that connects MSTP regions. The CIST is responsible for creating a loop-free topology by exchanging and propagating BPDUs across MSTP regions. You can configure only one CIST on each switch.

CIST regional root bridge

Within an MSTP region, the bridge with the lowest path cost to the CIST root bridge is the CIST regional root bridge If the CIST root bridge is inside an MSTP region, that same bridge is the CIST regional root for that region because it has the lowest path cost to the CIST root. If the CIST root bridge is outside an MSTP region, all regions connect to the CIST root through their respective CIST regional roots.

CIST root bridge

In an MSTP environment, the bridge with the lowest bridge ID becomes the CIST root bridge. The bridge ID includes the bridge priority and the MAC address. The CIST root bridge can be either inside or outside an MSTP region. The CIST root bridge is unique for all regions and non-MSTP bridges, regardless of its location.

CIST root port

In an MSTP environment, the port on the CIST regional root bridge that connects to the CIST root bridge is the CIST root port. The CIST root port is the master port for all MSTIs in that MSTP region, and it is the only port that connects the entire region to the CIST root bridge.

CLEAR-flow

CLEAR-Flow allows you to specify certain types of traffic to perform configured actions on. You can configure the switch to take an immediate, preconfigured action to the specified traffic or to send a copy of the traffic to a management station for analysis. CLEAR-Flow is an extension to ACLs, so you must be familiar with ACL policy files to apply CLEAR-Flow.

CLI

Command line interface. You can use the CLI to monitor and manage the switch or wireless appliance.

cluster

In BGP, a cluster is formed within an AS by a route reflector and its client routers.

collision

Two Ethernet packets attempting to use the medium simultaneously. Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. When two nodes at different locations attempt to send data at the same time, a collision will result. Segmenting the network with bridges or switches is one way of reducing collisions in an overcrowded network.

CNA

Converged Network Analyzer. This application suite, available from Avaya, allows the server to determine the best possible network path. The CNA Agent is a software piece of the entire CNA application that you install on Extreme Networks devices. You use the CNA Agent software only if you are using the Avaya CNA solution, and the CNA Agent cannot function unless you also obtain the rest of the CNA application from Avaya.

CNP

Customer Network Port.

combo port

Also known as a *combination port*. On some Extreme Networks devices (such as the Summit X450 a-series switch), certain ports can be used as either copper or fiber ports.

combo link

In EAPS, the common link is the physical link between the controller and partner nodes in a network where multiple EAPS share a common link between domains.

control VLAN

In EAPS, the control VLAN is a VLAN that sends and receives EAPS messages. You must configure one control VLAN for each EAPS domain.

controller node

In EAPS, the controller node is that end of the common line that is responsible for blocking ports if the common link fails, thereby preventing a superloop.

CoS

Class of Service. Specifying the service level for the classified traffic type. For more information, see QoS in the *ExtremeXOS User Guide*.

CRC

Cyclic Redundancy Check. This simple checksum is designed to detect transmission errors. A decoder calculates the CRC for the received data and compares it to the CRC that the encoder calculated, which is appended to the data. A mismatch indicates that the data was corrupted in transit.

CRC error

Cyclic redundancy check error. This is an error condition in which the data failed a checksum test used to trap transmission errors. These errors can indicate problems anywhere in the transmission path.

CSPF

Constrained shortest path first. An algorithm based on the shortest path first algorithm used in OSPF, but with the addition of multiple constraints arising from the network, the LSP, and the links. CSPF is used to minimize network congestion by intelligently balancing traffic.

CVID

CVLAN ID. The CVID represents the CVLAN tag for tagged VLAN traffic. (See CVLAN.)

CVLAN

Customer VLAN.

D

DAD

Duplicate Address Detection. IPv6 automatically uses this process to ensure that no duplicate IP addresses exist. For more information, see Duplicate Address Detection in the *ExtremeXOS User Guide*.

datagram

See packet.

dBm

An abbreviation for the power ratio in decibels (dB) of the measured power referenced to one milliwatt.

DCB

Data Center Bridging is a set of IEEE 802.1Q extensions to standard Ethernet, that provide an operational framework for unifying Local Area Networks (LAN), Storage Area Networks (SAN) and Inter-Process Communication (IPC) traffic between switches and endpoints onto a single transport layer.

DCBX

The Data Center Bridging eXchange protocol is used by DCB devices to exchange DCB configuration information with directly connected peers.

decapsulation

See tunelling.

default encapsulation mode

In STP, default encapsulation allows you to specify the type of BPDU encapsulation to use for all ports added to a given STPD, not just to one individual port. The encapsulation modes are:

- 802.1d—This mode is used for backward compatibility with previous STP versions and for compatibility with third-party switches using IEEE standard 802.1d.
- EMISTP—Extreme Multiple Instance Spanning Tree Protocol (EMISTP) mode is an extension of STP that allows a physical port to belong to multiple STPDs by assigning the port to multiple VLANs.
- PVST+—This mode implements PVST+ in compatibility with third-party switches running this version of STP.

designated port

In STP, the designated port provides the shortest path connection to the root bridge for the attached LAN segment. Each LAN segment has only one designated port.

destination address

The IP or MAC address of the device that is to receive the packet.

Device Manager

The Device Manager is an Extreme Networks-proprietary process that runs on every node and is responsible for monitoring and controlling all of the devices in the system. The Device Manager is useful for system redundancy.

device server

A specialized, network-based hardware device designed to perform a single or specialized set of server functions. Print servers, terminal servers, remote access servers, and network time servers are examples of device servers.

DF

Don't fragment bit. This is the don't fragment bit carried in the flags field of the IP header that indicates that the packet should not be fragmented. The remote host will return ICMP notifications if the packet had to be split anyway, and these are used in MTU discovery.

DHCP

Dynamic Host Configuration Protocol. DHCP allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DiffServ

Differentiated Services. Defined in RFC 2474 and 2475, DiffServ is an architecture for implementing scalable service differentiation in the Internet. Each IP header has a DiffServ (DS) field, formerly known as the Type of Service (TOS) field. The value in this field defines the QoS priority the packet will have throughout the network by dictating the forwarding treatment given to the packet at each node.

DiffServ is a flexible architecture that allows for either end-to-end QoS or intra-domain QoS by implementing complex classification and mapping functions at the network boundary or access points. In the Extreme Networks implementation, you can configure the desired QoS by replacing or mapping the values in the DS field to egress queues that are assigned varying priorities and bandwidths.

directory agent (DA)

A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices. With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'.

The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.
For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.
(SLP version 2, RFC 2608, updating RFC 2165)

diversity antenna and receiver

The AP has two antennae. Receive diversity refers to the ability of the AP to provide better service to a device by receiving from the user on which ever of the two antennae is receiving the cleanest signal. Transmit diversity refers to the ability of the AP to use its two antenna to transmit on a specific antenna only, or on a alternate antennae. The antennae are called diversity antennae because of this capability of the pair.

DNS

Domain Name Server. This system is used to translate domain names to IP addresses. Although the Internet is based on IP addresses, names are easier to remember and work with. All these names must be translated back to the actual IP address and the DNS servers do so.

domain

In CFM, a maintenance domain is the network, or part of the network, that belongs to a single administration for which connectivity faults are managed.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks. For more information, see DoS Protection in the *ExtremeXOS User Guide*.

DR

Designated router. In OSPF, the DR generates an LSA for the multi-access network and has other special responsibilities in the running of the protocol. The DR is elected by the OSPF protocol.

DSSS

Direct-Sequence Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with FHSS.)

DTIM

DTIM delivery traffic indication message (in 802.11 standard).

dynamic WEP

The IEEE introduced the concept of user-based authentication using per-user encryption keys to solve the scalability issues that surrounded static WEP. This resulted in the 802.1x standard, which makes use of the IETF's Extensible Authentication Protocol (EAP), which was originally designed for user authentication in dial-up networks. The 802.1x standard supplemented the EAP protocol with a mechanism to send an encryption key to a Wireless AP. These encryption keys are used as dynamic WEP keys, allowing traffic to each individual user to be encrypted using a separate key.

