



ExtremeWireless™ Maintenance Guide

Release V10.21.01



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.

145 Rio Robles

San Jose, California 95134

USA

Table of Contents

Chapter 1: About This Guide.....	6
Who Should Use This Guide.....	6
How to Use This Guide.....	7
Text Conventions.....	7
Providing Feedback to Us.....	8
Getting Help.....	8
Related Publications.....	9
Chapter 2: Backing Up and Restoring the Image.....	11
Creating a Backup Image.....	11
Backing Up and Restoring Characteristics by Controller Models.....	12
Backing Up Image File Name.....	12
Backing Up the Current Image During the Upgrade Process from the Wireless Assistant GUI.....	12
Backing Up the Current Image During Upgrade from the CLI.....	13
Backing Up the Current Image from Rescue Mode.....	14
Restoring the Backup Image from the GUI.....	18
Downloading a Backup Image from an FTP or SCP Server.....	19
Deleting a Backup Image That Is Available for Restore.....	20
Restoring Characteristics by Controller Models.....	20
Restoring the Backup Image from the CLI.....	20
Restoring the Backup Image from Rescue Mode.....	21
Restoring from the Local Drive.....	22
Restoring from a Remote FTP Server.....	23
Restoring the Rescue Image.....	24
Restoring to Factory Default.....	25
Chapter 3: Backing Up and Restoring the Configuration.....	27
Backing Up the Wireless Controller Configuration.....	27
Uploading a Backup to a Server.....	29
Copying a Local Backup to Flash.....	30
Scheduling a Backup.....	30
Deleting a Backup.....	32
Restoring the Wireless Controller Configuration.....	32
Downloading a Backup File.....	33
Chapter 4: Upgrading the Wireless Convergence Software.....	36
Upgrading Process.....	36
Upgrading Using the GUI.....	38
Upgrading Using the CLI.....	44
Migrating the Platform Configuration.....	45
Upgrading Two Controllers in Availability Mode.....	47
Upgrading Two Controllers in Session Availability Mode.....	49
Chapter 5: Working with External Storage Devices.....	50
Working with an External Storage Device.....	50
Mounting a Flash Device on the Wireless Controller.....	51
Un-mounting a Flash Device from the Controller.....	53
Deleting Files from a Flash Device.....	54

Chapter 6: Using the Console Port.....	55
Using the Console Port in the Wireless Controller Models C25, C35, C4110, C5110, and C5210.....	55
Using the Console Port for the V2110.....	55
Chapter 7: Performing System Maintenance.....	57
Changing Log Levels, Syslog Event Reporting, and AP Log Management.....	57
Enabling or Disabling the Poll Timer.....	61
Shutting Down the System.....	62
Resetting Your System Configuration.....	63
Resetting Wireless APs to Factory Default Settings.....	63
Replacing the CMOS Battery.....	69
Chapter 8: Using Controller Utilities.....	72
Using Controller Utilities.....	72
Enabling SNMP.....	75
Chapter 9: Recovering the Wireless Controller.....	83
Rescue Mode Authentication Service Management Menu.....	83
Recovering the Wireless Controller from File System Corruption.....	84
Chapter 10: Maintaining the Wireless Controller.....	86
Maintaining the C35 Controller.....	86
Maintaining the C25 Controller.....	88
Maintaining the C5110 Controller.....	90
Maintaining the C5210 Controller.....	95
Maintaining the C4110 Controller.....	98
Chapter 11: Maintaining the Wireless AP Software.....	99
Maintaining a List of Current Software Images.....	99
Deleting a Software Image.....	100
Downloading a New Software Image.....	101
Defining Parameters for a Software Upgrade.....	101
Chapter 12: Performing Wireless AP Diagnostics.....	103
Performing Wireless AP Diagnostics Using SSH.....	103
Appendix A: Glossary.....	107
A.....	107
B.....	110
C.....	111
D.....	116
E.....	119
F.....	123
G.....	125
H.....	126
I.....	127
J.....	131
L.....	131
M.....	133
N.....	137
O.....	138
P.....	140

Q.....143
R.....144
S.....147
T.....151
U.....153
V.....154
W.....157
X.....158



1 About This Guide

Who Should Use This Guide
How to Use This Guide
Text Conventions
Providing Feedback to Us
Getting Help
Related Publications

