



# IA-A-20 and IA-A-300 Installation Guide

*Extreme Management Center® Extreme Access  
Control Engine*

Copyright © 2017 All rights reserved.

## 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](http://www.extremenetworks.com/company/legal/trademarks)

## Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: <http://www.extremenetworks.com/support/contact/>

For product documentation online, visit: <https://www.extremenetworks.com/documentation/>

# Table of Contents

---

<b>About this Guide.....</b>	<b>4</b>
Text Conventions.....	4
Providing Feedback to Us.....	5
Getting Help.....	5
Related Publications.....	5
<b>Chapter 1: Engine Overview and Setup.....</b>	<b>7</b>
Kit Contents.....	7
Specifications.....	7
Front Panel Features.....	9
Back Panel Features.....	10
Removing and Installing the Front Bezel.....	11
Installing the Engine into a Rack.....	12
<b>Chapter 2: Configuration.....</b>	<b>14</b>
Pre-Configuration Tasks.....	14
Configuring the Engine.....	14
Changing Engine Settings.....	18
Upgrading Engine Software.....	20
<b>Chapter 3: Reinstalling Engine Software.....</b>	<b>21</b>
<b>Appendix A: Product Regulatory and Compliance Information.....</b>	<b>22</b>
<b>Appendix B: Glossary.....</b>	<b>27</b>
A.....	27
B.....	29
C.....	31
D.....	34
E.....	37
F.....	40
G.....	42
H.....	42
I.....	43
J.....	46
L.....	46
M.....	48
N.....	51
O.....	52
P.....	54
Q.....	57
R.....	57
S.....	59
T.....	63
U.....	65
V.....	65
W.....	67
X.....	68

# About this Guide






This document describes the installation and initial configuration of the Extreme Networks® Extreme Access Control IA-A-20 and IA-A-300 hardware engines.

This document is intended for experienced network administrators who are responsible for implementing and maintaining communications networks.

## 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	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 <b>enter</b> and <b>type</b>	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.”
<b>[Key]</b> names	Key names are written with brackets, such as <b>[Return]</b> or <b>[Esc]</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>[Ctrl]+[Alt]+[Del]</b>
<i>Words in italicized type</i>	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.

---

## 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](mailto:internalinfodev@extremenetworks.com).

---

## Getting Help

---

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

- **GTAC (Global Technical Assistance Center) for Immediate Support**
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)
  - **Email:** [support@extremenetworks.com](mailto: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 Networks 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 RMA (Return Material Authorization) numbers

---

## Related Publications

---

### Extreme Management Center™ Documentation

Extreme Management Center (EMC, formerly NetSight) documentation, including release notes, are available at: <http://documentation.extremenetworks.com>.

Extreme Management Center online help is available by clicking the ? icon in all EMC pages. The online help provides detailed explanations of how to configure and manage your network using EMC.

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

- *Application Analytics PV-A-300 Engine Installation Guide*
- *Application Analytics Deployment Guide*

## Other Documentation

- *ExtremeXOS 21.1 Command Reference Guide*
- *ExtremeXOS Release Notes*
- *ExtremeXOS 21.1 User Guide*

# 1 Engine Overview and Setup

**Kit Contents**  
**Specifications**  
**Front Panel Features**  
**Back Panel Features**  
**Removing and Installing the Front Bezel**  
**Installing the Engine into a Rack**

This chapter lists the components shipped with the IA-A-20 and IA-A-300 engines, describes the front and back panels, and provides information on engine specifications.

For complete regulatory compliance and safety information, refer to the document *Intel® Server Products Product Safety and Regulatory Compliance*, available at the following links:

[http://download.intel.com/support/motherboards/server/sb/g23122003\\_safetyregulatory.pdf](http://download.intel.com/support/motherboards/server/sb/g23122003_safetyregulatory.pdf)  
<http://extranet.extremenetworks.com/downloads/pages/NMS.aspx>

If you use the extranet URL, after entering your email address and password, you will be on the Extreme Management Center page. Follow this path to the document:

**Documentation > Manuals & Release Notes > select a version > Mobile IAM and NAC Appliances.**

## Kit Contents

The appliance ships with the following components:

- Extreme Networks URL card
- Front bezel label
- A rack mounting kit
- Two rack handles and appropriate screws
- AC power cord bracket and cable clamp kit
- One USB flash drive

## Specifications

The physical specifications for the engines are listed in [the table below](#). The environmental requirements are listed in [Table 4](#) on page 9.