E

EAPS

Extreme Automatic Protection Switching. This is an Extreme Networks-proprietary version of the Ethernet Automatic Protection Switching protocol that prevents looping Layer 2 of the network. This feature is discussed in RFC 3619.

EAPS domain

An EAPS domain consists of a series of switches, or nodes, that comprise a single ring in a network. An EAPS domain consists of a master node and transit nodes. The master node consists of one primary and one secondary port. EAPS operates by declaring an EAPS domain on a single ring.

EAPS link ID

Each common link in the EAPS network must have a unique link ID. The controller and partner shared ports belonging to the same common link must have matching link IDs, and not other instance in the network should have that link ID.

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.
EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also PEAP.)

EBGP

Exterior Border Gateway Protocol. EBGP is a protocol in the IP suite designed to exchange network reachability information with BGP systems in other autonomous systems. EBGP works between different ASs.

ECMP

Equal Cost Multi Paths. This routing algorithm distributes network traffic across multiple high-bandwidth OSPF, BGP, IS-IS, and static routes to increase performance. The Extreme Networks implementation supports multiple equal cost paths between points and divides traffic evenly among the available paths.

edge ports

In STP, edge ports connect to non-STP devices such as routers, endstations, and other hosts.

edge safeguard

Loop prevention and detection on an edge port configured for RSTP is called *edge safeguard*. Configuring edge safeguard on RSTP edge ports can prevent accidental or deliberate misconfigurations (loops) resulting from connecting two edge ports together or from connecting a hub or other non-STP switch to an edge port. Edge safeguard also limits the impact of broadcast storms that might occur on edge ports. This advanced loop prevention mechanism improves network resiliency but does not interfere with the rapid convergence of edge ports. For more information about edge safeguard, see Configuring Edge Safeguard in the *ExtremeXOS User Guide*.

EDP

Extreme Discovery Protocol. EDP is a protocol used to gather information about neighbor Extreme Networks switches. Extreme Networks switches use EDP to exchange topology information.

EEPROM

Electrically erasable programmable read-only memory. EEPROM is a memory that can be electronically programmed and erased but does not require a power source to retain data.

EGP

Exterior Gateway Protocol. EGP is an Internet routing protocol for exchanging reachability information between routers in different autonomous systems. BGP is a more recent protocol that accomplishes this task.

election algorithm

In ESRP, this is a user-defined criteria to determine how the master and slave interact. The election algorithm also determines which device becomes the master or slave and how ESRP makes those decisions.

ELRP

Extreme Loop Recovery Protocol. ELRP is an Extreme Networks-proprietary protocol that allows you to detect Layer 2 loops.

ELSM

Extreme Link Status Monitoring. ELSM is an Extreme Networks-proprietary protocol that monitors network health. You can also use ELSM with Layer 2 control protocols to improve Layer 2 loop recovery in the network.

EMISTP

Extreme Multiple Instance Spanning Tree Protocol. This Extreme Networks-proprietary protocol uses a unique encapsulation method for STP messages that allows a physical port to belong to multiple STPDs.

EMS

Event Management System. This Extreme Networks-proprietary system saves, displays, and filters events, which are defined as any occurrences on a switch that generate a log message or require action.

encapsulation mode

Using STP, you can configure ports within an STPD to accept specific BPDU encapsulations. The three encapsulation modes are:

- 802.1D—This mode is used for backward compatibility with previous STP versions and for compatibility with third-party switches using IEEE standard 802.1D.
- EMISTP—Extreme Multiple Instance Spanning Tree Protocol mode is an extension of STP that allows a physical port to belong to multiple STPDs by assigning the port to multiple VLANs.
- PVST+—This mode implements PVST+ in compatibility with third-party switches running this version of STP.

EPICenter

See Ridgeline.

ESRP

Extreme Standby Router Protocol. ESRP is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

ESRP-aware device

This is an Extreme Networks device that is not running ESRP itself but that is connected on a network with other Extreme Networks switches that are running ESRP. These ESRP-aware devices also fail over.

ESRP domain

An ESRP domain allows multiple VLANs to be protected under a single logical entity. An ESRP domain consists of one domain-master VLAN and zero or more domain-member VLANs.

ESRP-enabled device

An ESRP-enabled device is an Extreme Networks switch with an ESRP domain and ESRP enabled. ESRP-enabled switches include the ESRP master and slave switches.

ESRP extended mode

ESRP extended mode supports and is compatible only with switches running ExtremeXOS software exclusively.

ESRP group

An ESRP group runs multiple instances of ESRP within the same VLAN (or broadcast domain). To provide redundancy at each tier, use a pair of ESRP switches on the group.

ESRP instance

You enable ESRP on a per domain basis; each time you enable ESRP is an ESRP instance.

ESRP VLAN

A VLAN that is part of an ESRP domain, with ESRP enabled, is an ESRP VLAN.

ESS

Extended Service Set. Several Basic Service Sets (BSSs) can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. (See BSS and SSID.)

ethernet

This is the IEEE 802.3 networking standard that uses carrier sense multiple access with collision detection (CSMA/CD). An Ethernet device that wants to transmit first checks the channel for a carrier, and if no carrier is sensed within a period of time, the device transmits. If two devices transmit simultaneously, a collision occurs. This collision is detected by all transmitting devices, which subsequently delay their retransmissions for a random period. Ethernet runs at speeds from 10 Mbps to 10 Gbps on full duplex.

event

Any type of occurrence on a switch that could generate a log message or require an action. For more, see syslog.

external table

To route traffic between autonomous systems, external routing protocols and tables, such as EGP and BGP, are used.

F

fabric module (FM)

For more information about available fabric modules, see Understanding Fabric Modules in the *BlackDiamond X8 series Switches Hardware Installation Guide*.

fast convergence

In EAPS, Fast Convergence allows convergence in the range of 50 milliseconds. This parameter is configured for the entire switch, not by EAPS domain.

fast path

This term refers to the data path for a packet that traverses the switch and does not require processing by the CPU. Fast path packets are handled entirely by ASICs and are forwarded at wire speed rate.

FDB

Forwarding database. The switch maintains a database of all MAC address received on all of its ports and uses this information to decide whether a frame should be forwarded or filtered. Each FDB entry consists of the MAC address of the sending device, an identifier for the port on which the frame was received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not currently in the FDB are flooded to all members of the VLAN. For some types of entries, you configure the time it takes for the specific entry to age out of the FDB.

FHSS

Frequency-Hopping Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with DSSS.)

FIB

Forwarding Information Base. On BlackDiamond 8800 series switches and Summit family switches, the Layer 3 routing table is referred to as the FIB.

fit, thin, and fat APs

A *thin* AP architecture uses two components: an access point that is essentially a stripped-down radio and a centralized management controller that handles the other WLAN system functions. Wired network switches are also required.

A *fit* AP, a variation of the thin AP, handles the RF and encryption, while the central management controller, aware of the wireless users' identities and locations, handles secure roaming, quality of service, and user authentication. The central management controller also handles AP configuration and management.

A *fat* (or thick) AP architecture concentrates all the WLAN intelligence in the access point. The AP handles the radio frequency (RF) communication, as well as authenticating users, encrypting communications, secure roaming, WLAN management, and in some cases, network routing.

frame

This is the unit of transmission at the data link layer. The frame contains the header and trailer information required by the physical medium of transmission.

FQDN

Fully Qualified Domain Name. A 'friendly' designation of a computer, of the general form computer.[subnetwork.].organization.domain. The FQDN names must be translated into an IP address in order for the resource to be found on a network, usually performed by a DNS.

full-duplex

This is the communication mode in which a device simultaneously sends and receives over the same link, doubling the bandwidth. Thus, a full-duplex 100 Mbps connection has a bandwidth of 200 Mbps, and so forth. A device either automatically adjusts its duplex mode to match that of a connecting device or you can configure the duplex mode; all devices at 1 Gbps or higher run only in full-duplex mode.

FTM

Forwarding Table Manager.

FTP

File Transfer Protocol.

