



Switch Configuration with Chalet

For ExtremeXOS 16.2 and Earlier

Copyright © 2016 Extreme Networks, Inc. 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

Support

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

For information, contact:

Extreme Networks, Inc.

6480 Via Del Oro

San Jose, California 95119

USA

Table of Contents

Preface	5
Text Conventions.....	5
Providing Feedback to Us.....	5
Getting Help.....	6
Related Publications.....	6
Chapter 1: About Chalet	8
Chalet Features.....	8
Chapter 2: Getting Started with Chalet	9
Setting up the Switch.....	9
Logging In.....	10
Using the Quick Setup Wizard.....	11
Chapter 3: Chalet Dashboard	16
System Information	17
PoE Port List	19
Power and Cooling	21
Slots	22
Chapter 4: Configuring a Switch in Chalet	23
Configuring Ports.....	23
Configuring VLANs.....	27
Configuring Dynamic ACLs.....	31
Configuring Audio Video Bridges.....	37
Configuring Chalet Settings.....	38
Chapter 5: Monitoring a Switch	40
Monitoring Events.....	40
Monitoring System Performance.....	41
Monitoring Port Utilization.....	42
Monitoring Quality of Service.....	43
Monitoring User Sessions.....	43
Chapter 6: Managing Accounts	45
Adding Users.....	45
Deleting Users.....	46
Changing User Passwords.....	46
Account Security.....	47
Appendix A: Glossary	51
A.....	51
B.....	54
C.....	55
D.....	60
E.....	63
F.....	67
G.....	69
H.....	70
I.....	71

J.....	75
L.....	75
M.....	77
N.....	81
O.....	82
P.....	84
Q.....	87
R.....	88
S.....	91
T.....	95
U.....	97
V.....	98
W.....	101
X.....	102



Preface

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 enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc] . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
<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.

Getting Help

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

- **Global Technical Assistance Center (GTAC) 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
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme 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 Return Material Authorization (RMA) numbers

Related Publications

ExtremeXOS Publications

- *ACL Solutions Guide*
- *ExtremeXOS 16.2 Command Reference Guide*
- *ExtremeXOS 16.2 EMS Messages Catalog*
- *ExtremeXOS 16.2 Feature License Requirements*
- *ExtremeXOS 16.2 User Guide*
- *ExtremeXOS OpenFlow User Guide*
- *ExtremeXOS Quick Guide*
- *ExtremeXOS Legacy CLI Quick Reference Guide*
- *ExtremeXOS Release Notes*

- *Extreme Hardware/Software Compatibility and Recommendation Matrices*
- *Switch Configuration with Chalet for ExtremeXOS 16.2 and Earlier*
- *Using AVB with Extreme Switches*

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing

1 About Chalet

Chalet Features

Chalet is a web-based user interface for setting up and viewing information about a switch. Chalet removes the need to know and remember commands in a CLI environment. Viewable on desktop and mobile with a quick login and intuitive navigation, Chalet features an Quick Setup mode for configuring a switch in a few simple steps. Basic data surrounding port utilization, power, and Quality of Service (QoS) are available, and more advanced users can configure multiple VLANs, create Access Control Lists (ACLs), and configure Audio Video Bridging (AVB).

Chalet is packaged with ExtremeXOS release 15.7.1 and later for all platforms, so there's nothing extra to download or install. Chalet can be launched in any modern web browser and does not depend on any outside resources to work, including Java Applets, Adobe Flash, or dedicated mobile applications.



Note

The screens shown in this guide were captured from a variety of Extreme Networks switches. The information displayed on the screen will vary depending on the switch being used.

Browser Support

Chalet is supported on all modern, standards-compliant browsers, including:

- Internet Explorer 8.0 and later
- Mozilla Firefox 3.0 and later
- Microsoft Edge (Windows 10)
- Chrome
- Safari
- Opera

Chalet Features

Chalet helps you interact with the switch outside of a CLI environment and allows you to easily:

- Configure the switch for the first time without the use of a console cable.
- View status and details of the switch and its slots and ports.
- Analyze power efficiency of power supplies, fans, and PoE ports.
- Create VLANs and ACL policies.
- Enable and disable multiple features, including QoS, AVB, auto-negotiation, and flooding.
- View recent system events.
- View device topology (stacked switches only).
- Manage users, including defining global and individual security policies.

2 Getting Started with Chalet

Setting up the Switch Logging In Using the Quick Setup Wizard

This section describes how to:

- [Set up the switch to use Chalet](#)
- [Log in to Chalet](#)
- [Configure basic switch settings](#)

Setting up the Switch

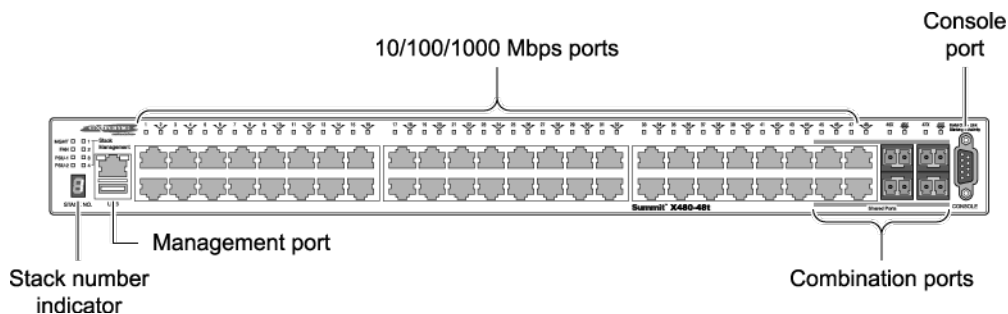
After removing the switch from the box, you would normally connect the switch using a console cable and log in directly to set it up for the first time. With Chalet, you can avoid doing this by plugging a cable into the MGMT port and letting the switch self-compute its IP address, which you will use to log into Chalet.

Zero Touch Provisioning (also known as Auto Provisioning) is enabled in ExtremeXOS 15.7 by default and directs this self-assigning behavior.

To get started:

- 1 Follow unpacking and site location instructions in the hardware manual.
- 2 Connect a cable to the management (MGMT) port.

- 3 Find the switch's IP address. There are several ways you can get this information.
 - If you have a switch with a stack number indicator window, the self-assigned IP address will scroll one digit at a time in this window. Enter this address in a web browser to log in to Chalet.



Note

Self-assigned addresses start with 169.254.x.x.

- If your switch does not have a stack number indicator window, you can get the IP address by taking the last two number/letter groups from the MAC address (printed on the switch label) and appending them to 0xa9fe (these are the HEX characters for 169.254). For example, if the last four characters of the switch's MAC address are E9 and EE, the login URL will be `http://0xa9fee9ee`.
- The last option is to convert the last two number/letter groups from the MAC address into decimal using a hex-to-decimal converter (such as www.binaryhexconverter.com/hex-to-decimal-converter). In our example, E9 and EE are converted to 233 and 238, respectively. Append these two numbers to the end of the base 169.254 IP address in order to log in to Chalet.

Logging In

- 1 To log in to the switch, enter the server's IP address (or HEX characters) in the browser window. If you do not know the switch's IP address, use one of the options in step 3 on page 10. When you've connected to the switch, the login screen displays.

Welcome to EXOS

Login

Password

Language

[Sign in](#)

- 2 Enter the user name and password. The default admin user name is 'admin' with no password.

**Note**

To create additional accounts after setup, see [Adding Users](#) on page 45.

- 3 Optional: Select your preferred language from the **Language** drop-down.

**Note**

English is the default unless your browser's default language is different.

- 4 Click **Sign in**.

The **Quick Setup** page displays automatically during first time setup when logging in with the 169.254.xx.xx address. Otherwise, the [Dashboard](#) displays.

**Note**

You will be logged out of your session after 10 minutes of inactivity. To change the default idle timeout settings, see [Configuring Chalet Settings](#) on page 38.

Using the Quick Setup Wizard

**Note**

Only the admin account can configure the switch.

The **Quick Setup** is similar to configuring the switch using a console cable, just with a web interface. [This video](#) shows the Quick Setup process documented below.

- 1 After logging in with the 169.254.xx.xx IP address, you are automatically directed to the **Quick Setup**. Otherwise, select **Configure > Quick Setup** from the top navigation.
- 2 On the **Account** page, provide a password for the admin account (this is strongly recommended), and then click **Next** to continue.

Dashboard Configure Monitoring Help Logout

Quick Setup

1 Account 2 Device 3 IP Address 4 Security 5 Summary

Account

User Name:

admin

New Password:

Password

Confirm Password

Cancel Next

- 3 On the **Device** page, enter the following information and click **Next** to continue:
- **Name:** Provide a unique name for the device.
 - **Location:** Enter the device's location.
 - **Contact:** Enter the name or phone number of the person or team responsible for this device.