The purpose of this guide is to assist you in performing the maintenance of the following hardware and software components of the ExtremeWireless Solution:

HARDWARE

- ExtremeWireless Appliances
- ExtremeWireless APs

This guide covers the following ExtremeWireless Appliance models:

- ExtremeWireless Appliance C5110
- ExtremeWireless Appliance C5210
- ExtremeWireless Appliance C4110
- ExtremeWireless Appliance C25
- ExtremeWireless Appliance C35
- Virtual Wireless Appliance V2110 (VMWare and MS Hyper-V platforms)

SOFTWARE

- ExtremeWireless Software

Who Should Use This Guide



Electrical Hazard: Only qualified personnel should install or service this unit.

Riesgo Electrico: Nada mas personal capacitado debe de instalar o darle servicio a esta unida.

Elektrischer Gefahrenhinweis: Installationen oder Servicearbeiten sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.

This guide is intended for network administrators who are responsible for maintaining the ExtremeWireless Solution.

How to Use This Guide

Read through this guide completely to familiarize yourself with its contents and to gain an understanding of the features and capabilities of the ExtremeWireless software. A general working knowledge of data communications networks is helpful when setting up these modules.

This section provides an overview of this guide and a brief summary of each chapter; defines the conventions used in this document; and instructs how to obtain technical support from Extreme Networks. To locate information about various subjects in this guide, refer to the following table.

For...	Refer to...
Information on how to back up the existing software image before performing the upgrades.	Backing Up and Restoring the Image on page 11
Information on how to restore the previously backed up configuration on various platforms.	Backing Up and Restoring the Configuration on page 27
Information on various upgrade paths to upgrade the ExtremeWireless Convergence Software.	Upgrading the Wireless Convergence Software on page 36
Information on how to work with ExtremeWireless external storage devices.	Working with External Storage Devices on page 50
Information on how to connect to the ExtremeWireless console port to access the Rescue mode.	Using the Console Port on page 55
Information on how to perform the following system maintenance tasks: Changing the log level, setting a poll interval for checking the status of the Wireless APs (Health Checking), enabling and defining parameters for Syslog event reporting, forcing an immediate system shutdown with, or without reboot, and resetting the ExtremeWireless to its factory defaults.	Performing System Maintenance on page 57
Information on how to configure the ExtremeWireless utilities.	Using Controller Utilities on page 72
Information on how to recover the ExtremeWireless lost login password via the Rescue mode.	Recovering the Wireless Controller on page 83
Information on how to maintain various platforms.	Maintaining the Wireless Controller on page 86
Information on how to perform Wireless AP software maintenance.	Maintaining the Wireless AP Software on page 99
Information about performing wireless AP diagnostics using SSH.	Performing Wireless AP Diagnostics on page 103

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

ExtremeWireless and ExtremeWireless AP documentation can be found on Extreme Documentation page at: <http://documentation.extremenetworks.com>

Extreme recommends the following guides for users of ExtremeWireless products:

- *ExtremeWireless AP3912i Installation Guide*
- *ExtremeWireless AP3965i & AP3965e Installation Guide*
- *ExtremeWireless AP3935i & AP3935e Installation Guide*
- *ExtremeWireless AP3825i & AP3825e Installation Guide*
- *ExtremeWireless AP3805i FCC/ROW Installation Guide*
- *ExtremeWireless AP3801i Quick Reference Guide*
- *ExtremeWireless Appliance C5210 Quick Reference*
- *ExtremeWireless Appliance C5110 Quick Reference*
- *ExtremeWireless Appliance C4110 Quick Reference*
- *ExtremeWireless Appliance C25 Quick Reference*
- *ExtremeWireless Appliance C35 Quick Reference*
- *ExtremeWireless CLI Reference Guide*
- *ExtremeWireless End User License Agreements*
- *ExtremeWireless External Antenna Site Preparation and Installation Guide*
- *ExtremeWireless External Antenna with Wave 2 Site Preparation and Installation Guide*

- [*ExtremeWireless Getting Started Guide*](#)
- [*ExtremeWireless Integration Guide*](#)
- [*ExtremeWireless Maintenance Guide*](#)
- [*ExtremeWireless Open Source Declaration*](#)
- [*ExtremeWireless User Guide*](#)
- [*IdentiFi Wireless WS-AP3865e Installation Guide*](#)
- [*IdentiFi Wireless WS-AP3825i & WS-AP3825e Installation Guide*](#)
- [*IdentiFi Wireless WS-AP3805i & WS-AP3805e Installation Guide*](#)