**Table 3: IA-A-20 and IA-A-300 Physical Specifications**

Processor	
Processor type	IA-A-20 - Intel® Xeon® E5-2620 processor IA-A-300 - Dual Intel® Xeon® E5-2620 processors

**Table 3: IA-A-20 and IA-A-300 Physical Specifications (continued)**

Processor speed	2.0 GHz
Internal cache	15 MB per processor
System bus speed	7.20 GT/s (Gigatransfers per second)
System bus type	QPI (Quick Path Interconnect)
<b>Memory</b>	
Architecture	1333MHz Dual Ranked Registered (RDIMM) ECC DDR3
Memory module sockets	Twenty-four 240-pin
Memory module capacities	2 GB RDIMMs
Minimum RAM (included)	12 GB (six 2 GB RDIMMs)
Maximum RAM	48 GB (twenty-four 2 GB RDIMMs)
<b>Drives</b>	
Hard drives	Two 1 TB 7200 RPM hard drives configured at RAID 1
<b>Connectors</b>	
Back	
NIC	Four RJ-45
Serial	9-pin, DTE, 16550-compatible
USB	Three 4-pin, USB 2.0-compliant
Video	15-pin VGA
Front	
USB	Two 4-pin, USB 2.0-compliant
<b>Power</b>	
AC power supply (per power supply)	Redundant power supply
Wattage	750 watts
Input voltage	<ul style="list-style-type: none"> <li>• 100 - 127 V at 50/60 Hz 8.2 A</li> <li>• 200 - 240 V at 50/60 Hz 4.4 A</li> </ul>
Output voltage	<ul style="list-style-type: none"> <li>• 62.0A at 12 V</li> <li>• 2.1A at 12 VSB</li> </ul>
<b>Physical</b>	
Height	4.45 cm (1.75 in.)
Width	43.0 cm (16.93 in.)
Depth	70.99 cm (27.95 in.)
Weight (maximum configuration)	26.1 kg (57.54 lb.)

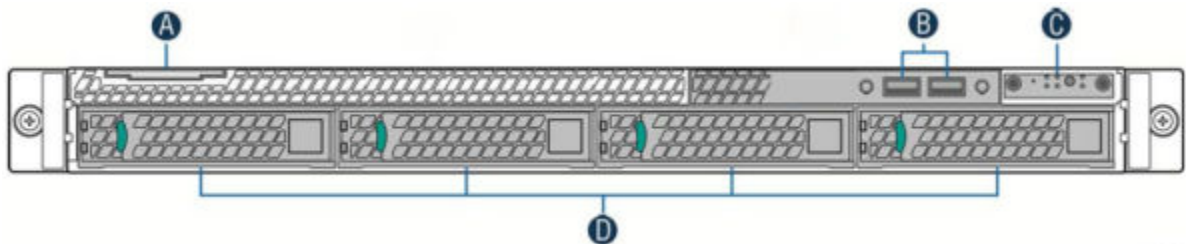


**Table 4: IA-A-20 and IA-A-300 Environmental Specifications**

Parameter	Limits
Operating temperature	+10°C to +35°C with the maximum rate of change not to exceed 10°C per hour
Storage temperature	-40°C to +70°C
Storage humidity	90%, non-condensing at 35°C
Vibration, unpackaged	5 Hz to 500 Hz, 2.20 g RMS random
Shock, operating	Half sine, 2 g peak, 11 milliseconds
Shock, unpackaged	Trapezoidal, 25 g, velocity change 136 inches/second (40 lbs to < 80 lbs)
Shock, packaged	Non-palletized free fall in height 24 inches (40 lbs to < 80 lbs)
ESD	±12 KV except I/O port ±8 KV per Intel® Environmental test specification
Estimated thermal dissipation	1550 BTU/Hr