G

gateway

In the wireless world, an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

gigabit ethernet

This is the networking standard for transmitting data at 1000 Mbps or 1 Gbps. Devices can transmit at multiples of gigabit Ethernet as well.

gratuitous ARP

When a host sends an ARP request to resolve its own IP address, it is called gratuitous ARP. For more information, see Gratuitous ARP Protection in the *ExtremeXOS User Guide*.

GUI

Graphical User Interface.

H

HA

Host Attach. In ExtremeXOS software, HA is part of ESRP that allows you to connect active hosts directly to an ESRP switch; it allows configured ports to continue Layer 2 forwarding regardless of their ESRP status.

half-duplex

This is the communication mode in which a device can either send or receive data, but not simultaneously. (Devices at 1 Gbps or higher do not run in half-duplex mode; they run only in full-duplex mode.)

header

This is control information (such as originating and destination stations, priority, error checking, and so forth) added in front of the data when encapsulating the data for network transmission.

heartbeat message

A UDP data packet used to monitor a data connection, polling to see if the connection is still alive.
In general terms, a heartbeat is a signal emitted at regular intervals by software to demonstrate that it is still alive. In networking, a heartbeat is the signal emitted by a Level 2 Ethernet transceiver at the end of every packet to show that the collision-detection circuit is still connected.

hitless failover

In the Extreme Networks implementation on modular switches, hitless failover means that designated configurations survive a change of primacy between the two MSMs with all details intact. Thus, those features run seamlessly during and after control of the system changes from one MSM to another.

host

1. A computer (usually containing data) that is accessed by a user working on a remote terminal, connected by modems and telephone lines.
2. A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

HTTP

Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. A Web browser makes use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. (RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1)

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL, is a web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

IBGP

Interior Border Gateway Protocol. IBGP is the BGP version used within an AS.

IBSS

Independent Basic Service Set (see BSS). An IBSS is the 802.11 term for an ad-hoc network. See ad-hoc mode.

ICMP

Internet Control Message Protocol. ICMP is the part of the TCP/IP protocol that allows generation of error messages, test packets, and operating messages. For example, the ping command allows you to send ICMP echo messages to a remote IP device to test for connectivity. ICMP also supports traceroute, which identifies intermediate hops between a given source and destination.

ICV

ICV (Integrity Check Value) is a 4-byte code appended in standard WEP to the 802.11 message. Enhanced WPA inserts an 8-byte MIC just before the ICV. (See WPA and MIC.)

IEEE

Institute of Electrical and Electronic Engineers. This technical professional society fosters the development of standards that often become national and international standards. The organization publishes a number of journals and has many local chapters and several large societies in special areas.

IETF

Internet Engineering Task Force. The IETF is a large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The technical work of the IETF is done in working groups, which are organized by topic.

IGMP

Internet Group Management Protocol. Hosts use IGMP to inform local routers of their membership in multicast groups. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. When all hosts leave a group, the router no longer forwards packets that arrive for the multicast group.

IGMP snooping

This provides a method for intelligently forwarding multicast packets within a Layer 2 broadcast domain. By “snooping” the IGMP registration information, the device forms a distribution list that determines which endstations receive packets with a specific multicast address. Layer 2 switches listen for IGMP messages and build mapping tables and associated forwarding filters. IGMP snooping also reduces IGMP protocol traffic.

IGP

Interior Gateway Protocol. IGP refers to any protocol used to exchange routing information within an AS. Examples of Internet IGPs include RIP and OSPF.

inline power

According to IEEE 802.3 af, inline power refers to providing an AC or DC power source through the same cable as the data travels. It allows phones and network devices to be placed in locations that are not near AC outlets. Most standard telephones use inline power.

infrastructure mode

An 802.11 networking framework in which devices communicate with each other by first going through an access point. In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. (See ad-hoc mode and BSS.)

intermediate certificate

A certificate in the middle of a certificate chain, that bridges the trust relationship between the server certificate and the trusted certificate.

IP

Internet Protocol. The communications protocol underlying the Internet, IP allows large, geographically diverse networks of computers to communicate with each other quickly and economically over a variety of physical links; it is part of the TCP/IP suite of protocols. IP is the Layer 3, or network layer, protocol that contains addressing and control information that allows packets to be routed. IP is the most widely used networking protocol; it supports the idea of unique addresses for each computer on the network. IP is a connectionless, best-effort protocol; TCP reassembles the data after transmission. IP specifies the format and addressing scheme for each packet.

IPC

Interprocess Communication. A capability supported by some operating systems that allows one process to communicate with another process. The processes can be running on the same computer or on different computers connected through a network.

IPsec/IPsec-ESP/IPsec-AH

Internet Protocol security (IPSec)	Internet Protocol security.
Encapsulating Security Payload (IPsec-ESP)	The encapsulating security payload (ESP) encapsulates its data, enabling it to protect data that follows in the datagram.
Internet Protocol security Authentication Header (IPsec-AH)	AH protects the parts of the IP datagram that can be predicted by the sender as it will be received by the receiver.

IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

IPv6

Internet Protocol version 6. IPv6 is the next-generation IP protocol. The specification was completed in 1997 by IETF. IPv6 is backward- compatible with and is designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses. IPv6 increases the address space from 32 to 128 bits, providing for an unlimited (for all intents and purposes) number of networks and systems; IPv6 is expected to slowly replace IPv4, with the two existing side by side for many years.

IP address

IP address is a 32-bit number that identifies each unique sender or receiver of information that is sent in packets; it is written as four octets separated by periods (dotted-decimal format). An IP address has two parts: the identifier of a particular network and an identifier of the particular device (which can be a server or a workstation) within that network. You may add an optional sub-network identifier. Only the network part of the address is looked at between the routers that move packets from one point to another along the network. Although you can have a static IP address, many IP addresses are assigned dynamically from a pool. Many corporate networks and online services economize on the number of IP addresses they use by sharing a pool of IP addresses among a large number of users. (The format of the IP address is slightly changed in IPv6.)

IPTV

Internal Protocol television. IPTV uses a digital signal sent via broadband through a switched telephone or cable system. An accompanying set top box (that sits on top of the TV) decodes the video and converts it to standard television signals.

IR

Internal router. In OSPF, IR is an internal router that has all interfaces within the same area.

IRDP

Internet Router Discovery Protocol. Used with IP, IRDP enables a host to determine the address of a router that it can use as a default gateway. In Extreme Networks implementation, IP multinetting requires a few changes for the IRDP.

ISO

This abbreviation is commonly used for the International Organization for Standardization, although it is not an acronym. ISO was founded in 1946 and consists of standards bodies from more than 75 nations. ISO had defined a number of important computer standards, including the OSI reference model used as a standard architecture for networking.

isochronous

Isochronous data is data (such as voice or video) that requires a constant transmission rate, where data must be delivered within certain time constraints. For example, multimedia streams require an isochronous transport mechanism to ensure that data is delivered as fast as it is displayed and to ensure that the audio is synchronized with the video. Compare: asynchronous processes in which data streams can be broken by random intervals, and synchronous processes, in which data streams can be delivered only at specific intervals.

ISP

An Internet Service Provider is an organization that provides access to the Internet. Small ISPs provide service via modem and ISDN while the larger ones also offer private line hookups (T1, fractional T1, etc.). Customers are generally billed a fixed rate per month, but other charges may apply. For a fee, a Web site can be created and maintained on the ISP's server, allowing the smaller organization to have a presence on the Web with its own domain name.

ITU-T

International Telecommunication Union-Telecommunication. The ITU-T is the telecommunications division of the ITU international standards body.

IV

Initialization Vector. Part of the standard WEP encryption mechanism that concatenates a shared secret key with a randomly generated 24-bit initialization vector. WPA with TKIP uses 48-bit IVs, an enhancement that significantly increases the difficulty in cracking the encryption. (See WPA and TKIP.)

J

jumbo frames

Ethernet frames larger than 1522 bytes (including the 4 bytes in the CRC). The jumbo frame size is configurable on Extreme Networks devices; the range is from 1523 to 9216 bytes.

L

LACP

Link Aggregation Control Protocol. LACP is part of the IEEE 802.3ad and automatically configures multiple aggregated links between switches.