2 Backing Up and Restoring the Image

Creating a Backup Image

Backing Up and Restoring Characteristics by Controller Models

Backing Up Image File Name

Backing Up the Current Image During the Upgrade Process from the Wireless Assistant GUI

Backing Up the Current Image During Upgrade from the CLI

Backing Up the Current Image from Rescue Mode

Restoring the Backup Image from the GUI

Downloading a Backup Image from an FTP or SCP Server

Deleting a Backup Image That Is Available for Restore

Restoring Characteristics by Controller Models

Restoring the Backup Image from the CLI

Restoring the Backup Image from Rescue Mode

Restoring from the Local Drive

Restoring from a Remote FTP Server

Restoring the Rescue Image

Restoring to Factory Default

Creating a Backup Image

When creating the image backup, the wireless controller makes an exact copy (snapshot) of the running image and saves it as a `tgz` file. Restoring the controller with a backup image restores the appliance to the exact state at the time backup was created.

A backup image can be created in two ways:

- 1 During upgrade of the image. Before installing the new image version, the upgrade process takes the backup of the running image. The backup image can be stored locally, on a flash drive (if present), or remotely on an FTP server.
- 2 From rescue mode using the menu driven commands. To do this, you have to enter rescue mode on startup. No service to clients is provided while you are in rescue mode. Again, the backup image can be stored on the local, flash (if flash is present) or an FTP server.

The only way to create a backup image independently of an upgrade is to run it from the rescue mode.

Backing Up and Restoring Characteristics by Controller Models

The following table describes the backup and restore capabilities and characteristics for all wireless controllers.

Table 3: Controller Backup and Restore Capabilities and Characteristics

FTP	Local	Flash
Requires management port connectivity	Administrator can upload/download local backup images provided they end in '-rescue-user.tgz'	USB device



Note

Backup file names must end in '-rescue-user.tgz'.



Note

Before you proceed with an FTP backup, ensure that the management port is configured correctly and connected to the network. To enter **Rescue** mode, you must connect to the serial console. The V2110 (MS Hyper-V platform) does not support flash functionality.

Backing Up Image File Name

The default file name used for backup image is: <hostname/domain>-<platform>-<version>-rescue-user.tgz

In order to distinguish multiple backup images, rename the file when saving to flash or FTP. If modification is required, you should prepend the custom text to the default image name.

Backing Up the Current Image During the Upgrade Process from the Wireless Assistant GUI

You must follow the procedures detailed in this section if you want to backup the current image via the Wireless Assistant GUI while upgrading the image. For more information on how to upgrade the image, see [Upgrading Using the GUI](#) on page 38.



Note

When you backup the current image, the license activation key and option keys are also backed up.

External Storage

The wireless controller models C25, C35, C4110, C5110, C5210 and V2110 support only the USB storage device. If you select the Flash option to backup the existing image in these models, the image will be backed up on the USB device. You must ensure that the USB device is installed and mounted on the wireless controller. For more information, see [Working with an External Storage Device](#) on page 50.

To back up the existing software:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**. The **EWC Software** tab displays.
- 3 Select the **Backup system image to:** checkbox and choose the appropriate backup option.

To save the existing software image in local storage, select the **Local** option. The upgrade process will delete the previous backup image stored in local storage (if one exists).

To save the existing software image on the flash device, select the **Flash** option, and then type a file name for the backup image in the **Filename** box.

Note



The backup image file name is self generated when saved for both local or remote options (for example, EWC-<platform>10.01.0001-rescue-user.tgz). It is recommended that you maintain this format for the backup image file name. If you must customize the file name, prepend the customized file name to the original generated file name of the backup image.

To save the existing software image on a remote FTP server, select the **Remote** option, and then type the following:

FTP Server – The IP address of the FTP server that stores the image file.

User ID – The user ID used to log on to the FTP server.

Password – The corresponding password for the user ID.

Confirm – The corresponding password for the user ID to confirm the password was typed correctly.

Directory – The directory on the server in which the image file is stored.