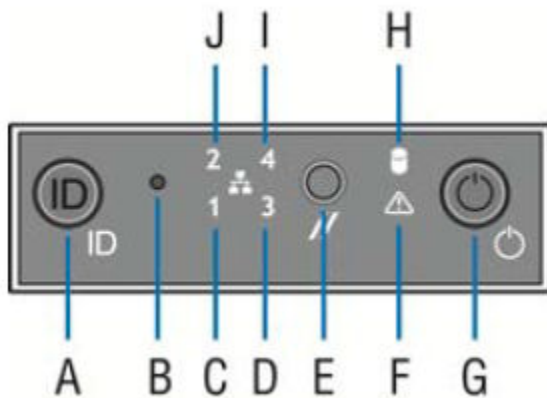
## Front Panel Features

The figure below shows the front panel features. Figure 2 on page 9 shows the front control panel.



**Figure 1: IA-A-20 and IA-A-300 Front Panel Features**

A	System label pull-out	C	Front control panel (see Figure 2 on page 9)
B	USB 2.0 port	D	Hard disk drive bays



**Figure 2: Front Control Panel**

A	System ID button w/integrated LED	F	System status LED
B	NMI button (recessed, tool required for use)	J	Power button w/integrated LED
C	Mgmt port activity LED	H	Hard drive activity LED
D	Not used	I	Not used
E	System cold reset button	J	Not used

## Hard Drive LED Indicator Patterns

The hard drive has two LED indicators visible from the front of the system: one is a green LED for disk activity, and the other is amber and indicates hard drive status. The LEDs have the following states, as described in [the tables below](#).

**Table 5: Hard Drive Activity LED Indicator Patterns**

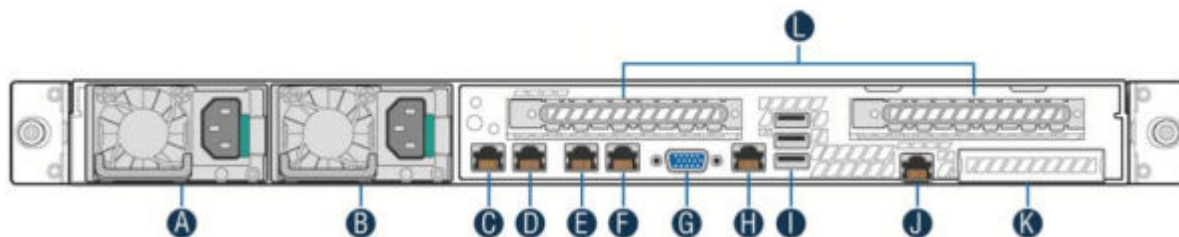
Hard Drive Condition	Activity LED Patterns
Power on and drive spinning up or spinning down	Off
Power on with drive activity	Blinking green

**Table 6: Hard Drive Status LED Indicator Patterns**

Hard Drive Condition	Status LED Patterns
No access or no fault	Off
Hard drive fault has occurred	Solid amber

## Back Panel Features

The figure below shows the back panel.



**Figure 3: IA-A-20 and IA-A-300 Back Panel**

A	Power supply module #1	F	Video connector
B	Power supply module #2	J	Not used
C	eth0, Mgmt Port, 1 GbE RJ45	H	USB 2.0 ports
D	eth1	I	Not used
E	eth2	J	Not used
F	eth3	G	Not used

The following table describes the LEDs for the RJ45 management port.

**Table 7: RJ45 Port LEDs (Management Port)**

LED Type	LED Pattern	Status Indication
Network speed (right)	Off	10 Mbps
	Amber	100 Mbps
	Green	1000 Mbps
Link activity (left)	Off	No link
	Solid green	Active link
	Blinking green	Data traffic activity

## Power Supply Status Indicator Patterns

The engine has two power supplies, supplying hot-pluggable power redundancy. The system distributes the power load across both power supplies to maximize efficiency.

Each power supply has a single bi-color LED to indicate power supply status, as described in the table below.