LAG

Link aggregation group. A LAG is the logical high-bandwidth link that results from grouping multiple network links in link aggregation (or load sharing). You can configure static LAGs or dynamic LAGs (using the LACP).

Layer 2

Layer 2 is the second, or data link, layer of the OSI model, or the MAC layer. This layer is responsible for transmitting frames across the physical link by reading the hardware, or MAC, source and destination addresses.

Layer 3

Layer 3 is the third layer of the OSI model. Also known as the network layer, Layer 3 is responsible for routing packets to different LANs by reading the network address.

LED

Light-emitting diode. LEDs are on the device and provide information on various states of the device’s operation. See your hardware documentation for a complete explanation of the LEDs on devices running ExtremeXOS.

legacy certificate

The certificates that shipped with NetSight and NAC 4.0.0 and earlier.

LFS

Link Fault Signal. LFS, which conforms to IEEE standard 802.3ae-2002, monitors 10 Gbps ports and indicates either remote faults or local faults.

license

ExtremeXOS version 11.1 introduces a licensing feature to the ExtremeXOS software. You must have a license, which you obtain from Extreme Networks, to apply the full functionality of some features.

link aggregation

Link aggregation, also known as trunking or load sharing, conforms to IEEE 802.3ad. This feature is the grouping of multiple network links into one logical high-bandwidth link.

link type

In OSPF, there are four link types that you can configure: auto, broadcast, point-to-point, and passive.

LLDP

Link Layer Discovery Protocol. LLDP conforms to IEEE 802.1ab and is a neighbor discovery protocol. Each LLDP-enabled device transmits information to its neighbors, including chassis and port identification, system name and description, VLAN names, and other selected networking information. The protocol also specifies timing intervals in order to ensure current information is being transmitted and received.

load sharing

Load sharing, also known as trunking or link aggregation, conforms to IEEE 802.3ad. This feature is the grouping of multiple network links into one logical high-bandwidth link. For example, by grouping four 100 Mbps of full-duplex bandwidth into one logical link, you can create up to 800 Mbps of bandwidth. Thus, you increase bandwidth and availability by using a group of ports to carry traffic in parallel between switches.

loop detection

In ELRP, loop detection is the process used to detect a loop in the network. The switch sending the ELRP PDU waits to receive its original PDU back. If the switch received this original PDU, there is a loop in the network.

LSA

Link state advertisement. An LSA is a broadcast packet used by link state protocols, such as OSPF. The LSA contains information about neighbors and path costs and is used by the receiving router to maintain a routing table.

LSDB

Link state database. In OSPF, LSDB is a database of information about the link state of the network. Two neighboring routers consider themselves to be adjacent only if their LSDBs are synchronized. All routing information is exchanged only between adjacent routers.

M

MAC

Media Access Control layer. One of two sub-layers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one NIC to another across a shared channel.

MAC address

Media access control address. The MAC address, sometimes known as the hardware address, is the unique physical address of each network interface card on each device.

MAN

Metropolitan area network. A MAN is a data network designed for a town or city. MANs may be operated by one organization such as a corporation with several offices in one city, or be shared resources used by several organizations with several locations in the same city. MANs are usually characterized by very high-speed connections.

master node

In EAPS, the master node is a switch, or node, that is designated the master in an EAPS domain ring. The master node blocks the secondary port for all non-control traffic belonging to this EAPS domain, thereby avoiding a loop in the ring.

master router

In VRRP, the master router is the physical device (router) in the VRRP virtual router that is responsible for forwarding packets sent to the VRRP virtual router and for responding to ARP requests. The master router sends out periodic advertisements that let backup routers on the network know that it is alive. If the VRRP IP address owner is identified, it always becomes the master router.

master VLAN

In ESRP, the master VLAN is the VLAN on the ESRP domain that exchanges ESRP-PDUs and data between a pair of ESRP-enabled devices. You must configure one master VLAN for each ESRP domain, and a master VLAN can belong to only one ESRP domain.

MED

Multiple exit discriminator. BGP uses the MED metric to select a particular border router in another AS when multiple border routers exist.

member VLAN

In ESRP, you configure zero or more member VLANs for each ESRP domain. A member VLAN can belong to only one ESRP domain. The state of the ESRP device determines whether the member VLAN is in forwarding or blocking state.

MEP

In CFM, maintenance end point is an end point for a single domain, or maintenance association. The MEP may be either an UP MEP or a DOWN MEP.

metering

In QoS, metering monitors the traffic pattern of each flow against the traffic profile. For out-of-profile traffic the metering function interacts with other components to either re-mark or drop the traffic for that flow. In the Extreme Networks implementation, you use ACLs to enforce metering.

MIB

Management Information Base. MIBs make up a database of information (for example, traffic statistics and port settings) that the switch makes available to network management systems. MIB names identify objects that can be managed in a network and contain information about the objects. MIBs provide a means to configure a network device and obtain network statistics gathered by the device. Standard, minimal MIBs have been defined, and vendors often have private enterprise MIBs.

MIC

Message Integrity Check or Code (MIC), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte integrity check value (ICV) that is appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.

Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with. (See WPA, TKIP, and ICV.)

MIP

In CFM, the maintenance intermediate point is intermediate between endpoints. Each MIP is associated with a single domain, and there may be more than one MIP in a single domain.

mirroring

Port mirroring configures the switch to copy all traffic associated with one or more ports to a designated monitor port. The monitor port can be connected to an network analyzer or RMON probe for packet analyzer.

MLAG

Multi-switch Link Aggregation Group (a.k.a. Multi-Chassis Link Aggregation Group). This feature allows users to combine ports on two switches to form a single logical connection to another network device. The other network device can be either a server or a switch that is separately configured with a regular LAG (or appropriate server port teaming) to form the port aggregation.

MM

Management Module. For more information, see Understanding Management Modules in the *BlackDiamond X8 series Switches Hardware Installation Guide*.

MMF

Multimode fiber. MMF is a fiber optic cable with a diameter larger than the optical wavelength, in which more than one bound mode can propagate. Capable of sending multiple transmissions simultaneously, MMF is commonly used for communications of 2 km or less.

MSDP

Multicast Source Discovery Protocol. MSDP is used to connect multiple multicast routing domains. MSDP advertises multicast sources across Protocol Independent Multicast-Sparse Mode (PIM-SM) multicast domains orRendezvous Points (RPs). In turn, these RPs run MSDP over TCP to discover multicast sources in other domains.

MSM

Master Switch Fabric Module. This Extreme Networks-proprietary name refers to the module that holds both the control plane and the switch fabric for switches that run the ExtremeXOS software on modular switches. One MSM is required for switch operation; adding an additional MSM increases reliability and throughput. Each MSM has two CPUs. The MSM has LEDs as well as a console port, management port, modem port, and compact flash; it may have data ports as well. The MSM is responsible for upper-layer protocol processing and system management functions. When you save the switch configuration, it is saved to all MSMs.

MSTI

Multiple Spanning Tree Instances. MSTIs control the topology inside an MSTP region. An MSTI is a spanning tree domain that operates within a region and is bounded by that region; and MSTI does not exchange BPDUs or send notifications to other regions. You can map multiple VLANs to an MSTI; however, each VLAN can belong to only one MSTI.You can configure up to 64 MSTIs in an MSTP region.

MSTI regional root bridge

In an MSTP environment, each MSTI independently elects its own root bridge. The bridge with the lowest bridge ID becomes the MSTI regional root bridge. The bridge ID includes the bridge priority and the MAC address.

MSTI root port

In an MSTP environment, the port on the bridge with the lowest path cost to the MSTI regional root bridge is the MSTI root port.

MSTP

Multiple Spanning Tree Protocol. MSTP, based on IEEE 802.1Q-2003 (formerly known as IEEE 892.1s), allows you to bundle multiple VLANs into one spanning tree (STP) topology, which also provides enhanced loop protection and better scaling. MSTP uses RSTP as the converging algorithm and is compatible with legacy STP protocols.