The screenshot shows the 'Setup Device' page in the Chalet interface. At the top, there is a navigation bar with 'Dashboard', 'Configure', 'Monitoring', 'Help', and 'Logout'. Below this is a 'Quick Setup' section with a progress indicator showing five steps: 1. Account, 2. Device (highlighted), 3. IP Address, 4. Security, and 5. Summary. The 'Setup Device' form contains three input fields: 'Name' with the value 'tech_pubs', 'Location' with the value 'R1C2S3', and 'Contact' with the value 'Information Development'. At the bottom of the form are 'Back' and 'Next' buttons.

- 4 On the **IP Address** page, assign IP addresses for the following and click **Next** to continue:
- Default VLAN
 - Default Gateway
 - Management VLAN
 - Management Gateway

Dashboard Configure Monitoring Help Logout

Quick Setup

1 Account 2 Device 3 IP Address 4 Security 5 Summary

Assign IP Address

Default VLAN:
10.69.12.34

Default Gateway:
123.45.67.1

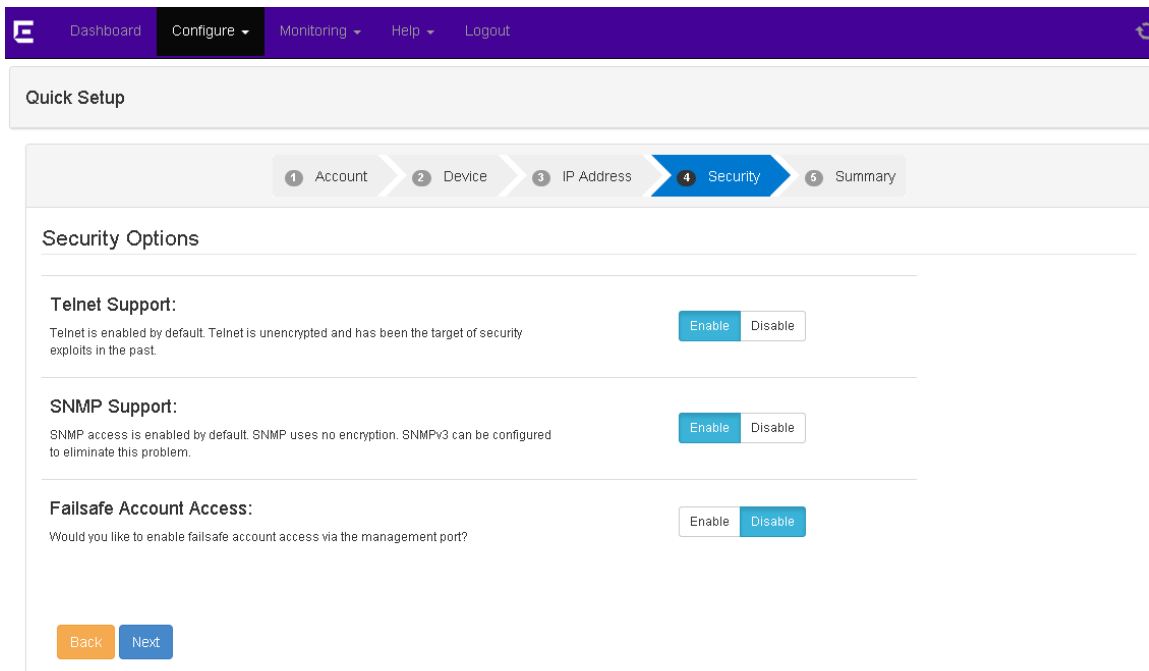
Management VLAN:
10.1.4.1

Management Gateway:
10.1.4.2

WARNING:
Without setting IP address for at least one VLAN, you will lose connection to the switch.

Back Next

- 5 On the **Security** page, you can enable or disable Telnet, SNMP, and failsafe account access. If you are unsure, leave the default and click **Next** to continue. You can always enable or disable these features later.



The screenshot shows the Chalet web interface. At the top is a navigation bar with a logo 'E' and links for Dashboard, Configure, Monitoring, Help, and Logout. Below this is a 'Quick Setup' section with a progress indicator showing five steps: 1 Account, 2 Device, 3 IP Address, 4 Security (highlighted), and 5 Summary. The main content area is titled 'Security Options' and contains three sections:

- Telnet Support:** 'Telnet is enabled by default. Telnet is unencrypted and has been the target of security exploits in the past.' There are 'Enable' and 'Disable' buttons.
- SNMP Support:** 'SNMP access is enabled by default. SNMP uses no encryption. SNMPv3 can be configured to eliminate this problem.' There are 'Enable' and 'Disable' buttons.
- Failsafe Account Access:** 'Would you like to enable failsafe account access via the management port?' There are 'Enable' and 'Disable' buttons.

At the bottom of the form are 'Back' and 'Next' buttons.



Note

If you are using (or plan to use) an external network management system such as NetSight or Ridgeline, SNMP must be enabled.

- 6 At the **Summary** page, click **Apply** to save the configuration.

Quick Setup

1 Account
2 Device
3 IP Address
4 Security
5 Summary

Summary

Account:	User Name: admin	Password:
Device:	Name	tech_pubs
	Location:	R1C2S3
	Contact:	Information Development
IP Address:	Default VLAN	
	Default Gateway	123.45.67.1
	Mgmt VLAN	10.1.4.1
	Management Gateway	10.1.4.2
Security Option:	Telnet Access	Enabled
	SNMP Access:	Enabled
	Failsafe Account Access:	Disabled

Back
Apply

You are directed back to the Dashboard. If you have configured anything incorrectly, you will see a pop-up warning dialog.

- 7 Next, change the IP address of the management workstation to the same IP subnet as the switch (the IP address you assigned during Quick Setup).

You can now log in to Chalet with the switch's newly assigned IP address.

3 Chalet Dashboard

System Information
PoE Port List
Power and Cooling
Slots

The screenshot shows the Chalet Dashboard interface. At the top is a navigation bar with the Extreme Networks logo and menu items: Dashboard, Configure, Monitoring, Help, and Logout. Below the navigation bar are several widgets:

- System:** Name: J12U16_X460, Type: X460-48t, Version: EXOS 16.2.2.3
- PoE Ports:** Total Counts: 0, Errors: 0, Warnings: 0
- Recent Events:** Critical: 0, Errors: 1, Warnings: 3
- VLANs:** 7
- Ports:** 52
- Power and Cooling:** Power Supplies: ✓, Fans: ✓
- Top 5 Ports:** 6, 5, 1, 2, 3 (all with status ✓)
- Slots:** Unit: Switch, Status: ✓, Temp.: ✓
- Last 5 Error Events:** 12/14/2016 13:31:05.83 <Error:cm.sys.actionErr> Error while loading "cfgTechSupport": Source IP address 10.68.63.86 does not belong to the VR VR-Mgmt.

At the bottom of the dashboard is a "Save Config" button and the copyright notice "© Extreme Networks".

The **Dashboard** is the home page for Chalet and displays the following information:


- System Information** Switch type and model information, including the ExtremeXOS version the switch is running. Clicking this table takes you to the [Switch Information](#) page.
- VLANs** The number of VLANs currently configured. Clicking this table takes you to the [VLAN List](#) page.
- Ports** The number of configured ports. Clicking this table takes you to the [Ports](#) page.
- Power and Cooling** List of power supplies and fans, including status of installation and operation. Clicking this table takes you to the [Power and Cooling](#) page.

PoE Ports	A list of configured Power over Ethernet ports. Not all switches are capable of PoE or may have inline-power disabled. Clicking this link takes you to the PoE Port List page.
Top 5 Ports	A list of the five most active ports. Clicking this table takes you to the Ports page.
Recent Events	The number of Warning, Critical, and Error messages from the last 48 hours of the Event Log .
Slots	Status of installed slots. Clicking this table directs you to the Devices page.
Last 5 Error Events	A list of the most recent error events. Clicking this table takes you to the Event Log page.

The following sections describe the pages and tabs that are only accessible from the Dashboard. Pages accessible from the navigation menu are described in the [Configuration](#) and [Monitoring](#) sections.

Note



When the  displays in the header, Chalet is updating. This happens when changes are being made or data is being retrieved from or sent to the switch. Chalet automatically updates every three minutes even if no changes have been made.

System Information

Clicking the **System Information** table from the Dashboard takes you to the **System Detail** page.