**Table 8: Power Supply Status LED Indicator Patterns**

Power Supply Condition	LED Pattern
Output on and OK	Green
No AC power to all power supplies	Off
AC present / Only 12VSB on (PS off) or PS in cold redundant state	1Hz blinking green
AC power cord unplugged or AC power lost. With a 2nd PS in parallel still with AC input power	Amber
Power supply warning events where PS continues to operate — high temp, high power, high current, slow fan	1Hz blinking amber
Power supply critical event causing a shutdown, failure, OCP, OVP, fan fail	Amber
Power supply firmware updating	2Hz blinking green

## Removing and Installing the Front Bezel

The engine comes with an optional front panel bezel that you can attach to the front of the chassis by snapping the bezel onto the chassis handles. A key lock allows you to lock the bezel in place so that front panel controls cannot be used. You can still monitor system status indicators with the bezel in place.

### Removing the Front Bezel

To remove the front bezel:

- 1 Unlock the bezel if it is locked.
- 2 Remove the left end of the front bezel from rack handle.
- 3 Rotate the front bezel counterclockwise to release the latches on the right end from the rack handle.

## Installing the Front Bezel



### Note

Before installing the bezel, you must install the rack handles. See [Installing the Engine into a Rack](#) on page 12.

To install the front bezel:

- 1 Lock the right end of the front bezel to the rack handle.
- 2 Rotate the front bezel clockwise till the left end clicks into place.
- 3 Lock the bezel, if needed.

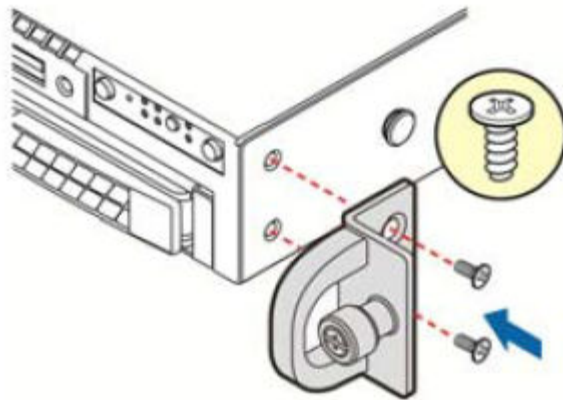
## Installing the Engine into a Rack

A rack mounting kit and installation guide are included with the engine. The rack mounting kit allows you to install the engine into a four-post rack cabinet. Refer to the installation guide for complete installation instructions.

If you are table mounting the engine, ensure at least 6 cm of clearance on all sides of the engine for proper ventilation.

If you are installing the engine in a rack:

- 1 Install the rack handles by aligning a rack handle with the two holes on each side of the engine and attaching each handle to the engine with two screws as shown in [the figure below](#).



**Figure 4: Installing the Rack Handles**

- 2 Read the installation guide included with the rack mounting kit.
- 3 Install the rails and mount the controller in the rack as instructed.

## Torque Values

The following table describes the recommended torque values to use when installing the engine using standard threaded fastener machine screws and bolts.

**Table 9: Recommended Torque Values by Screw Size**

Screw Size		Torque in Pounds			Bit Size
English	Metric	-%5	Nominal	+%5	
N/A	N/A	1.42	1.5	1.57	0
2 - 56	1.5	2.85	3.0	3.15	0
4 - 40	2.5	4.75	5.0	5.25	0/1
6 - 32	3.5	8.55	9.0	9.45	1
8 - 32	4.5	17.10	18.0	18.90	2
10 - 32	5	30.40	32.0	33.60	2
1/4 - 20	6.5	63.65	67.0	70.35	3

# 2 Configuration

Pre-Configuration Tasks  
Configuring the Engine  
Changing Engine Settings  
Upgrading Engine Software

Once you have installed the engine into a rack, you need to connect a monitor and a USB keyboard, connect the power cord and network cable, and power the engine on (see [Figure 1](#) on page 9 and [Figure 3](#) on page 10).

After the engine boots and the engine installation is complete, you must go through the initial configuration process described in this chapter.

This chapter also includes information on how to change your engine settings following your initial configuration, (see [Changing Engine Settings](#) on page 18).