MSTP region

An MSTP region defines the logical boundary of the network. Interconnected bridges that have the same MSTP configuration are referred to as an MSTP region. Each MSTP region has a unique identifier, is bound together by one CIST that spans the entire network, and contains from 0 to 64 MSTIs. A bridge participates in only one MSTP region at one time. An MSTP topology is individual MSTP regions connected either to the rest of the network with 802.1D and 802.1w bridges or to each other.

MTU

Maximum transmission unit. This term is a configurable parameter that determines the largest packet than can be transmitted by an IP interface (without the packet needing to be broken down into smaller units).

Note
Packets that are larger than the configured MTU size are dropped at the ingress port. Or, if configured to do so, the system can fragment the IPv4 packets and reassemble them at the receiving end.

multicast

Multicast messages are transmitted to selected devices that specifically join the multicast group; the addresses are specified in the destination address field. In other words, multicast (point-to-multipoint) is a communication pattern in which a source host sends a message to a group of destination hosts.

multinetting

IP multinetting assigns multiple logical IP interfaces on the same circuit or physical interface. This allows one bridge domain (VLAN) to have multiple IP networks.

MVR

Multicast VLAN registration. MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN; it allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the The application from the subscriber VLANs for bandwidth and security reasons. MVR allows a multicast stream received over a Layer 2 VLAN to be forwarded to another VLAN, eliminating the need for a Layer 3 routing protocol; this feature is often used for IPTV applications.

N

NAS

Network Access Server. This is server responsible for passing information to designated RADIUS servers and then acting on the response returned. A NAS-Identifier is a RADIUS attribute identifying the NAS server. (RFC 2138)

NAT

Network Address Translation (or Translator). This is a network capability that enables a group of computers to dynamically share a single incoming IP address. NAT takes the single incoming IP address and creates a new IP address for each client computer on the network.

netlogin

Network login provides extra security to the network by assigning addresses only to those users who are properly authenticated. You can use web-based, MAC-based, or IEEE 802.1X-based authentication with network login. The two modes of operation are campus mode and ISP mode.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

neutral state/switch

In ESRP, the neutral state is the initial state entered by the switch. In a neutral state, the switch waits for ESRP to initialize and run. A neutral switch does not participate in ESRP elections.

NIC

Network Interface Card. An expansion board in a computer that connects the computer to a network.

NLRI

Network layer reachability information. In BGP, the system sends routing update messages containing NLRI to describe a route and how to get there. A BGP update message carries one or more NLRI prefixes and the attributes of a route for each NLRI prefix; the route attributes include a BGP next hop gateway address, community values, and other information.

NMS

Network Management System. The system responsible for managing a network or a portion of a network. The NMS talks to network management agents, which reside in the managed nodes.

node

In general networking terms, a node is a device on the network. In the Extreme Networks implementation, a node is a CPU that runs the management application on the switch. Each MSM on modular switches installed in the chassis is a node.

node manager

The node manager performs the process of node election, which selects the master, or primary, MSM when you have two MSMs installed in the modular chassis. The node manager is useful for system redundancy.

NSSA

Not-so-stubby area. In OSPF, NSSA is a stub area, which is connected to only one other area, with additional capabilities:

- External routes originating from an ASBR connected to the NSSA can be advertised within the NSSA.
- External routes originating from the NSSA can be propagated to other areas.

NTP

Network Time Protocol, an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Based on UTC, NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. (RFC 1305)

O

odometer

In the Extreme Networks implementation, each field replaceable component contains a system odometer counter in EEPROM.

On modular switches, using the CLI, you can display how long each following individual component has been in service:

- chassis
- MSMs
- I/O modules
- power controllers

On standalone switches, you display the days of service for the switch.

OFDM

Orthogonal frequency division multiplexing, a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. OFDM is similar to conventional frequency division multiplexing (FDM). The difference lies in the way in which the signals are modulated and demodulated. Priority is given to minimizing the interference, or crosstalk, among the channels and symbols comprising the data stream. Less importance is placed on perfecting individual channels. OFDM is used in European digital audio broadcast services. It is also used in wireless local area networks.

OID

Object identifier.

option 82

This is a security feature that you configure as part of BOOTP/DHCP. Option 82 allows a server to bind the client's port, IP address, and MAC number for subscriber identification.

OSI

Open Systems Interconnection. OSI is an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, down through the presentation, session, transport, network, data link layer to the physical layer at the bottom, over the channel to the next station and back up the hierarchy.

OSI Layer 2

At the Data Link layer (OSI Layer 2), data packets are encoded and decoded into bits. The data link layer has two sub-layers:

- The Logical Link Control (LLC) layer controls frame synchronization, flow control and error checking.
- The Media Access Control (MAC) layer controls how a computer on the network gains access to the data and permission to transmit it.

OSI Layer 3

The Network layer (OSI Layer 3) provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, inter-networking, error handling, congestion control and packet sequencing.

OSI reference model

The seven-layer standard model for network architecture is the basis for defining network protocol standards and the way that data passes through the network. Each layer specifies particular network functions; the highest layer is closest to the user, and the lowest layer is closest to the media carrying the information. So, in a given message between users, there will be a flow of data through each layer at one end down through the layers in that computer and, at the other end, when the message arrives, another flow of data up through the layers in the receiving computer and ultimately to the end user or program. This model is used worldwide for teaching and implementing networking protocols.

OSPF

Open Shortest Path First. An interior gateway routing protocol for TCP/IP networks, OSPF uses a link state routing algorithm that calculates routes for packets based on a number of factors, including least hops, speed of transmission lines, and congestion delays. You can also configure certain cost metrics for the algorithm. This protocol is more efficient and scalable than vector-distance routing protocols. OSPF features include least-cost routing, ECMP routing, and load balancing. Although OSPF requires CPU power and memory space, it results in smaller, less frequent router table updates throughout the network. This protocol is more efficient and scalable than vector-distance routing protocols.

OSPFv3

OSPFv3 is one of the routing protocols used with IPV6 and is similar to OSPF.

OUI

Organizational(ly) Unique Identifier. The OUI is the first 24 bits of a MAC address for a network device that indicate a specific vendor as assigned by IEEE.

P

packet

This is the unit of data sent across a network. Packet is a generic term used to describe units of data at all levels of the protocol stack, but it is most correctly used to describe application data units. The packet is a group of bits, including data and control signals, arranged in a specific format. It usually includes a header, with source and destination data, and user data. The specific structure of the packet depends on the protocol used.

PAP

Password Authentication Protocol. This is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. (See CHAP.)

partner node

In EAPS, the partner node is that end of the common link that is not a controller node; the partner node does not participate in any form of blocking.

PD

Powered device. In PoE, the PD is the powered device that plugs into the PoE switch.

PDU

Protocol data unit. A PDU is a message of a given protocol comprising payload and protocol-specific control information, typically contained in a header.

PEAP

Protected Extensible Authentication Protocol. PEAP is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also EAP-TLS.)

PEC

Power Entry Circuit.

PEM

Power Entry Module.

PIM-DM

Protocol-Independent Multicast - Dense mode. PIM-DM is a multicast protocol that uses Reverse Path Forwarding but does not require any particular unicast protocol. It is used when recipients are in a concentrated area.

PIM-SM

Protocol-Independent Multicast - Sparse mode. PIM-SM is a multicast protocol that defines a rendezvous point common to both sender and receiver. Sender and receiver initiate communication at the rendezvous point, and the flow begins over an optimized path. It is used when recipients are in a sparse area.

ping

Packet Internet Groper. Ping is the ICMP echo message and its reply that tests network reachability of a device. Ping sends an echo packet to the specified host, waits for a response, and reports success or failure and statistics about its operation.

PKCS #8 (Public-Key Cryptography Standard #8)

One of several standard formats which can be used to store a private key in a file. It can optionally be encrypted with a password.

PKI

Public Key Infrastructure.

PMBR

PIM multicast border router. A PIMBR integrates PIM-DM and PIM-SM traffic.