Filename – The image file name, which must end with -rescue-user.tgz.

Backing Up the Current Image During Upgrade from the CLI

A backup image can be created during an upgrade from the CLI.

- 1 Check the backups present on the controller by running the **show upgrade** command.

```
EWC.extremenetworks.com# show upgrade
1: AC-MV-09.01.01.0123-1.rue
2: rue-08.31.01.0192-rescue-user.tgz
```

If you want a local backup file to be created, the upgrade process removes any previous *-rescue-user.tgz file. Optionally, you can remove any existing local backup file by running the no upgrade <filename> command.

```
EWC.extremenetworks.com# no upgrade 2
```

The command deletes the image with index 2, which, in this example, is vps-08.31.01.0192-rescue-user.tgz. You can also specify the full image name.

- Upgrade the software with a backup image to local storage using the `upgrade ac new-image-name bckto local` command. During the upgrade process, a backup image with the default backup image name is created on the local storage:

```
upgrade ac AC-MV-09.01.01.0123-1.rue
bckto local
```

- Upgrade the software with a backup image to flash using the `upgrade ac new-image-name bckto flash [filename]` command.

```
upgrade ac AC-MV-09.01.01.0123-1.rue
bckto flash
```

The command will upgrade and create a backup image with the default name on the flash drive.

You can also specify the custom name for the backup image.

```
upgrade ac AC-MV-09.01.01.0123-1.rue bckto flash backup-rescue-user.tgz
```



Note

To backup to flash, you must insert a flash drive before running the command.

- If backing up the software to FTP, set up the FTP server credentials before running the upgrade by running the `upgrade_backup_dest ftp server ip user password dir file` command.

```
upgrade_backup_dest 192.168.4.10 test abc123 system/backups backup-rescue-user.tgz
```

The name specified for “upgrade_backup_dest” is used as the backup file name.

- Start the upgrade by running the `upgrade ac new-image-name bckto ftp` command.

```
upgrade ac AC-MV-09.01.01.0123-1.rue bckto ftp
```

The command first makes a backup image of the running system preserved on the FTP server, then installs the selected upgrade image.

Backing Up the Current Image from Rescue Mode

You must follow the procedures in this section if you are backing up the current image.

You can also backup the current image via the Wireless Assistant GUI. For more information, see [Backing Up the Current Image During the Upgrade Process from the Wireless Assistant GUI](#) on page 12.



Note

When you backup the current image, the license activation key and option keys are also backed up.

To back up the existing current image:

- Connect to the console port. Do not use the ESA ports or the Admin management port. For more information, see [Using the Console Port](#) on page 55.
- Reboot the system. The following menu appears during the reboot process.

```
-----
Controller
Controller Rescue
-----
```

- 3 Select **Controller Rescue**, and then press **Enter**. The first repairFS script runs after the OS initialization.

**Note**

The above process may take several minutes. You must not reboot the system. After the filesystem check is completed, the main rescue menu is displayed.

Rescue Start-up Menu. Use with extreme caution.

- 1) Force System Recovery
- 2) Create System Backup Image
- 3) Display Backup Images
- 4) FTP Menu
- 5) Network Interface Menu
- 6) Manually run File System Check Utility (fsck)
- 7) Restore Backup Image directly from the FTP server
- 8) Authentication Service Management Menu
- 9) Flash Menu
- R) Reboot

WARNING! - Forcing system recovery will erase all files, and reinstall the selected image (either backup or factory).

Reboot will restart the system back into Normal mode.

If you have any questions about these options, please contact Support.

Your choice:

**Note**

If you want to create a backup image either on the wireless controller local drive or the USB device, follow Step 4 and skip the remaining steps. If you want to upload the backup image, follow steps 6 to 12.

- 4 Type **2** in the **Rescue** menu to create a backup image.

Your choice: 2

mounting rest of normal mode partitions...done

Do you want to create a system backup image to USB key? (Y/N)

- 5 Type **Y** to backup the image to a USB device or **N** to backup the image to the controller's local drive.

**Note**

Creating a system backup image to the controller's local drive will overwrite the existing backup image.

If you type **Y**, the following screen is displayed:

Please enter a backup filename:

- a Enter the backup image filename ending in **-rescue-user.tgz** and press Enter.

The following screen is displayed.