## Pre-Configuration Tasks

Ensure that you have the following information prior to executing any of the procedures in this chapter:

- Engine hostname, IP address, and netmask
- Default gateway IP address
- Extreme Management Center server IP address
- Name server IP address and domain name
- Network Time Protocol (NTP) server IP address

## Configuring the Engine

After the initial engine installation is complete, use the following steps to configure the engine to run the Extreme Access Control engine software:

- 1 Login as root with no password, and press [Enter].  
The following screen appears.

```
=====
Extreme Networks - Network Access Control Appliance
Welcome to the NAC Appliance Setup
=====

Please enter the information as it is requested to continue with
the configuration. Typically a default value is displayed in brackets. Pressing the
[enter] key without entering a new value will use the bracketed value and proceed to
the next item.

If a default value cannot be provided, the prompt will indicate that the item is either
(Required) or (Optional). The [enter] key may be pressed without entering data for
```

(Optional) items. A value must be entered for (Required) items.

At the end of the setup process, the existing settings will be displayed and opportunity will be provided to correct any errors.

=====

Press [enter] to begin setup or CTRL-C to exit:

- 2 Press [Enter] to begin the setup.

The **Root Password Configuration** screen appears:

=====

Root Password Configuration

=====

There is currently no password set in the system administrator account (root). It is recommended that you set one that is active the first time the machine is rebooted.

=====

Would you like to set a root password (y/n) [y]?

- 3 Press [Enter] to set a new root password. Enter the new password as prompted.

Enter new UNIX password:

Retype new UNIX password:

Password updated successfully.

- 4 In the **NAC Gateway Configuration** screen, enter the requested information for each line and press [Enter].

=====

NAC Gateway Configuration

=====

Enter the hostname for the appliance [nacappliance]:  
 Please enter the IP address for <hostname> (Required):  
 Enter the IP netmask [255.255.255.0]:  
 Enter the gateway address [192.168.2.1]:  
 Enter the IP address of the name server (Optional):  
 Enter the IP address of an alternate name server (Optional):  
 Enter the domain name for <hostname> (Optional):  
 Enter the IP address of the Extreme Management Center Server (Required):

- 5 In the **SNMP Configuration** screen, enter the requested information for each line and press [Enter].

=====

SNMP Configuration

=====

The following information will be used to configure SNMP management of this device. The SNMP information entered here must be used to contact this device with remote management applications such as Extreme Management Center Console.

=====

Please enter the SNMP user name [snmpuser]:  
 Please enter the SNMP authentication credential [snmpauthcred]:  
 Please enter the SNMP privacy credential [snmpprivcred]:



- In the **Configure Date and Time Settings** screen, select whether you want to use an external Network Time Protocol (NTP) server. Enter **y** to use NTP, and enter your NTP server IP address(es). Enter **n** to configure the date and time manually and proceed to step 8 on page 16.

```

=====
Configure Date And Time Settings
=====
The appliance date and time can be set manually or using an external Network Time
Protocol (NTP) server. It is strongly recommended that
NTP is used to configure the date and time to ensure accuracy of time
values for SNMP communications and logged events. Up to 5 server
IP addresses may be entered if NTP is used.
=====
Do you want to use NTP (y/n) [y]? y
Please enter a NTP Server IP Address (Required): 144.131.10.120
Would you like to add another server (y/n) [n]? y
Please enter a NTP Server IP Address (Required): 144.131.10.121
Would you like to add another server (y/n) [n]? n
    
```

- In the NTP validate selection screen, enter 0 to accept the current settings and proceed to the Set Time Zone screen at step 10 on page 17.

```

=====
NTP Servers
=====
These are the currently specified NTP servers. Enter 0 or any key other than a valid
selection to complete NTP configuration and continue.

If you need to make a change, enter the appropriate number from the choices listed
below.
144.131.10.120
144.131.10.121

0. Accept the current settings
1. Restart NTP server selection
2. Set date and time manually
=====
Enter selection [0]: 0
    
```

- If you answered no to using an NTP server to set date and time, set the date and time in the **Set Date and Time** screen.

```

=====
Set Date And Time
=====
The current system date and time is: Thu Apr 24 09:34:08 2008
Please enter the values for date and time as directed where input is expected in the
following format:

MM - 2 digit month of year
DD - 2 digit day of month
YYYY - 4 digit year
hh - 2 digit hour of day using a 24 hour clock
mm - 2 digit minute of hour
ss - 2 digit seconds
=====

Please enter the month [06]:
Please enter the day of the month [24]:
Please enter the year [2013]:
Please enter the hour of day [09]:
Please enter the minutes [34]:
Please enter the seconds [34]:
    
```

- In the **Use UTC** screen, select whether you want the system clock to be set to use UTC.

```

=====
Use UTC
    
```





```

=====
The system clock can be set to use UTC. Specifying no for using UTC, sets the hardware
clock using localtime.
=====
Do you want to use UTC (y/n) [n]?