PoE

Power over Ethernet. The PoE standard (IEEE 802.3af) defines how power can be provided to network devices over existing Ethernet connections, eliminating the need for additional external power supplies.

policy files

You use policy files in ExtremeXOS to specify ACLs and policies. A policy file is a text file (with a .pol extension) that specifies a number of conditions to test and actions to take. For ACLs, this information is applied to incoming traffic at the hardware level. Policies are more general and can be applied to incoming routing information; they can be used to rewrite and modify routing advertisements.

port mirroring

Port mirroring configures the switch to copy all traffic associated with one or more ports to a designated monitor port. A packet bound for or heading away from the mirrored port is forwarded onto the monitor port as well. The monitor port can be connected to a network analyzer or RMON probe for packet analysis. Port mirroring is a method of monitoring network traffic that a network administrator uses as a diagnostic tool or debugging feature; it can be managed locally or remotely.

POST

Power On Self Test. On Extreme Networks switches, the POST runs upon powering-up the device. Once the hardware elements are determined to be present and powered on, the boot sequence begins. If the MGMT LED is yellow after the POST completes, contact your supplier for advice.

primary port

In EAPS, a primary port is a port on the master node that is designated the primary port to the ring.

protected VLAN

In STP, protected VLANs are the other (other than the carrier VLAN) VLANs that are members of the STPD but do not define the scope of the STPD. Protected VLANs do not transmit or receive STP BPDUs, but they are affected by STP state changes and inherit the state of the carrier VLAN. Also known as non-carrier VLANs, they carry the data traffic.

In EAPS, a protected VLAN is a VLAN that carries data traffic through an EAPS domain. You must configure one or more protected VLANs for each EAPS domain. This is also known as a data VLAN.

proxy ARP

This is the technique in which one machine, usually a router, answers ARP requests intended for another machine. By masquerading its identity (as an endstation), the router accepts responsibility for routing packets to the real destination. Proxy ARP allows a site to use a single IP address with two physical networks. Subnetting is normally a better solution.

pseudowire

Sometimes spelled as "pseudo-wire" or abbreviated as PW. As described in RFC 3985, there are multiple methods for carrying networking services over a packet-switched network. In short, a pseudowire emulates networking or telecommunication services across packet-switched networks that use Ethernet, IP, or MPLS. Emulated services include T1 leased line, frame relay, Ethernet, ATM, TDM, or SONET/SDH.

push-to-talk (PTT)

The push-to-talk is feature on wireless telephones that allows them to operate like a walkie-talkie in a group, instead of standard telephone operation. The PTT feature requires that the network be configured to allow multicast traffic.
A PTT call is initiated by selecting a channel and pressing the 'talk' key on the wireless telephone. All wireless telephones on the same network that are monitoring the channel will hear the transmission. On a PTT call you hold the button to talk and release it to listen.

PVST+

Per VLAN Spanning Tree +. This implementation of STP has a 1:1 relationship with VLANs. The Extreme Networks implementation of PVST+ allows you to interoperate with third-party devices running this version of STP. PVST is a earlier version of this protocol and is compatible with PVST+.

Q

QoS

Quality of Service. Policy-enabled QoS is a network service that provides the ability to prioritize different types of traffic and to manage bandwidth over a network. QoS uses various methods to prioritize traffic, including IEEE 802.1p values and IP DiffServ values. QoS features provide better network service by supporting dedicated bandwidth, improving loss characteristics, avoiding and managing network congestion, shaping network traffic, and setting traffic priorities across the network. (RFC 2386)

R

radar

Radar is a set of advanced, intelligent, Wireless-Intrusion-Detection-Service-Wireless-Intrusion-Prevention-Service (WIDS-WIPS) features that are integrated into the Wireless Controller and its access points (APs). Radar provides a basic solution for discovering unauthorized devices within the wireless coverage area. Radar performs basic RF network analysis to identify unmanaged APs and personal ad-hoc networks. The Radar feature set includes: intrusion detection, prevention and interference detection.

RADIUS

Remote Authentication Dial In User Service. RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. With RADIUS, you can track usage for billing and for keeping network statistics.

RARP

Reverse ARP. Using this protocol, a physical device requests to learn its IP address from a gateway server's ARP table. When a new device is set up, its RARP client program requests its IP address from the RARP server on the router. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

rate limiting

In QoS, rate limiting is the process of restricting traffic to a peak rate (PR). For more information, see rate limiting and rate shaping in the *ExtremeXOS User Guide*.

rate shaping

In QoS, rate shaping is the process of reshaping traffic throughput to give preference to higher priority traffic or to buffer traffic until forwarding resources become available. For more information, see rate limiting and rate shaping in the *ExtremeXOS User Guide*.

RF

Radio Frequency. A frequency in the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that can propagate through space. These frequencies in the electromagnetic spectrum range from Ultra-low frequency (ULF):0-3 Hz to Extremely high frequency (EHF): 30 GHz–300 GHz. The middle ranges are: Low frequency (LF): 30 kHz–300 kHz; Medium frequency (MF): 300 kHz–3 MHz; High frequency (HF): 3 MHz–30 MHz; Very high frequency (VHF): 30 MHz–300 MHz; and Ultra-high frequency (UHF): 300 MHz–3 GHz.

RFC

Request for Comment. The IETF RFCs describe the definitions and parameters for networking. The RFCs are catalogued and maintained on the IETF RFC website: www.ietf.org/rfc.html.

Ridgeline

Ridgeline is an Extreme Networks-proprietary graphical user interface (GUI) network management system. The name was changed from EPICenter to Ridgeline in 2011.

RIP

Routing Information Protocol. This IGP vector-distance routing protocol is part of the TCP/IP suite and maintains tables of all known destinations and the number of hops required to reach each. Using RIP, routers periodically exchange entire routing tables. RIP is suitable for use only as an IGP.

RIPng

RIP next generation. RIPng is one of the routing protocols used with IPv6 and is similar to RIP.

RMON

Remote monitoring. RMON is a standardized method to make switch and router information available to remote monitoring applications. It is an SNMP network management protocol that allows network information to be gathered remotely. RMON collects statistics and enables a management station to monitor network devices from a central location. It provides multivendor interoperability between monitoring devices and management stations. RMON is described in several RFCs (among them IETF RFC 1757 and RFC 2201).

Network administrators use RMON to monitor, analyze, and troubleshoot the network. A software agent can gather the information for presentation to the network administrator with a graphical user interface (GUI). The administrator can find out how much bandwidth each user is using and what web sites are being accessed; you can also set alarms to be informed of potential network problems.

roaming

In 802.11, roaming occurs when a wireless device (a station) moves from one Access Point to another (or BSS to another) in the same Extended Service Set (ESS) -identified by its SSID.

root bridge

In STP, the root bridge is the bridge with the best bridge identifier selected to be the root bridge. The network has only one root bridge. The root bridge is the only bridge in the network that does not have a root port.

root port

In STP, the root port provides the shortest path to the root bridge. All bridges except the root bridge contain one root port.

route aggregation

In BGP, you can combine the characteristics of several routes so they are advertised as a single route, which reduces the size of the routing tables.

route flapping

A route is flapping when it is repeatedly available, then unavailable, then available, then unavailable. In the ExtremeXOS BGP implementation, you can minimize the route flapping using the route flap dampening feature.

route reflector

In BGP, you can configure the routers within an AS such that a single router serves as a central routing point for the entire AS.

routing confederation

In BGP, you can configure a fully meshed autonomous system into several sub-ASs and group these sub-ASs into a routing confederation. Routing confederations help with the scalability of BGP.

RP-SMA

Reverse Polarity-Subminiature version A, a type of connector used with wireless antennas.

RSN

Robust Security Network. A new standard within IEEE 802.11 to provide security and privacy mechanisms. The RSN (and related TSN) both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

RSSI

RSSI received signal strength indication (in 802.11 standard).

RTS/CTS

RTS request to send, CTS clear to send (in 802.11 standard).

RSTP

Rapid Spanning Tree Protocol. RSTP, described in IEEE 802.1w, is an enhanced version of STP that provides faster convergence. The Extreme Networks implementation of RSTP allows seamless interoperability with legacy STP.

S

SA

Source address. The SA is the IP or MAC address of the device issuing the packet.

SCP

Secure Copy Protocol. SCP2, part of SSH2, is used to transfer configuration and policy files.