[Dashboard](#)[Configure](#) ▾[Monitoring](#) ▾[Help](#) ▾[Logout](#)

System

System Name	J12U16_X460
System Type	X460-48t
Location	
Contact	support@extremenetworks.com, +1 8
IP Address	10.68.63.86
MAC Address	00:04:96:83:73:F2
Switch Time	2016-12-15T00:43:14
Boot Time	2016-12-14T13:28:06
System Uptime	11 hours 15 minutes 8 seconds
Next Reboot	None scheduled

Current State

Image Selected

Image Booted

Primary Version

Secondary Version

Config Selected

Config Booted

SysHealth Check

Enabled (Normal)

Recovery Mode**License:**

Enabled License Level:

Core

Enabled Feature Packs:

[Back](#)[Edit](#)[Save Config](#)

This page displays detailed information about the switch, eliminating the need to enter multiple "show" commands (such as `show switch`, `show licenses`, and `show version`) on the switch to get the same information.

The following buttons are present on this page:

- **Edit**—Edit the System Name, Location, and Contact person. Click **Apply** to save your changes, **Restore** to go restore the default settings, or **Back** to return to the Dashboard.
- **Turn On LED**—Turn on the switch's LED panel to find the switch in a rack. The lights flash across the front of the switch from high to low. This is equivalent to running the command `enable led locator`.
- **Turn Off LED**—Turn off the switch's LED panel. This is equivalent to issuing the command `disable led locator`.
- **Reboot Switch**—Reboot the switch.

Clicking the **Inventory** tab displays the number of slots, their serial numbers, Boot ROM versions, and ExtremeXOS software version.

PoE Port List

Clicking the **PoE Ports** table from the Dashboard takes you to the **PoE Port List** (defaulting to the **Basic** tab).

Note



It is not possible to detect if PoE ports are present, so if you see the following message, either your switch is not PoE-capable or inline power is disabled.

No Power Over Ethernet ports were found on this switch. This switch may not be capable of PoE or may have inline-power disabled.

If your switch is PoE-capable, issue the command `enable inline-power ports [all | port_list]` from the CLI.

This screen shows which ports are enabled with PoE, listed in numerical order by default. The table also shows their PoE status, power (in Watts), and No Fault state, which are helpful when troubleshooting power issues. The information shown is the equivalent output of the `show inline-power info` command.

To easily see which ports are delivering power, type `delivering` in the search bar.

Port	Status	Power (Watts)	No Fault	Details
1	searching	0.0	✓	➔
2	searching	0.0	✓	➔
3	searching	0.0	✓	➔
4	searching	0.0	✓	➔
5	searching	0.0	✓	➔
6	searching	0.0	✓	➔
7	searching	0.0	✓	➔
8	searching	0.0	✓	➔
9	searching	0.0	✓	➔
10	searching	0.0	✓	➔
11	searching	0.0	✓	➔
12	searching	0.0	✓	➔
13	searching	0.0	✓	➔
14	searching	0.0	✓	➔
15	searching	0.0	✓	➔
16	searching	0.0	✓	➔
17	searching	0.0	✓	➔
18	searching	0.0	✓	➔
19	searching	0.0	✓	➔

To see more details about a port, click the ➔ to the right. You are directed to the PoE Port details screen. This is the same information displayed in the **Advanced** tab.

Dashboard
Configure
Monitoring
Help
Logout

PoE Port: 1 General

General	
Port	1
Display String	1
Inline Power	On
Status	searching
Class	-----
Volts	0.0
Current	0.0
Power	0.0
No Fault	✓

Back
Port Details
On Off

To enable or disable PoE on an individual port, click **On** or **Off** buttons at the bottom of the screen. These buttons perform the same functionality as the `enable inline-power ports` and `disable inline-power ports` commands.



Note

The port's class defines how much power the port is allowed and how the switch can get to it.

To view additional information about the port, click the **Port Details** button. This will direct you to the editable **Port Details** page. For more information about editing port information, see [Configuring Ports](#) on page 23.

Power and Cooling


Clicking the **Power and Cooling** table from the Dashboard takes you to the **Power Supplies** page. This screen shows the status of the installed power supplies.

Power Supplies	
Location	Status
1 : 1	Powered On
1 : 2	Empty

Back

The Status column will change based on the switch platform:

- P (stacked switches)
- Powered on (Summits)
- Empty or " - "

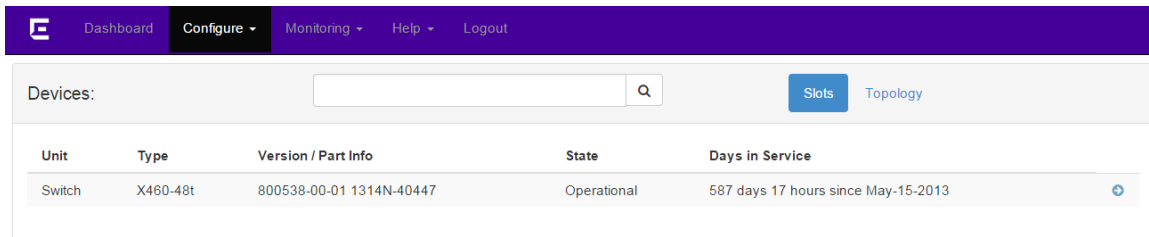
Clicking the **Fans** tab displays the location and status of installed fans. Clicking the  to the right displays more details about the fan, including number of fans, revision number, temperature, and speed.

Fans		
Location	Status	Details
1 : 01	operational	↗
1 : 02	operational	↗
1 : 03	operational	↗
1 : 04	operational	↗

Back

Slots

Clicking the **Slots** table on the Dashboard takes you to the **Devices** page. This page shows the switch name, type, version and part number, current state, and days in service.




Unit	Type	Version / Part Info	State	Days in Service
Switch	X460-48t	800538-00-01 1314N-40447	Operational	587 days 17 hours since May-15-2013

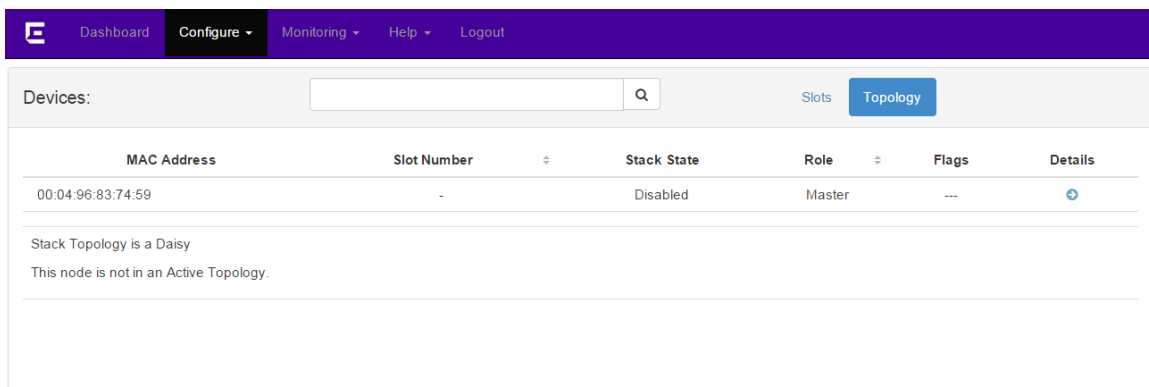
Clicking the **Topology** tab displays the type of topology (daisy, ring, etc.), and whether the topology is active. For each node in the stack, you are also provided the MAC address, stack state, role (Master/Slave), and any flags present.




Note

Topology information is available only on stacked switches.

Clicking the  to the right provides further details about the slot. You can also turn the slot's LEDs on and off, but the information shown is not editable.



MAC Address	Slot Number	Stack State	Role	Flags	Details
00:04:96:83:74:59	-	Disabled	Master	---	

Stack Topology is a Daisy
This node is not in an Active Topology.

Clicking the  to the right provides further details about the slot topology.