```

- 10 In the **Set Time Zone** screen, select the appropriate time zone and press [Enter].

```

=====
Set Time Zone
=====
You will now be asked to enter the time zone information for this system. Available
time zones are stored in files in the
/usr/share/zoneinfo directory.
Please select from one of the following example time zones:

1. US Eastern
2. US Central
3. US Mountain
4. US Pacific
5. Other - Shows a graphical list
=====

Enter selection [1]:

```

- 11 In the **Current Appliance Configuration** screen, review the current settings and press [Enter] to continue.

```

NAC Gateway Configuration:
Host Info:                <hostname>/<IP address>/<netmask>
Gateway/Name Server/Domain: <gateway>/<dns server>/<domain>
SNMP User/Auth/Privacy:    snmpuser/snmpauthcred/snmpprivcred
Extreme Management Center Server IP: <EMC server ip>

Press [enter] to continue:

```

- 12 In the **Appliance Network Configuration Complete** screen, you can accept the current configuration or modify the settings.

```

=====
Appliance Network Configuration Complete
=====
Configuration of the appliance network settings is now complete.
Enter 0 or any key other than a valid selection to continue.
If you need to make a change, enter the appropriate number from
the choices listed below.
=====

0. Accept the current settings
1. Edit NAC Appliance settings
2. Edit SNMP settings
3. Edit date and time
4. Modify all settings
=====

Enter selection [0]:

```

When you see the following screen, configuration is complete.

```

=====
Extreme Networks - Network Access Control Appliance - Setup Complete
=====

Setup of the NAC Appliance is now complete. Details of the appliance setup process are
located in the log files in the /var/log/install directory.

```



=====

You are now ready to use NAC Manager to manage your engine. If this is your initial commissioning of the engine, you can launch NAC Manager and view the Getting Started video available on the **Welcome** tab.

If you have reinstalled your Extreme Access Control engine software, use NAC Manager to enforce the engine. Enforcing writes your NAC Manager configuration information to the engine.

## Changing Engine Settings

This section provides instruction for changing your engine settings following your initial engine configuration, should the need arise. Depending on the settings you want to change, you can use either NAC Manager or the engine CLI to make the changes.

### Using NAC Manager

Use NAC Manager to easily change appliance settings including DNS, NTP, SSH, and SNMP configuration. You can also use NAC Manager to change the engine hostname and default gateway, as well as configure static routes for advanced routing configuration.

#### *Changing DNS, NTP, SSH, and SNMP Settings*

Use the **Network** tab in the **NAC Manager Appliance Settings** window to change the following:

- DNS Configuration — Search domains and DNS servers
- NTP Configuration — Time zone and NTP servers
- SSH Configuration — Port number and RADIUS authentication
- SNMP Configuration — SNMP credentials for the engine

To access the **Network** tab in the **Appliance Settings** window:

- 1 From the NAC Manager menu bar, select **Tools > Management and Configuration > Advanced Configurations**.

The **Advanced Configuration** window opens.

- 2 In the left-panel tree, expand the Global and Appliance Settings folder and then expand the Appliance Settings folder.
- 3 Click on the desired appliance settings (typically Default unless you have configured a custom engine setting).
- 4 In the right panel, select the **Network** tab to change your engine configurations.

For more information, see the "New/Edit Appliance Settings Window" topic in the NAC Manager online Help.

#### *Changing Hostname, Gateway, and Static Routes*

In NAC Manager, use the Interface Summary section of the **Configuration** tab for an engine to change the engine hostname, default gateway, and static routes.

- 1 Select the engine in the NAC Manager left-panel tree.
- 2 Select the right-panel **Configuration** tab.
- 3 In the Interface Summary section, click **Edit** to open the **Interface Configuration** window where you can change the engine hostname and default gateway.  
For more information, see the "Interface Configuration Window" topic in the NAC Manager online Help
- 4 Back in the Interface Summary section, click **Static Routes** to open the **Static Route Configuration** window where you can add or edit the static routes used for advanced routing configuration.  
For more information, see the "Static Route Configuration Window" topic in the NAC Manager online Help.