SDN

Software-defined Networking. An approach to computer networking that seeks to manage network services through decoupling the system that makes decisions about where traffic is sent (control plane) from the underlying systems that forward traffic to the selected destination (data plan).

secondary port

In EAPS, the secondary port is a port on the master node that is designated the secondary port to the ring. The transit node ignores the secondary port distinction as long as the node is configured as a transit node.

segment

In Ethernet networks, a section of a network that is bounded by bridges, routers, or switches. Dividing a LAN segment into multiple smaller segments is one of the most common ways of increasing available bandwidth on the LAN.

server certificate

A certificate identifying a server. When a client connects to the server, the server sends its certificate to the client and the client validates the certificate to trust the server.

sFlow

sFlow allows you to monitor network traffic by statistically sampling the network packets and periodically gathering the statistics. The sFlow monitoring system consists of an sFlow agent (embedded in a switch, router, or stand-alone probe) and an external central data collector, or sFlow analyzer.

SFP

Small form-factor pluggable. These transceivers offer high speed and physical compactness.

slow path

This term refers to the data path for packets that must be processed by the switch CPU, whether these packets are generated by the CPU, removed from the network by the CPU, or simply forwarded by the CPU.

SLP

Service Location Protocol. A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network.

Using SLP, networking applications can discover the existence, location and configuration of networked devices.
With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.
For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.
(SLP version 2, RFC2608, updating RFC2165)

SMF

Single-mode fiber. SMF is a laser-driven optical fiber with a core diameter small enough to limit transmission to a single bound mode. SMF is commonly used in long distance transmission of more than three miles; it sends one transmission at a time.

SMI

Structure of Management Information. A hierarchical tree structure for information that underlies Management Information Bases (MIBs), and is used by the SNMP protocol. Defined in RFC 1155 and RFC 1442 (SNMPv2).

SMON

Switch Network Monitoring Management (MIB) system defined by the IETF document RFC 2613. SMON is a set of MIB extensions for RMON that allows monitoring of switching equipment from a SNMP Manager in greater detail.

SMT

Station Management. The object class in the 802.11 MIB that provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network. The four branches of the 802.11 MIB are:

- dot11smt—objects related to station management and local configuration
- dot11mac—objects that report/configure on the status of various MAC parameters
- dot11res—objects that describe available resources
- dot11phy—objects that report on various physical items

SNMP

Simple Network Management Protocol. SNMP is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multivendor environment, and the agent uses MIBs, which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

SNTP

Simple Network Time Protocol. SNTP is used to synchronize the system clocks throughout the network. An extension of the Network Time Protocol, SNTP can usually operate with a single server and allows for IPv6 addressing.

SSH

Secure Shell, sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol of securely gaining access to a remote computer. With SSH commands, both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. At Extreme Networks, the SSH is a separate software module, which must be downloaded separately. (SSH is bundled with SSL in the software module.)

SSID

Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the Basic Service Set (BSSs). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS.

In 802.11 networks, each access point (AP) advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named access point, it sends an associate request frame containing the desired SSID. The AP replies with an associate response frame, also containing the SSID.
Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.

SSL

Secure Sockets Layer. SSL is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

spoofing

Hijacking a server's IP address or hostname so that requests to the server are redirected to another server. Certificate validation is used to detect and prevent this.

standard mode

Use ESRP standard mode if your network contains switches running ExtremeWare and switches running ExtremeXOS, both participating in ESRP.

STP

Spanning Tree Protocol. STP is a protocol, defined in IEEE 802.1d, used to eliminate redundant data paths and to increase network efficiency. STP allows a network to have a topology that contains physical loops; it operates in bridges and switches. STP opens certain paths to create a tree topology, thereby preventing packets from looping endlessly on the network. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the STP topology and re-establishes the link by activating the standby path.

STPD

Spanning Tree Domain. An STPD is an STP instance that contains one or more VLANs. The switch can run multiple STPDs, and each STPD has its own root bridge and active path. In the Extreme Networks implementation of STPD, each domain has a carrier VLAN (for carrying STP information) and one or more protected VLANs (for carrying the data).

STPD mode

The mode of operation for the STPD. The two modes of operation are:

- 802.1d—Compatible with legacy STP and other devices using the IEEE 802.1d standard.
- 802.1w—Compatible with Rapid Spanning Tree (RSTP).

stub areas

In OSPF, a stub area is connected to only one other area (which can be the backbone area). External route information is not distributed to stub areas.

subnet mask

See netmask.

subnets

Portions of networks that share the same common address format. A subnet in a TCP/IP network uses the same first three sets of numbers (such as 198.63.45.xxx), leaving the fourth set to identify devices on the subnet. A subnet can be used to increase the bandwidth on the network by breaking the network up into segments.

superloop

In EAPS, a superloop occurs if the common link between two EAPS domains goes down and the master nodes of both domains enter the failed state putting their respective secondary ports into the forwarding state. If there is a data VLAN spanning both EAPS domains, this action forms a loop between the EAPS domains.

SVP

SpectraLink Voice Protocol, a protocol developed by SpectraLink to be implemented on access points to facilitate voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

system health check

The primary responsibility of the system health checker is to monitor and poll error registers. In addition, the system health checker can be enabled to periodically send diagnostic packets. System health check errors are reported to the syslog.

T

TACACS+

Terminal Access Controller Access Control System. Often run on UNIX systems, the TACAS+ protocol provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services. User passwords are administered in a central database rather than in individual routers, providing easily scalable network security solutions.

tagged VLAN

You identify packets as belonging to the same tagged VLAN by putting a value into the 12-bit (4 octet) VLAN ID field that is part of the IEEE 802.1Q field of the header. Using this 12-bit field, you can configure up to 4096 individual VLAN addresses (usually some are reserved for system VLANs such as management and default VLANs); these tagged VLANs can exist across multiple devices. The tagged VLAN can be associated with both tagged and untagged ports.

TCN

Topology change notification. The TCN is a timer used in RSTP that signals a change in the topology of the network.

TCP / IP

Transmission Control Protocol. Together with Internet Protocol (IP), TCP is one of the core protocols underlying the Internet. The two protocols are usually referred to as a group, by the term TCP/IP. TCP provides a reliable connection, which means that each end of the session is guaranteed to receive all of the data transmitted by the other end of the connection, in the same order that it was originally transmitted without receiving duplicates.

TFTP

Trivial File Transfer Protocol. TFTP is an Internet utility used to transfer files, which does not provide security or directory listing. It relies on UDP.

TKIP

Temporal Key Integrity Protocol (TKIP) is an enhancement to the WEP encryption technique that uses a set of algorithms that rotates the session keys. The protocol's enhanced encryption includes a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. The encryption keys are changed (re-keyed) automatically and authenticated between devices after the re-key interval (either a specified period of time, or after a specified number of packets has been transmitted).

TLS

Transport Layer Security. See SSL

ToS / DSCP

ToS (Type of Service) / DSCP (Diffserv Codepoint). The ToS/DSCP box contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service.

transit node

In EAPS, the transit node is a switch, or node, that is not designated a master in the EAPS domain ring.

TRILL

Transparent Interconnection of Lots of Links. TRILL allows for improved scaling of data center servers and virtual machine interconnections by combining bridged networks with network topology control and routing management.

truststore

A repository containing trusted certificates, used to validate an incoming certificate. A truststore usually contains CA certificates, which represent certificate authorities that are trusted to sign certificates, and can also contain copies of server or client certificates that are to be trusted when seen.

TSN

Transition Security Network. A subset of Robust Security Network (RSN), which provides an enhanced security solution for legacy hardware. The Wi-Fi Alliance has adopted a solution called Wireless Protected Access (WPA), based on TSN. RSN and TSN both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

tunnelling

Tunnelling (or encapsulation) is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating packets of a network protocol within packets carried by the second network. The receiving device then decapsulates the packets and forwards them in their original format.