4 Configuring a Switch in Chalet

Configuring Ports
Configuring VLANs
Configuring Dynamic ACLs
Configuring Audio Video Bridges
Configuring Chalet Settings

The screenshot shows the Chalet web interface. At the top, there is a navigation bar with a logo 'E' and menu items: Dashboard, Configure (selected), Monitoring, Help, and Logout. A dropdown menu is open under 'Configure', listing: Quick Setup, Ports, VLANs, Dynamic ACLs, Accounts, Audio Video Bridging, and Chalet. Below the navigation bar, there are several system status cards:

- System**: Name, Type, Version
- VLANs**: 7
- Ports**: 52
- Power and Cooling**: Power Supplies, Fans
- PoE Ports**: Total Counts, Errors, Warnings
- Top 5 Ports**: 6, 5, 1, 2, 3

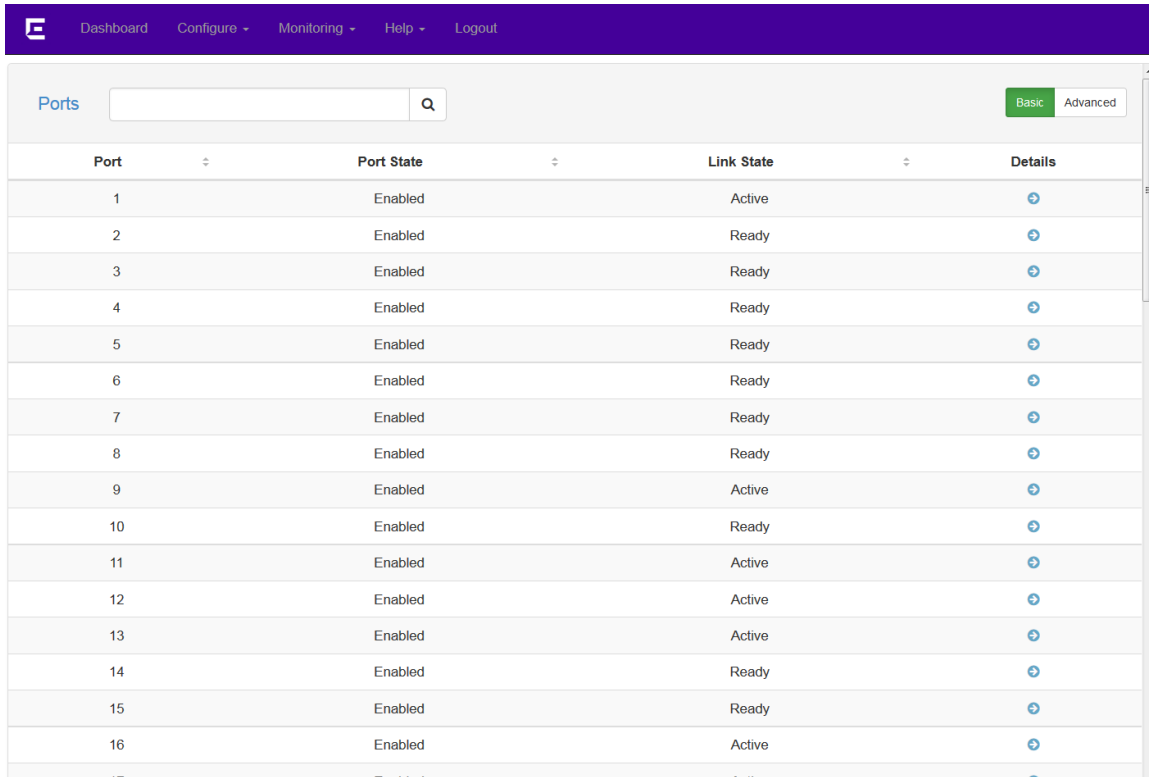
The **Configure** menu allows administrators to configure:

- **Ports**: Configure port details, including QoS profiles and VLANs.
- **VLANs**: Create and delete VLANs, and assign ports.
- **Dynamic ACLs**: Create ACL policies on the switch.
- **Accounts**: Manage user accounts and set password policies.
- **Audio Video Bridging**: Enable AVB.
- **Chalet**: Configure settings in Chalet, including session idle timeout.

Configuring Ports

Port information displays automatically after clicking the **Ports** table from the Dashboard, or selecting **Configure > Ports**.

On the **Basic** tab, the table displays each port and its port and link states. The **Advanced** tab provides flags, link speed, duplex mode, and auto negotiation state.



Port	Port State	Link State	Details
1	Enabled	Active	
2	Enabled	Ready	
3	Enabled	Ready	
4	Enabled	Ready	
5	Enabled	Ready	
6	Enabled	Ready	
7	Enabled	Ready	
8	Enabled	Ready	
9	Enabled	Active	
10	Enabled	Ready	
11	Enabled	Active	
12	Enabled	Active	
13	Enabled	Active	
14	Enabled	Ready	
15	Enabled	Ready	
16	Enabled	Active	

To change a port's details:

- 1 Click the  for the port you wish to edit.

You are directed to the **Port Details, General** tab, where you can edit basic information about the port. Clicking the **QoS**, or **VLAN** tabs allow you to create and edit additional information about the port.

Port Details

General QoS VLAN

General	
Port Number	1
Display String	<input type="text"/>
Auto Negotiation	Enabled Speed: AUTO Duplex: auto
Type	UTP
Virtual Router	VR-Default
Port State	Enabled
Link State	Ready
Link Up Count	0
Link Down Count	0
ELSM	Disabled
EDP	Enabled

Back Edit Enable Disable

- 2 Click **Edit** to change the following information:
 - Display String—A string of up to 255 characters that displays on all `show port` commands. Some characters such as <, >, ?, & are not permitted, as they have special meanings.
 - Auto Negotiation
 - If Auto Negotiation is Enabled, the Speed and Duplex will display "AUTO".
 - Click **Disable** to disable Auto Negotiation and set Speed and Duplex manually.
- 3 To save your changes, click **Apply**. If you do not want to save, choose one of the following options:
 - Click **Restore** to cancel your changes.
 - Click **Back** to return to the **Ports** page.
- 4 To disable the port entirely, click **Disable** at the bottom of the screen. To re-enable the port, click **Enable**.

Port Details -- QoS

The **Quality of Service** tab allows you to enable or disable the following traffic groups on a per-port basis:

- Ingress IPTOS Examination
- Ingress 802.1p Examination, both Examination and Inner Exam.



Note

These items are mutually exclusive.

- Egress IPTOS Replacement
- Egress 802.1p

E
Dashboard
Configure ▾
Monitoring ▾
Help ▾
Logout

Port Details General **QoS** VLAN

QoS	
QoS Profile	none
Explicit CoS Traffic Grouping Config	
Ingress IPTOS Examination	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Disable
Ingress 802.1p Examination	Examination <input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable Inner Exam <input type="checkbox"/> Enable <input checked="" type="checkbox"/> Disable
Egress IPTOS Replacement	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Disable
Egress 802.1p Replacement	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Disable
Egress Traffic Rate Limiting	
Egress Port Rate	No Limit
Max Burst Size	No Limit
Broadcast Rate	No Limit
Multicast Rate	No Limit
Unknown Destination MAC Rate	No Limit

When finished, click **Apply** to save your changes. Otherwise:

- Click **Restore** to cancel your changes.
- Click **Back** to return to the **Ports** page.

To disable the port entirely, click **Disable** at the bottom of the screen. To re-enable the port, click **Enable**.

To assign or change the QoS Profile, refer to [Configuring VLANs](#) on page 27.



Note

QoS Profiles must be created before you can assign ports. For more information, see "Configuring QoS" in the *ExtremeXOS 16.2 User Guide*.

Port Details -- VLAN

On the **VLAN** tab, you can enable or disable the following on a per-port basis:

- FDB Learning Port
- Unicast Flooding
- Multicast Flooding
- Broadcast Flooding

This page also displays what VLAN this port belongs to. To edit this, continue to [Configuring VLANs](#) on page 27.

The screenshot shows the 'Port Details' configuration page in the Chalet web interface. The page has a dark blue header with navigation links: Dashboard, Configure, Monitoring, Help, and Logout. Below the header, there are tabs for 'General', 'QoS', and 'VLAN', with 'VLAN' being the active tab. The main content area is titled 'FDB and VLAN' and contains several sections with toggle controls:

- Learning Port:** A toggle switch set to 'Enable'.
- Flooding:** A section containing three sub-sections:
 - Unicast Flooding:** A toggle switch set to 'Enable'.
 - Multicast Flooding:** A toggle switch set to 'Enable'.
 - Broadcast Flooding:** A toggle switch set to 'Enable'.
- VLAN:** A section containing one sub-section:
 - Member VLANs:** A dropdown menu currently set to 'Default'.

At the bottom of the form, there are three buttons: 'Back' (blue), 'Restore' (orange), and 'Apply' (blue). On the right side, there is a green 'Enable' button and a grey 'Disable' button.

When finished, click **Apply** to save your changes. Otherwise:

- Click **Restore** to cancel your changes.
- Click **Back** to return to the **Ports** page.

To disable the port entirely, click **Disable** at the bottom of the screen. To re-enable the port, click **Enable**.

Configuring VLANs

Chalet allows you to create and configure VLANs, tag them, and assign ports and QoS profiles. After clicking the **VLANs** table from the Dashboard, or after selecting **Configure > VLAN**, you are directed to the **VLAN List** page.

Note



Assigning VLANs into VRs is not currently supported in Chalet. Any VLANs that are created are assigned to VR-Default automatically. To create a VLAN in a different VR, create them through the CLI (see the `create vlan` command in the [ExtremeXOS 16.2 Command Reference Guide](#)).