## Using the Appliance CLI

Use the appliance CLI to change the appliance IP address, Extreme Management Center server IP address, and web service credentials. If desired, you can also use the CLI to change basic network settings such as appliance hostname, SNMP configuration, and date and time settings, although you should use NAC Manager to make these changes, if possible (see [Using NAC Manager](#) on page 18).

### *Changing the Extreme Management Center Server IP Address*

To change the IP address of the Extreme Management Center server, enter the following command at the appliance CLI:

```
/opt/nac/configMgmtIP <IP address>
```

Then, start using the new Extreme Management Center server by typing:

```
nacctl restart
```

### *Changing Web Service Credentials*

The web service credentials provide access to the NAC Appliance Administration web page and the web services interface between the Extreme Management Center server and the NAC appliance. Appliances ship with a preconfigured default password.

If you change the web service credentials in NAC Manager (in the Appliance Settings), the new credentials automatically propagate to the new appliance when you enforce the appliance.

In the event that you need to manually change the web service credentials on the appliance, enter the following command at the appliance CLI:

```
/opt/nac/configWebCredentials <username> <password>
```

Then, restart the appliance by typing:

```
nacctl restart
```

### *Changing the Appliance IP Address and Basic Network Settings*

To change the appliance IP address, as well as basic network settings such as hostname and SNMP configuration (including system contact, system location, trap server, SNMP trap community string, SNMP user, SNMP authentication, and SNMP privacy credentials), enter the following command at the appliance CLI:

```
/usr/postinstall/nacconfig
```

This will start the network configuration script and allow you to make the desired changes.

### *Changing Date and Time Settings*

To enable or disable NTP for appliance date and time, or to manually set the date and time on the appliance, enter the following command at the appliance CLI:

```
/usr/postinstall/dateconfig
```

This will start the date and time configuration script and allow you to change the settings.

## Upgrading Engine Software

---

Upgrades to the Extreme Access Control engine software are available on the Extreme Management Center web page: <http://extranet.extremenetworks.com/downloads/pages/NMS.aspx>. After entering your email address and password, you will be on the Extreme Management Center page. Click on the **Software** tab and select a version of Extreme Management Center. Scroll down to see the Access Control engine images.

Instructions for performing the software upgrade are also available on the Extreme Management Center web page. Click on the **Documentation** tab and follow this path to the document:

**Manuals & Release Notes > select a version > Extreme Access Control.**

# 3 Reinstalling Engine Software

---

Use the procedure in this chapter to reinstall the engine software, in the event a software reinstall becomes necessary. Be aware that this procedure reformats the hard drive and reinstalls all the engine software, the operating system, and all related Linux packages.

You will need to connect a monitor and a USB keyboard to the engine prior to performing these steps.

- 1 On a Windows platform system, go to the Extreme Management Center web page to download the Extreme Access Control Engine Image 64bit (ZIP) file to your system:

<http://extranet.extremenetworks.com/downloads/pages/NMS.aspx>

After entering your email address and password, you will be on the Extreme Management Center page. Click on the **Software** tab and select a version of EMC. Scroll down to the Access Control Engine Image 64bit (ZIP) file and extract the file to a directory on your system.

- 2 Insert the USB flash drive that came with the engine into the USB port on your system and note the drive letter it is assigned.
- 3 Open a command prompt window and cd to the directory where you extracted the file.
- 4 Type `make_disk.bat <drive letter>:`. Since the reinstall procedure reformats the drive, be sure you have specified the correct drive letter. Press **[Enter]**.