Proceed with backup (Y/N):

- b Type **Y**. The system backs up the image to the USB device.

Creating a Backup image is Complete!

<< Press any key to continue >>

If you type **N**, the following message is displayed:

Proceed with backup (Y/N):

Type **Y**. The system backs up the image.

----- Creating 'Normal' mode backup -----

Please be patient. It may take a while. Do not reboot the machine

```

Mount the normal mode partitions:
mounting root partition...done.
mounting rest of normal mode partitions...done.
Creating a backup, please wait
Creating a Backup image is Complete!
Unmounting partitions...
done.
<< Press any key to continue >>

```

**Note**

You can also upload the backed up image to the FTP server. To upload the image to the FTP server, continue with the following procedures.

- 6 Enter Rescue mode.
 - a Type 5 in Rescue menu to enter the Network Interface menu.
 - b Type 2 in the Network Interface menu. The following screen is displayed.

```

Your choice: 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
Input: 192.168.1.210:255.255.255.0 192.168.1.1

```

**Note**

You can use the Network Interface menu options from 3 to 5 (IP, Netmask, and default gateway) one at a time.

- 7 Press **[Enter]**. The following screen is displayed.

```

ip is 192.168.1.210 netmask is 255.255.255.0
Configuring interface ...
Setting up network interface ... Done!
<< Press any key to continue >>

```

- 8 Test the interface.
 - a Type 6 in the Network Interface menu.

```

PING 192.168.3.10 (192.168.3.10) from 192.168.1.210 : 56(84)
bytes of data.
64 bytes from 192.168.3.10: icmp_seq=1 ttl=63 time=2.49 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=63 time=0.881 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=63 time=0.706 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=63 time=0.738 ms
64 bytes from 192.168.3.10: icmp_seq=5 ttl=63 time=0.707 ms
--- 192.168.3.10 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4031ms
rtt min/avg/max/mdev = 0.706/1.106/2.498/0.698 ms
<< Press any key to continue >>

```

**Note**

If the Network Interface is not configured properly, the following screen is displayed.

```

PING 192.168.3.10 (192.168.3.10) from 192.168.1.210 : 56(84) bytes of data.
--- 192.168.3.10 ping statistics ---
9 packets transmitted, 0 received, 100% loss, time 9038ms
<< Press any key to continue >>

```

- 9 Type **B** to return to the top menu. The following screen is displayed.

```

Your choice: B
Going back to the top menu...

```


10 Configure the FTP Settings.

- a Type 4 in the Rescue menu to configure the FTP Settings. The following screen is displayed:

```
FTP MENU
-----
1) Enter FTP Settings
2) Change FTP server IP address
3) Change FTP port
4) Change user name
5) Change password
6) Change FTP directory
7) Change file name
8) Display current FTP Settings
9) Display locally stored images
10) Download Image from FTP server
11) Upload Image onto the FTP server
12) Remove locally stored images
B) Return back to the top menu
Your choice:
```

- b Type 1 to enter the FTP settings.
c Type 1 in the FTP menu. The following screen is displayed.

```
Your choice: 1
Command syntax: ftp://<user>:<password>@<ftp_ip>:<port>/<directory&filename>
~port information is optional: the default value is 21~
Please enter ftp info:
```

- d Type the name of the image to be uploaded, as part of the FTP settings. For example:

Please enter FTP info:

```
ftp://tester:123456@192.168.10.10:21/backup_dir/rue-rescue-user.tgz
```

Note



When you are uploading the backup image, the filename in the command syntax corresponds to the image that is being uploaded to the FTP server (filenames can be displayed by typing 9 in the FTP menu). When you are downloading the backup image, the filename in the command syntax corresponds to a file that is being downloaded from the FTP server.

11 Check the FTP settings.

- a Type 8 in the FTP menu. The following screen is displayed.

```
Your choice: 8
Current Settings:
-----
FTP IP address: 192.168.10.10 port: 21
user name: tester
password: 123456
FTP directory: "backup_dir"
FTP file: "rue-rescue-user.tgz"
<< Press any key to continue >>
```

- b Confirm that the name of the file to be uploaded to the FTP server is correct.

- 12 If applicable, modify the FTP settings.