Name	Tag	Protocol Address	Protocol	Ports Active/Total	Virtual Router	Details
Default	1	10.1.1.12 / 8	ANY	9 / 54	VR-Default	
Mgmt	4095	-	ANY	1 / 1	VR-Mgmt	
test	30	-	ANY	0 / 0	VR-Default	
VLAN_0100	100	-	ANY	0 / 0	VR-Default	
VLAN_0101	101	-	ANY	0 / 0	VR-Default	
VLAN_0102	102	-	ANY	0 / 0	VR-Default	
VLAN_0103	103	-	ANY	0 / 0	VR-Default	
VLAN_0104	104	-	ANY	0 / 0	VR-Default	
VLAN_0105	105	-	ANY	0 / 0	VR-Default	

This page displays a list of all VLANs in alphabetical order, but the list can be sorted by any column or filtered using the search bar.

Clicking the to the right of a VLAN displays the [Assign Ports](#) page.

To create a new VLAN:


- 1 Click the **Create VLAN** button.

Create VLAN

Name:	<input type="text" value="VLAN_0106"/>
Tag:	<input type="text" value="106"/>
Description:	<input type="text"/>

- 2 In the pop-up dialog, provide a name for the VLAN. This is required.
- 3 Provide a VLAN tag and description, if desired.
- 4 Click **Submit**.

You are directed back to the **VLAN List** page, with the new VLAN listed.


- 5 To edit the details of the VLAN, click the  to the right.
The **VLAN Details** page displays, showing the **General** tab by default.

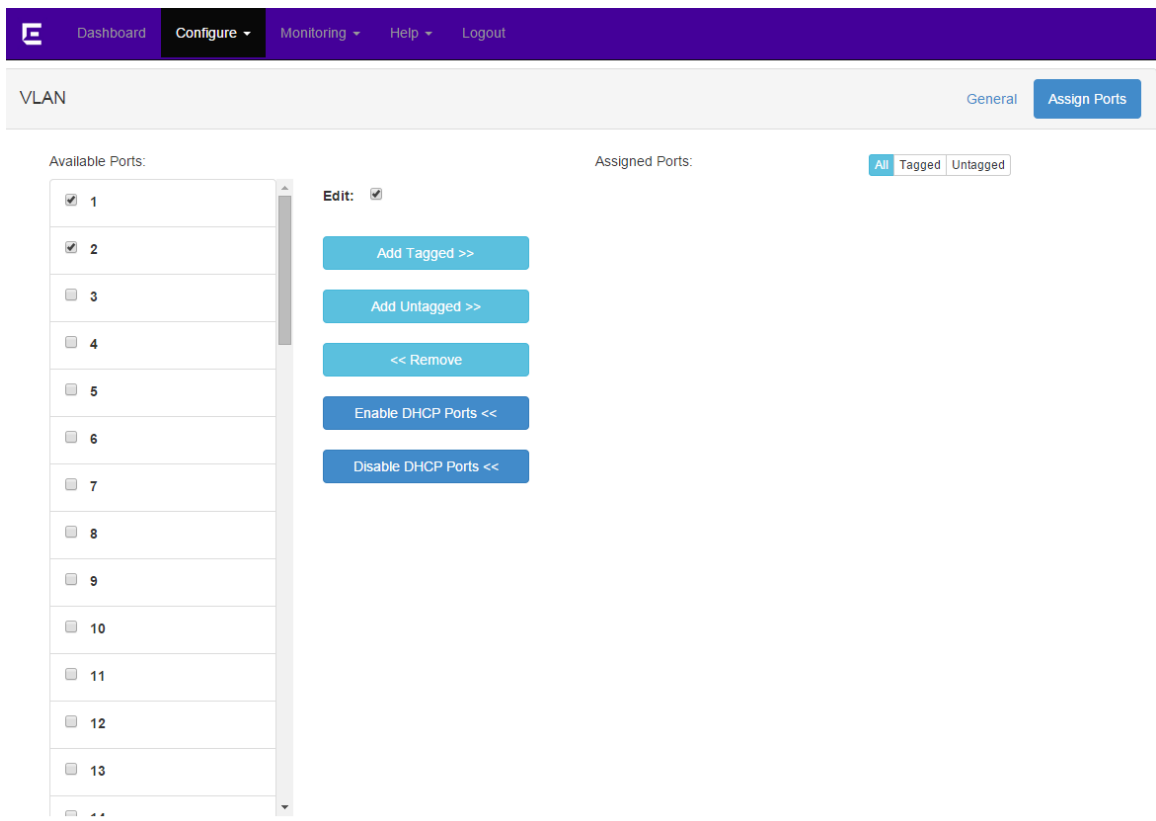
On this page, you can edit every field with a drop-down menu or a text field.
- 6 To save your edits, click **Apply**. If you do not want to save, choose one of the following options:
 - Click **Restore** to cancel your edits.
 - Click **Back** to return to the **VLAN List** page.
 - Click **Delete** to delete the VLAN and return to the **VLAN List** page.

To assign ports to the new VLAN, refer to [Assigning Ports to VLANs](#) on page 29.

Assigning Ports to VLANs


Assigning tagged and untagged ports to a VLAN is simple and quick with Chalet.

- 1 To begin, select **Configure > VLAN**, and then click the  next to the VLAN you wish to assign ports to.
The **General** tab displays.
- 2 Select the **Assign Ports** tab, and then select the **Edit** checkbox. This stops the refresh timer so the switch will not update during this configuration.
The Available Ports list and buttons become active.



The screenshot shows the Chalet web interface for configuring a VLAN. The top navigation bar includes 'Dashboard', 'Configure', 'Monitoring', 'Help', and 'Logout'. The main content area is titled 'VLAN' and has two tabs: 'General' and 'Assign Ports'. The 'Assign Ports' tab is active. On the left, there is a list of 'Available Ports' from 1 to 13. Ports 1 and 2 have their checkboxes checked. In the center, there is an 'Edit' checkbox which is checked. Below it are several buttons: 'Add Tagged >>', 'Add Untagged >>', '<< Remove', 'Enable DHCP Ports <<', and 'Disable DHCP Ports <<'. On the right, there is an 'Assigned Ports' section with a filter for 'All' (selected), 'Tagged', and 'Untagged'.

- 3 Select the check boxes next to the ports you wish to assign, and then click **Add Tagged** or **Add Untagged**
The ports move to the "Assigned Ports" area on the right.


- 4 To remove ports from the VLAN, select the ports from the Assigned Ports area and then click **Remove**.
- 5 When finished, clear the **Edit** checkbox to restart the refresh timer.
- 6 Click **Save Config** to save your changes.
- 7 To confirm that your changes have been made to the switch, click .
You are directed to the **Port Details** page.
- 8 Click the **VLAN** tab to see that the Member VLANs field has been updated.

To enable DHCP on the assigned ports, refer to [Enabling DHCP](#) on page 30.

Enabling DHCP

If desired, Chalet allows you to configure the DHCP server included in the switch, including the IP address range, IP address lease, and multiple DHCP options. For more information about this feature, see the "DHCP Server" section of the *ExtremeXOS 16.2 User Guide*.

You must first assign ports to VLANs (see [Assigning Ports to VLANs](#) on page 29) before you can enable DHCP on the ports.

- 1 To begin, select **Configure** > **VLAN**, and then click the  next to the VLAN you wish to enable DHCP on.
The **General** tab displays.
- 2 Click **Edit**.
- 3 Assign IP address ranges. The Primary IP on the VLAN is required.



Note

DHCP IP ranges must be in the same subnet.

- 4 Click **Apply** to save your changes.
- 5 Select the **Assign Ports** tab.
- 6 Select the **Edit** checkbox. This stops the refresh timer so the switch will not update during this configuration.
- 7 Select the ports you just added and then click **Enable DHCP Ports**.
- 8 When finished, clear the **Edit** checkbox to restart the refresh timer.
- 9 Click **Save Config** to save your changes.
- 10 To confirm your changes, return to the **General** tab. The **DHCP Ports** area will display the ports enabled with DHCP.
- 11 To disable DHCP ports, return to the **Assign Ports** tab and select the **Edit** checkbox.
- 12 Select the ports from the Assigned Ports area and then click **Disable DHCP Ports**.
- 13 When finished, clear the **Edit** checkbox to restart the refresh timer.
- 14 Click **Save Config** to save your changes.
- 15 To confirm your changes, return to the **General** tab to see the updated **DHCP Ports** area.

Configuring Dynamic ACLs

The **Dynamic Access Control Lists** page allows you to create dynamic rules for Access Control Lists (ACLs) and is equivalent to entering the command `create access-list dynamic_rule conditions actions {non_permanent}` with its different variables.



Note

For more information, refer to the [ACL Solutions Guide](#) or the ACLs section of the [ExtremeXOS 16.2 User Guide](#).

- 1 Select **Configure > Dynamic ACL**.

Any current ACLs on the switch will be listed in a searchable table.

- 2 Click the **Create Policy** button.

A new screen displays showing the match conditions and actions (defaulted to the **Basic** tab).

Clicking the **Advanced** tab shows more configuration options.