U

U-NII

Unlicensed National Information Infrastructure. Designated to provide short-range, high-speed wireless networking communication at low cost, U-NII consists of three frequency bands of 100 MHz each in the 5 GHz band: 5.15-5.25GHz (for indoor use only), 5.25-5.35 GHz and 5.725-5.825GHz. The three frequency bands were set aside by the FCC in 1997 initially to help schools connect to the Internet without the need for hard wiring. U-NII devices do not require licensing.

UDP

User Datagram Protocol. This is an efficient but unreliable, connectionless protocol that is layered over IP (as is TCP). Application programs must supplement the protocol to provide error processing and retransmitting data. UDP is an OSI Layer 4 protocol.

unicast

A unicast packet is communication between a single sender and a single receiver over a network.

untagged VLAN

A VLAN remains untagged unless you specifically configure the IEEE 802.1Q value on the packet. A port cannot belong to more than one untagged VLAN using the same protocol.

USM

User-based security model. In SNMPv3, USM uses the traditional SNMP concept of user names to associate with security levels to support secure network management.

V

virtual router

In the Extreme Networks implementations, virtual routers allow a single physical switch to be split into multiple virtual routers. Each virtual router has its own IP address and maintains a separate logical forwarding table. Each virtual router also serves as a configuration domain. The identity of the virtual router you are working in currently displays in the prompt line of the CLI. The virtual routers discussed in relation to Extreme Networks switches themselves are not the same as the virtual router in VRRP.

In VRRP, the virtual router is identified by a virtual router (VRID) and an IP address. A router running VRRP can participate in one or more virtual routers. The VRRP virtual router spans more than one physical router, which allows multiple routers to provide redundant services to users.

VEPA

Virtual Ethernet Port Aggregator. This is a Virtual Machine (VM) server feature that works with the ExtremeXOS Direct Attach Feature to support communications between VMs.

virtual link

In OSPF, when a new area is introduced that does not have a direct physical attachment to the backbone, a virtual link is used. Virtual links are also used to repair a discontiguous backbone area.

virtual router

In the Extreme Networks implementations, virtual routers allow a single physical switch to be split into multiple virtual routers. Each virtual router has its own IP address and maintains a separate logical forwarding table. Each virtual router also serves as a configuration domain. The identity of the virtual router you are working in currently displays in the prompt line of the CLI. The virtual routers discussed in relation to Extreme Networks switches themselves are not the same as the virtual router in VRRP.

In VRRP, the virtual router is identified by a virtual router (VRID) and an IP address. A router running VRRP can participate in one or more virtual routers. The VRRP virtual router spans more than one physical router, which allows multiple routers to provide redundant services to users.

virtual router MAC address

In VRRP, RFC 2338 assigns a static MAC address for the first five octets of the VRRP virtual router. These octets are set to 00-00-5E-00-01. When you configure the VRRP VRID, the last octet of the MAC address is dynamically assigned the VRID number.

VLAN

Virtual LAN. The term VLAN is used to refer to a collection of devices that communicate as if they are on the same physical LAN. Any set of ports (including all ports on the switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the CLI.

VLSM

Variable-length subnet masks. In OSPF, VLSMs provide subnets of different sizes within a single IP block.

VM

Virtual Machine. A VM is a logical machine that runs on a VM server, which can host multiple VMs.

VMAN

Virtual MAN. In ExtremeXOS software, VMANs are a bi-directional virtual data connection that creates a private path through the public network. One VMAN is completely isolated from other VMANs; the encapsulation allows the VMAN traffic to be switched over Layer 2 infrastructure. You implement VMAN using an additional 892.1Q tag and a configurable EtherType; this feature is also known as Q-in-Q switching.

VNS

Virtual Network Services. An Extreme Networks-specific technique that provides a means of mapping wireless networks to a wired topology.

VoIP

Voice over Internet Protocol is an Internet telephony technique. With VoIP, a voice transmission is cut into multiple packets, takes the most efficient path along the Internet, and is reassembled when it reaches the destination.

VPN

Virtual private network. A VPN is a private network that uses the public network (Internet) to connect remote sites and users. The VPN uses virtual connections routed through the Internet from a private network to remote sites or users. There are different kinds of VPNs, which all serve this purpose. VPNs also enhance security.

VR-Control

This virtual router (VR) is part of the embedded system in Extreme Networks switches. VR-Control is used for internal communications between all the modules and subsystems in the switch. It has no ports, and you cannot assign any ports to it. It also cannot be associated with VLANs or routing protocols. (Referred to as VR-1 in earlier ExtremeXOS software versions.)

VR-Default

This VR is part of the embedded system in Extreme Networks switches. VR-Default is the default VR on the system. All data ports in the switch are assigned to this VR by default; you can add and delete ports from this VR. Likewise, VR-Default contains the default VLAN. Although you cannot delete the default VLAN from VR-Default, you can add and delete any user-created VLANs. One instance of each routing protocol is spawned for this VR, and they cannot be deleted. (Referred to as VR-2 in earlier ExtremeXOS software versions.)

VR-Mgmt

This VR is part of the embedded system in Extreme Networks switches. VR-Mgmt enables remote management stations to access the switch through Telnet, SSH, or SNMP sessions; and it owns the management port. The management port cannot be deleted from this VR, and no other ports can be added. The Mgmt VLAN is created VR-Mgmt, and it cannot be deleted; you cannot add or delete any other VLANs or any routing protocols to this VR. (Referred to as VR-0 in earlier ExtremeXOS software versions.)

VRID

In VRRP, the VRID identifies the VRRP virtual router. Each VRRP virtual router is given a unique VRID. All the VRRP routers that participate in the VRRP virtual router are assigned the same VRID.

VRRP

Virtual Router Redundancy Protocol. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the master router, and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility should the master router become unavailable. In case the master router fails, the virtual IP address is mapped to a backup router's IP address; this backup becomes the master router. This allows any of the virtual router IP addresses on the LAN to be used as the default first-hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every host. VRRP is defined in RFC 2338.

VRRP router

Any router that is running VRRP. A VRRP router can participate in one or more virtual routers with VRRP; a VRRP router can be a backup router for one or more master routers.

VSA

Vendor Specific Attribute. An attribute for a RADIUS server defined by the manufacturer.(compared to the RADIUS attributes defined in the original RADIUS protocol RFC 2865). A VSA attribute is defined in order that it can be returned from the RADIUS server in the Access Granted packet to the Radius Client.

W

walled garden

A restricted subset of network content that wireless devices can access.

WEP

Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

WINS

Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer, called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS supports dynamic addressing (DHCP) by maintaining a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.

WLAN

Wireless Local Area Network.

WMM

Wi-Fi Multimedia (WMM), a Wi-Fi Alliance certified standard that provides multimedia enhancements for Wi-Fi networks that improve the user experience for audio, video, and voice applications. This standard is compliant with the IEEE 802.11e Quality of Service extensions for 802.11 networks. WMM provides prioritized media access by shortening the time between transmitting packets for higher priority traffic. WMM is based on the Enhanced Distributed Channel Access (EDCA) method.

WPA

Wireless Protected Access, or Wi-Fi Protected Access is a security solution adopted by the Wi-Fi Alliance that adds authentication to WEP's basic encryption. For authentication, WPA specifies IEEE 802.1x authentication with Extensible Authentication Protocol (EAP). For encryption, WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet. Certificate Authentication (CA) can also be used. Also part of the encryption mechanism are 802.1x for dynamic key distribution and Message Integrity Check (MIC) a.k.a. Michael.

WPA requires that all computers and devices have WPA software.

WPA-PSK

Wi-Fi Protected Access with Pre-Shared Key, a special mode of WPA for users without an enterprise authentication server. Instead, for authentication, a Pre-Shared Key is used. The PSK is a shared secret (passphrase) that must be entered in both the AP or router and the WPA clients.

This pre-shared key should be a random sequence of characters at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. After the initial shared secret, the Temporal Key Integrity Protocol (TKIP) handles the encryption and automatic re-keying.

X

XENPAK

Pluggable optics that contain a 10 Gigabit Ethernet module. The XENPAKs conform to the IEEE 802.3ae standard.

XNV

Extreme Network Virtualization. This ExtremeXOS feature enables the software to support VM port movement, port configuration, and inventory on network switches.