The files will be copied to the USB flash drive. When the copy is complete you will see the message: `Successfully installed into <drive letter>: Press any key to continue.`

- 5 Remove the USB flash drive from your system.
- 6 Insert the USB flash drive into a USB port on the appliance (see [Figure 1](#) on page 9).
- 7 Boot the engine from the USB drive using either of these two methods.
  - Method 1:
    - 1 Press the power button, and then press F6 to go to the Boot Menu.
    - 2 Select the USB drive on the menu.
    - 3 The engine starts booting from the USB flash drive.
    - 4 When the boot is complete, the Appliance (Engine) Installation screen appears and the installation begins.
  - Method 2:
    - 1 Press the power button, and then press F2 to go to the BIOS setup.
    - 2 Use the arrow keys to navigate to the Boot Options menu.
    - 3 Ensure that the USB flash drive is listed as Boot Option #1 at the top.
    - 4 Save changes and exit.
    - 5 The engine starts booting from the USB flash drive.
    - 6 When the boot is complete, the Appliance Installation screen appears and the installation begins.
- 8 After the installation completes, reboot the engine and remove the USB flash drive.
- 9 Proceed to [Configuration](#) on page 14, and follow the instructions for configuring the engine.

# A Product Regulatory and Compliance Information

---

For complete regulatory compliance and safety information, refer to the document Intel® Server Products Product Safety and Regulatory Compliance, available at the following links:

[http://download.intel.com/support/motherboards/server/sb/g23122003\\_safetyregulatory.pdf](http://download.intel.com/support/motherboards/server/sb/g23122003_safetyregulatory.pdf)  
<https://extranet.enterasys.com/downloads/pages/NMS.aspx>

## Federal Communications Commission (FCC) Notice

This product 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 product uses, generates, and can radiate radio frequency energy and if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference to radio communications. Operation of this product in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

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.

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

Intel Corporation  
5200 N.E. Elam Young Parkway  
Hillsboro, OR 97124-6497  
Phone: 1-800-628-8686

## Industry Canada, Class A

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

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le Ministre Canadien des Communications.

## CE Notice

This product has been determined to be in compliance with 2006/95/EC (Low Voltage Directive), 2004/108/EC (EMC Directive).

## 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。

## 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。**

## 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 Enterasys Customer Support at +353 61 705500 (Ireland).



## 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 <sup>6+</sup> )	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)	×	○	○	○	○	○
塑料和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	○	○
电路开关 (Circuit Breakers)	○	○	○	○	○	○

○： 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's 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.



## Declaration of Conformity

Application of Council Directive(s):	2004/108/EC 2006/95/EC 2011/65/EU
Manufacturer's Name:	Extreme Networks, Inc.

Manufacturer's Address:	145 Rio Robles San Jose, CA 95134 USA
European Representative Name:	Enterasys Networks Limited
European Representative Address:	Nexus House, Newbury Business Park London Road, Newbury Berkshire RG14 2PZ, England
Conformance to Directive(s)/Product Standards:	EC Directive 2004/108/EC EN55022:2006 A1:2007 EN 55024:1998 A1:2001 A2:2003 EN 61000-3-2:2006 A1:2009 A2:2009 EN 61000-3-3:2008 EC Directive 2006/95/EC EN 60950-1:2006 A1:2009 EN 60825-1:2007 EN 60825-2:2004 A1:2007 EC Directive 2011/65/EU
Equipment Type/Environment:	Information Technology Equipment, for use in a Commercial or Light Industrial Environment.

The object of the declaration described above is in conformity with 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.

# B 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, autonegotiation 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 X440-G2 series switch), certain ports can be used as either copper or fibre 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 21.1 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 21.1 User Guide](#).

**dBm**

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

**DCB**

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.

**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 21.1 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 . 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 21.1 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 "Fabric Modules" in the *ExtremeSwitching 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 21.1 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 and SummitStacks, hitless failover means that designated configurations survive a change of primacy between the two MSMs (modular switches) or master/backup nodes (SummitStacks) with all details intact. Thus, those features run seamlessly during and after control of the system changes from one MSM or node 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 Extreme Management Center 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 a 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 "Management Modules" in the [ExtremeSwitching 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 or Rendezvous 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 PMBR 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 an 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 21.1 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 21.1 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](http://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.

**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).

Time-Sensitive Networking. Standards under development by the Time-Sensitive Networking task group of the IEEE 802.1 working group. There are various characteristics of TSN, including packet preemption, prioritized packet queuing, congestion control, bandwidth reservation, and transmit latency determination used to guarantee that data packets always arrive within a certain predetermined window of time.

**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 discontinuous 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.