- 3 Give the policy a name and provide IP addresses and actions. When complete, click **Next**.
- 4 On the **ACL Rule: <policy name>** page, complete the **If** area by entering the ethernet-source and ethernet-destination addresses.
- 5 Complete the **Then** field (`deny;` is common here).
- 6 In the **Bindings** area, determine where this policy will be used—VLANs, ports, or both, and egress or ingress.

The following examples show ACLs applying the to VLANs and Ports using `ingress any;` and `egress any;`

ACL Rule: Test		General
General		
Rule Name	<input type="text" value="Test"/>	
If	<pre>ethernet-source-address 00:00:00:00:01 ethernet-destination-address 00:00:00</pre>	
Then	<pre>deny;</pre>	
Bindings (designate Ports or VLANS)	<pre>ingress any;</pre>	

To create this ACL in the CLI, you would use the following commands:

```
create access-list Test
  "ethernet-source-address 00:00:00:00:00:01 ;
  ethernet-destination-address 00:00:00:00:00:02 ;"
  " deny ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM any ingress
```


ACL Rule: Test		General
General		
Rule Name	Test	
If	<pre>ethernet-source-address 00:00:00:00:01 ethernet-destination-address 00:00:00</pre>	
Then	<pre>deny ;</pre>	
Bindings (designate Ports or VLANS)	<pre>egress any;</pre>	

[Back](#)
[Edit](#)
[Delete](#)

To create this ACL in the CLI, you would use the following commands:

```
create access-list Test
  "ethernet-source-address 00:00:00:00:00:01 ;
  ethernet-destination-address 00:00:00:00:00:02 ;"
  " deny ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM any egress
```

The following ACL examples apply bindings to only ports on ingress and egress. For Summit platforms, use the port number only; for SummitStack and chassis, use the slot:port format.

ACL Rule: Test		General
General		
Rule Name	<input type="text" value="Test"/>	
If	<pre> ethernet-source-address 00:00:00:00:01 ethernet-destination-address 00:00:00 </pre>	
Then	<pre> deny; </pre>	
Bindings (designate Ports or VLANS)	<pre> ingress ports 1; </pre>	

To create this ACL in the CLI, use the following commands:

```

create access-list Test
  " ethernet-source-address 00:00:00:00:01 ;
  ethernet-destination-address 00:00:00:00:02 ;"
  " deny ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM ports 1 ingress

```

ACL Rule: Test		General
General		
Rule Name	<input type="text" value="Test"/>	
If	<pre>ethernet-source-address 00:00:00:00:01 ethernet-destination-address 00:00:00</pre>	
Then	<pre>deny;</pre>	
Bindings (designate Ports or VLANs)	<pre>egress ports 1;</pre>	

To create this ACL in the CLI, use the following commands:

```
create access-list Test
  " ethernet-source-address 00:00:00:00:00:01 ;
  ethernet-destination-address 00:00:00:00:00:02 ;"
  " deny ;" application "Cli"
```

```
configure access-list add Test last priority 0 zone SYSTEM ports 1 egress
```

The following example ACLs apply bindings to ports on a specific VLAN on ingress and egress (assuming the VLAN has been created previously). These examples use the Default VLAN.

ACL Rule: Test		General
General		
Rule Name	<input type="text" value="Test"/>	
If	<pre>ethernet-source-address 00:00:00:00:01 ethernet-destination-address 00:00:00</pre>	
Then	<pre>deny;</pre>	
Bindings (designate Ports or VLANS)	<pre>ingress VLAN default;</pre>	

To create this ACL in the CLI, use the following commands:

```
create access-list Test
  " ethernet-source-address 00:00:00:00:00:01 ;
  ethernet-destination-address 00:00:00:00:00:02 ;"
  " deny ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM vlan Default ingress
```

ACL Rule: Test

General

General	
Rule Name	Test
If	<pre>ethernet-source-address 00:00:00:00:01 ethernet-destination-address 00:00:00</pre>
Then	<pre>deny;</pre>
Bindings (designate Ports or VLANS)	<pre>egress VLAN Default;</pre>

Back

Edit

Delete

To create this ACL in the CLI, use the following commands:

```
create access-list Test
  " ethernet-source-address 00:00:00:00:01 ;
  ethernet-destination-address 00:00:00:00:02 ;"
  " deny ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM vlan Default egress
```

- Click **Apply** to complete the policy setup, or click **Delete** to start over.

When the ACL is complete, you are returned to the **Dynamic Access Control Lists** screen, where your new policy will be displayed.

Configuring Audio Video Bridges

Chalet allows you to enable or disable the Audio Video Bridging (AVB) feature to the switch and all ports, and is the equivalent of issuing commands `enable avb` and `enable avb ports [port_list | all]` (and their equivalent disable commands). Transmitter and receiver devices must be set up before enabling AVB.



Note

AVB is only supported on a few Summit platforms. For more information, refer to the [Using AVB with Extreme Switches](#) guide and the "AVB" section of the [ExtremeXOS 16.2 User Guide](#).

To enable AVB from Chalet, your switch must be AVB-capable and you must have an existing license. Follow the instructions below to enter the license key and configure the feature.

- 1 Select **Configure > Audio Video Bridging**.

- 2 Enter the AVB license key and click **Apply**.

Chalet pushes the license information to the switch. Once complete, the page refreshes and displays a list of ports.

Port	Link State	gPTP Enabled	MSRP Enabled	MVRP Enabled	Audio Video Bridging
48	Active	Disabled	Boundary	Active	✗



Note

If you see ✗ next to a port, AVB is not functioning on that port. A receiver and transmitter must be properly set up for AVB to function.

- 3 Click the **Advanced** tab to see enable/disable information for gPTP, MSRP, and MVRP.



Configuring Chalet Settings

You can configure Chalet's settings, including session idle timeout for the user currently logged in. There is no global setting, so each user will set their individual preferences from this screen.




Note

Your browser will store this value so you do not have to set the idle timeout each time you log in. However, if you switch browsers, you will need to configure this setting for the new browser.

- 1 Select **Configure > Chalet**.
- 2 From the **Session settings** area, type the number of minutes your session will last. The default is 10 minutes.
- 3 Click **Apply** and then **Save Config**.

Chalet settings

Session settings

Chalet Idle timeout (minutes) Min: 10 min - Max: 60 min	60 
---	--

[Back](#) [Apply](#)

5 Monitoring a Switch

Monitoring Events
Monitoring System Performance
Monitoring Port Utilization
Monitoring Quality of Service
Monitoring User Sessions

Chalet's monitoring features allow you to view:

- Event logs by time, date, severity, and event detail.
- System processes and CPU performance by ExtremeXOS feature.
- Port utilization by Percent, Bytes, and Packets.
- Port Quality of Service for each profile (QP1-QP8) by Bytes or Packets and Ingress or Egress.
- User sessions on the switch.

Monitoring Events

The **Dashboard** shows the number of recent Critical events, Errors, and Warnings, along with listing the last five errors. To get more information about these events, click anywhere in either of these tables (or select **Monitoring > Event Log**).

The **Event Log** screen displays a searchable and sortable list that displays the following for each event:

- Date and time
- Severity
- Event details

Time	Severity	Event
2015-01-26 15:52:25.99	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_info -d portList=* port=None
2015-01-26 15:52:25.60	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_config portList=* port=None
2015-01-26 15:52:25.54	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show one vlan.vlanProc action=SHOW_VLAN name1=None
2015-01-26 15:52:24.41	<Info:AAA.authPass>	: Login passed for user admin through xml (10.6.105.52)
2015-01-26 15:52:03.61	<Warn:DM.Warning>	: Switch, Code 5: Air flow mismatch detected in slot 1. Ensure all fantray and psu models are of similar air flow. (X460G2-48t-10G4, P/N: 800550-00-00, S/N: 1345G-00529, Rev: 0.0)
2015-01-26 15:51:52.19	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_qos_monitor portList=* port=None ingress=0 countType=0
2015-01-26 15:51:50.79	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_info -d portList=* port=None
2015-01-26 15:51:50.49	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_config portList=* port=None
2015-01-26 15:51:50.42	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show one vlan.vlanProc action=SHOW_VLAN name1=None
2015-01-26 15:51:33.63	<Warn:DM.Warning>	: Switch, Code 5: Air flow mismatch detected in slot 1. Ensure all fantray and psu models are of similar air flow. (X460G2-48t-10G4, P/N: 800550-00-00, S/N: 1345G-00529, Rev: 0.0)
2015-01-26 15:48:33.64	<Warn:DM.Warning>	: Previous message repeated 6 additional times in the last 150 second(s)

This screen provides the same information as issuing the `show log` command. For more information about system events, refer to the [ExtremeXOS 16.2 User Guide](#).

Monitoring System Performance

Select **Monitoring > System** directs you to the **CPU Performance** page.

The table shows each switch's performance over the last hour in a few pre-determined increments. Nothing on this page is editable, but the information can be filtered using the search bar.


Dashboard Configure **Monitoring** Help Logout

CPU Performance:

Process		% last 5 secs	% last 10 secs	% last 30 secs	% last 1 min	% last 5 mins	% last 30 mins	% last 1 hour	Max %	Total User CPU Usage (secs)	Total System CPU Usage (secs)
MM-A	System	2.7	2.5	2.4	2.4	2.4	2.3	2.3	7.3	27.25	154615.72
MM-B	System	1.8	2.2	2.4	2.4	2.4	2.4	2.4	4.1	0.00	0.00
MM-A	aaa	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.96	1.41
MM-A	acl	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	63.69	160.05
MM-A	bfd	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.8	54.73	94.43
MM-A	bgp	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.04	0.05
MM-A	brm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.04	0.02
MM-A	cfgmgr	0.0	0.0	0.0	0.2	0.1	0.0	0.0	0.9	13.32	34.98
MM-A	cli	0.0	0.0	0.0	1.6	0.6	0.1	0.2	3.7	223.10	15.26
MM-A	devmgr	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	10.88	4.65
MM-A	dirser	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.13	0.13
MM-A	dosprotect	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.02	0.03
MM-A	dot1ag	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.3	0.25	0.56
MM-A	eaps	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.07	0.08
MM-A	edp	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.5	3.96	1.92
MM-A	elrp	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.02	0.03
MM-A	elism	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.3	0.36	0.41










Monitoring Port Utilization

Clicking **Monitoring** > **Port Utilization** provides a summary of all ports with their link states and receive and transmit details that can be viewed in Percent, Bytes, or Packets. The table can be sorted by any column or filtered using the search bar.

The information shown cannot be edited, but you can view more information about the port by clicking the  to the right. This will take you to the **Port Details** screen, where you can [configure ports](#)).

Dashboard Configure **Monitoring** Help Logout

Port Utilization: Percent Bytes Packets


Port	Link State	Receive Peak	Receive	Transmit Peak	Transmit	Details
1:1	Active	0.000024	0.000007	0.000031	0.000007	
1:24	Active	0.000019	0.000007	0.000018	0.000009	
2:1	Active	0.000001	0.000000	0.000002	0.000000	
2:5	Active	0.000001	0.000000	0.000001	0.000000	
2:17	Active	0.000001	0.000000	0.000002	0.000000	
3:5	Active	0.000001	0.000000	0.000001	0.000000	
3:17	Active	0.000001	0.000000	0.000001	0.000000	
4:1	Active	0.000000	0.000000	0.000034	0.000007	
5:1	Active	0.000000	0.000000	0.000013	0.000007	

Monitoring Quality of Service

Clicking **Monitoring** > **Quality of Service** provides a summary of QoS profiles and the packets or bytes on each port, and is equivalent to entering the `show ports qosmonitor` command.

The QoS information shown cannot be edited, but you can rearrange the data by Bytes or Packets and Ingress or Egress. You can also sort by column or use the search bar to filter the results.

Port	QP1	QP2	QP3	QP4	QP5	QP6	QP7	QP8	Details
1:1	18	0	0	0	0	0	0	105893	➔
1:2	0	0	0	0	0	0	0	0	➔
1:3	0	0	0	0	0	0	0	0	➔
1:4	0	0	0	0	0	0	0	0	➔
1:5	0	0	0	0	0	0	0	0	➔
1:6	0	0	0	0	0	0	0	0	➔
1:7	0	0	0	0	0	0	0	0	➔
1:8	0	0	0	0	0	0	0	0	➔
1:9	0	0	0	0	0	0	0	0	➔
1:10	0	0	0	0	0	0	0	0	➔
1:11	0	0	0	0	0	0	0	0	➔
1:12	0	0	0	0	0	0	0	0	➔
1:13	0	0	0	0	0	0	0	0	➔
1:14	0	0	0	0	0	0	0	0	➔
1:15	0	0	0	0	0	0	0	0	➔
1:16	0	0	0	0	0	0	0	0	➔
1:17	0	0	0	0	0	0	0	0	➔

For more information about a particular port, click the  to the right. This will take you to the **Port Details** screen (see [Port Details -- QoS](#) on page 25).



Note

QoS Profiles must be created before you can assign ports. For more information, see [Configuring QoS in the ExtremeXOS 16.2 User Guide](#).

Monitoring User Sessions

The **Sessions** page shows all current sessions in chronological order, including the user name, the type of user (XML, SSH, or Telnet), the authentication, location (IP address), and login date/time stamp.

To view the session list, select **Monitoring > Session**.

**Note**

Every time a user refreshes the web browser, a duplicate session is created. Currently, Chalet does not allow administrators to clear duplicate or rogue sessions for other users. To clear your own session, click **Logout** in the navigation menu.

**Note**

A maximum of six XML session are allowed per device.

ID	User	Type	Authentication	Location	Login Time
14	admin	xml	local	10.6.82.136	Fri Jan 9 21:59:04 2015
15	admin	xml	local	10.6.82.136	Fri Jan 9 21:59:13 2015

6 Managing Accounts

Adding Users
Deleting Users
Changing User Passwords
Account Security

From the **User Detail** page (**Configure > Accounts**), administrators can:

- Add users.
- Delete users.
- Change user passwords.
- Set global and individual password policies.
- Set RADIUS and TACACS authentications.

Adding Users

Administrators can add multiple users that have either read-only or read-write access. To add a new user:

- 1 Click **Configure > Accounts** to display the user list.
- 2 Click the **New User** button.

Create New User

User Name:	<input type="text" value="manager"/>
Password:	<input type="password" value="....."/>
Re-enter Password:	<input type="password" value="....."/>
Access Permission:	<input type="text" value="Read-Write"/>

- 3 In the pop-up dialog, enter the user name and password, confirm the password, and select the permission level.


**Note**

If a **global password policy** is set, you will be notified if the password you choose does not conform to this policy.

- 4 Click **Submit** to finish.
The page refreshes to show the new user.

Deleting Users

To delete a user:

- 1 Click **Configure** > **Accounts** to display the user list.
- 2 Click the  icon on the row of the user you wish to delete.
The **User Detail** page appears.
- 3 Click the **Delete User** button and confirm the deletion in the resulting dialog.

Please confirm:

This command will delete user manager


Do you really want to continue?

Yes

No

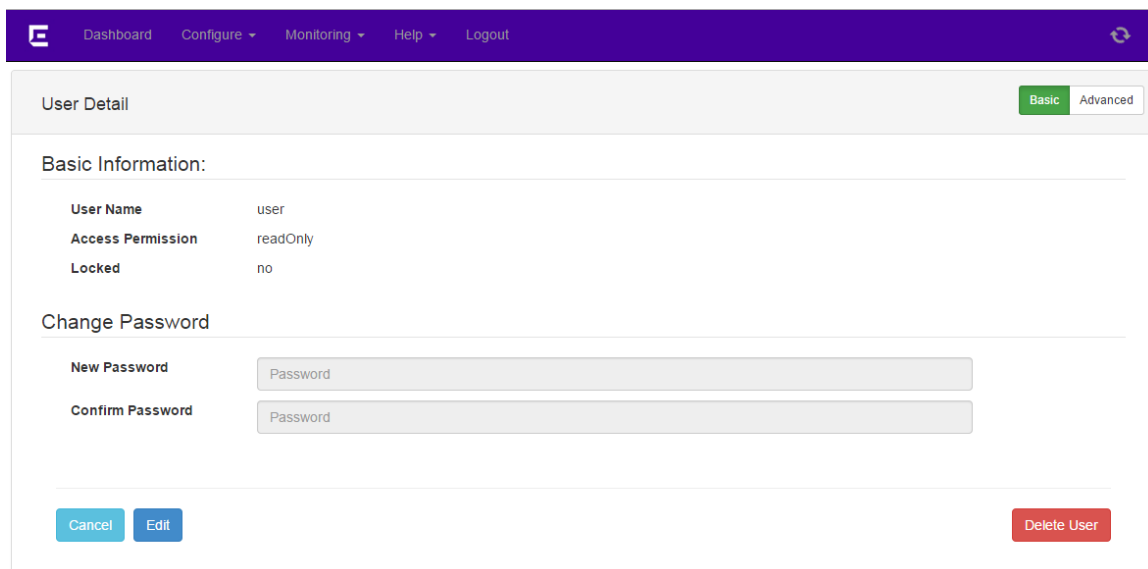
Changing User Passwords

To change a user's password:

- 1 Click **Configure** > **Accounts** to display the user list.
- 2 Click the  icon on the row of the desired user.
The **User Detail** page appears.

3 Click **Edit**.

The Change Password area becomes editable.


4 Enter a new password and confirm it, and then click **Apply**.**Note**

If you have set a global password policy, the new password must conform to the new policy.

5 If you want to create a separate password policy *for just this user*, click the **Advanced** button and complete the following information:

- **Maximum Age (days)**—Maximum password age, in days. For example, if you enter 60, users will be required to set a new password in 60 days.
- **Minimum Length**—Set a minimum password length.
- **History Limit**—Set the number of new passwords before a user can reuse an older password. For example, if you enter 3, the user must create three new passwords until a former password can be reused.
- **Character Validation**—Enforce passwords that have *at least two* of each of the following:
 - upper case letters
 - lower case letters
 - numbers
 - special character

For example: P@Sw04d!

- **Lockout on Login Failures**—Lock the user out after three unsuccessful login attempts.

6 When finished, click **Save Config**.

Account Security

To add greater security to accounts created on the switch, you can:

- [Set a Global Password Policy](#)

- [Configure RADIUS](#)
- [Configure TACACS](#)

Setting a Global Password Policy

Chalet allows you to set a password policy for all users to enhance security. To set up the global password policy:

- 1 Click **Configure** > **Accounts**.
- 2 Click the **Security Options** button, and then click **Edit** on the **Password Policy** tab.
The grayed-out fields become editable.
- 3 You can set great security for account passwords by setting any of the following:
 - **Maximum Age (days)**—Maximum password age, in days. For example, if you enter 60, users will be required to set a new password in 60 days.
 - **Minimum Length**—Set a minimum password length.
 - **History Limit**—Set the number of new passwords before a user can reuse an older password. For example, if you enter 3, the user must create three new passwords until a former password can be reused.
 - **Character Validation**—Enforce passwords that have *at least two* of each of the following:
 - upper case letters
 - lower case letters
 - numbers
 - special character

For example: P@Sw04d!

- **Lockout on Login Failures**—Lock the user out after three unsuccessful login attempts.

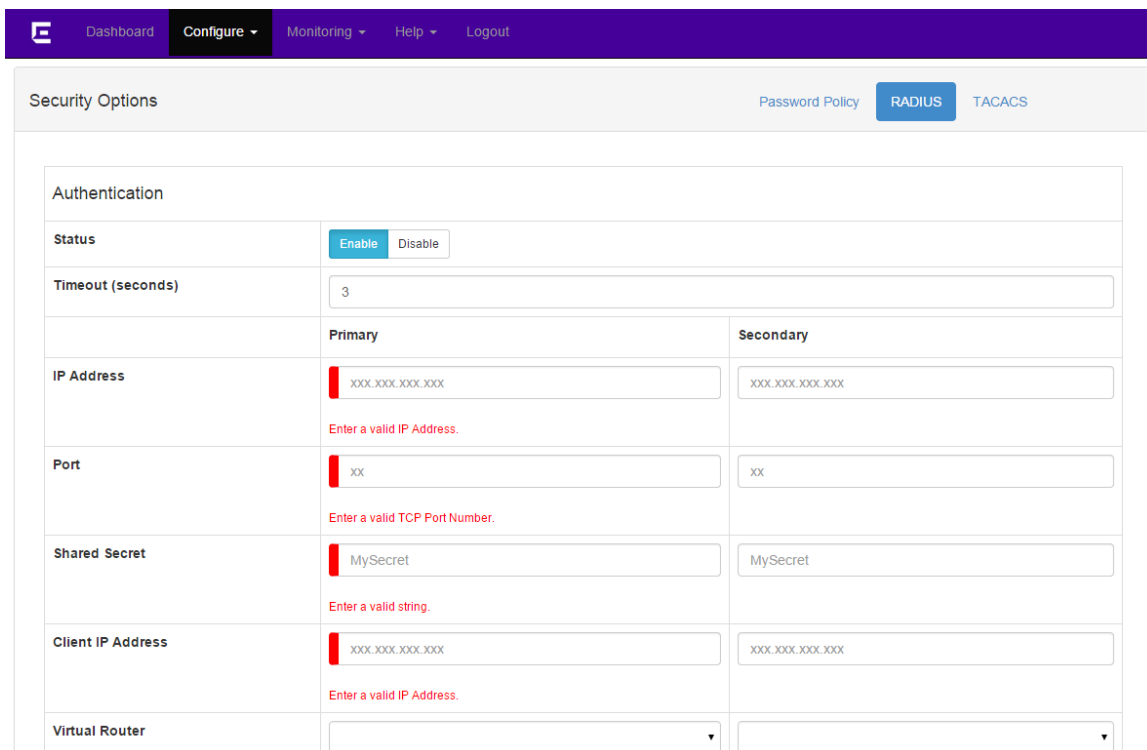
- 4 Click **Apply** when finished.
All new account password must meet these requirements unless the security options are removed.

Configuring RADIUS

You can enable and configure RADIUS on the switch in one Chalet screen instead of entering multiple commands on the CLI. For more information about configuring RADIUS, see the "Security" section of the *ExtremeXOS 16.2 User Guide*.

To configure RADIUS:

- 1 Click **Configure** > **Accounts** to display the user list.
- 2 Click the **Security Options** tab.
- 3 Click the **RADIUS** tab.
- 4 Click **Edit** at the bottom of the page.
- 5 To enable RADIUS, click the **Enable** button in the Status field.



The screenshot shows the RADIUS configuration interface. At the top, there is a navigation bar with 'Dashboard', 'Configure', 'Monitoring', 'Help', and 'Logout'. Below this is the 'Security Options' section with tabs for 'Password Policy', 'RADIUS', and 'TACACS'. The 'RADIUS' tab is active. The 'Authentication' section is expanded, showing a table with fields for 'Status', 'Timeout (seconds)', 'IP Address', 'Port', 'Shared Secret', 'Client IP Address', and 'Virtual Router'. The 'Status' field has 'Enable' and 'Disable' buttons. The 'Timeout (seconds)' field has a value of '3'. The 'IP Address' field is split into 'Primary' and 'Secondary' columns. The 'Primary' IP Address field has a red error message: 'Enter a valid IP Address.' The 'Port' field is also split into 'Primary' and 'Secondary' columns. The 'Primary' Port field has a red error message: 'Enter a valid TCP Port Number.' The 'Shared Secret' field is split into 'Primary' and 'Secondary' columns. The 'Primary' Shared Secret field has a red error message: 'Enter a valid string.' The 'Client IP Address' field is split into 'Primary' and 'Secondary' columns. The 'Primary' Client IP Address field has a red error message: 'Enter a valid IP Address.' The 'Virtual Router' field is split into 'Primary' and 'Secondary' columns.

- 6 Supply the information in the required fields.



Note

For the Shared Secret field, enter the *unencrypted* (plain text)

secret, not the encrypted version. The switch will encrypt the shared secret for you.



Note

For the Client IP Address field, you must choose an IP interface existing on the switch so it is contained within the virtual router.

- 7 When finished configuring RADIUS, click **Save Config**.

To unconfigure this feature (by pushing down the "unconfigure" commands to the switch), you must remove all the text in any configured fields, disable the feature, and then apply and save your changes.

Configuring TACACS

You can enable and configure TACACS on the switch in one Chalet screen instead of entering multiple commands on the CLI. For more information about TACACS, see the "Security" section of the *ExtremeXOS 16.2 User Guide*.

To configure TACACS:

- 1 Click **Configure** > **Accounts** to display the user list.
- 2 Click the **Security Options** tab.
- 3 Click the **TACACS** tab.
- 4 Click **Edit** at the bottom of the page.
- 5 To enable TACACS, click the **Enable** button in the Status field.

Security Options		Password Policy	RADIUS	TACACS
Authentication				
Status	<input type="button" value="Enable"/> <input type="button" value="Disable"/>			
Timeout (seconds)	<input type="text" value="3"/>			
	Primary	Secondary		
IP Address	<input type="text" value="xxx.xxx.xxx.xxx"/> <small>Enter a valid IP Address.</small>	<input type="text" value="xxx.xxx.xxx.xxx"/>		
Port	<input type="text" value="xx"/> <small>Enter a valid TCP Port Number.</small>	<input type="text" value="xx"/>		
Shared Secret	<input type="text" value="MySecret"/> <small>Enter a valid string.</small>	<input type="text" value="MySecret"/>		
Client IP Address	<input type="text" value="xxx.xxx.xxx.xxx"/> <small>Enter a valid IP Address.</small>	<input type="text" value="xxx.xxx.xxx.xxx"/>		
Virtual Router	<input type="text"/>	<input type="text"/>		

- 6 Supply the information in the required fields.
- 7 When finished configuring TACACS, click **Save Config**.

To unconfigure this feature (by pushing down the "unconfigure" commands to the switch), you must remove all the text in any configured fields, disable the feature, and then apply and save your changes.

A 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

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

DCBX

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

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

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 plane).

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.