In the FTP menu, choose options from 2 to 7 to individually configure the FTP settings:

- FTP server's IP address
- FTP port
- User name
- Password
- FTP directory
- File Name

- 13 Upload the image on the FTP server:

- a Type 11 in the FTP menu. The following screen is displayed:

```
Your choice: 11
Attempting to upload an image to the ftp server. Please be patient
Please verify at the ftp server that image has successfully been uploaded
<< Press any key to continue >>
```



Note

The minimum backup image size is approximately 250 MB.

You must have write permission for the FTP server and the specified FTP directory.

- 14 Confirm that the image is backed up.

Type 9 in the FTP menu. The following screen is displayed:

```
Your choice: 9
Currently Locally Stored Images:
-----
1 ) rue-rescue-user.tgz
2 ) AC-MV-09.01.01.0163-1.rue
<< Press any key to continue >>
```

Restoring the Backup Image from the GUI

The following section describes how to restore the backup image using the GUI.

To restore the Wireless Controller Software:

- 1 From the top menu, click **Controller**.

- From the left pane, click **Administration** > **Software Maintenance**.

The **EWC Software** tab is displayed.

The screenshot shows the EWC Software interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The left sidebar shows Administration, Availability, Flash, Host Attributes, Installation Wizard, Login Management, Software Maintenance (selected), System Maintenance, and Web Settings. The main content area is titled 'EWC Software' and has tabs for Backup, Restore, and EWC Product Keys. Under 'Select upgrade:', there are radio buttons for Local (selected), Remote, Flash, Local, and Remote. A list of backup images is shown, with 'AC-MV-09.01.01.0207T-1.qxe' selected. Below the list is a 'Delete selected' button. Under 'Backup system image to:', there is a checked checkbox and radio buttons for Local (selected) and Remote. A 'Filename:' field contains 'lab-422-g-qxe-09.01.01.0207T-res'. Below this are radio buttons for 'Upgrade now' (selected) and 'Schedule upgrade for:', which includes dropdown menus for Month, Day, Hour, and Min. A status message at the bottom right says 'Current controller time is [Mon Mar 3 14:44 2014]'. At the bottom, there is a 'Disk space left for images: 1727 MB' and an 'Upgrade now' button.

The list displays items that are available.

- In the list, click the backup image you want to restore. The list displays all images available on the local disk or the flash card, if the flash card is mounted. Backup images have names ending in -rescue-user.tgz (see [Backing Up Image File Name](#) on page 12).



Note

The Local option must be cleared in the **Backup system image** to section.

- To restore the image, click **Upgrade now**. A dialog is displayed informing you that the restore process requires rebooting the wireless controller.



Note

The Upgrade now parameter does not support IPv6 FTP.

- Click **OK** to confirm the restore.
The **Software Maintenance** window is displayed.

The wireless controller reboots automatically.

Downloading a Backup Image from an FTP or SCP Server

You can choose to download a backup image from an FTP or SCP server for a restore. After it is downloaded, the system is restored in the same way as restoring from the local storage.

To download a backup image from an FTP or SCP Server for a restore:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.
- 3 Select the **Remote option**, and then type the following:
 - **Protocol** – FTP or SCP.
 - **Server** – The server to retrieve the backup file from.



Note

The Server parameter supports both IPv4 and IPv6 addresses.

- **User ID** – The user ID used to log into the server.
 - **Password** – The corresponding password for the user ID.
 - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
 - **Directory** – The directory on the server in which the backup file that is to be retrieved is stored.
 - **Filename** – The name of the image file to retrieve.
- 4 Click **Get Image now**. The image is downloaded and added to the list.



Note

SCP can only be used to download an image and cannot be used to start remote upgrade. The Upgrade now button is disabled when SCP is selected from the drop-down list.

Deleting a Backup Image That Is Available for Restore

To delete a backup image that is available for restore:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.
- 3 To delete a backup image from the list, click the image in the list that you want to delete.
- 4 Click **Delete selected**.

A dialog box is displayed. If correct, click **OK** to confirm the deletion.

Restoring Characteristics by Controller Models

Refer to [Table 3](#) on page 12 for details on the backup and restoration capabilities and characteristics for each wireless controller.



Note

Before you proceed with an FTP restoration, ensure that the Management Port is configured correctly and connected to the network. You cannot enter Rescue mode without the management port's connectivity to the network.

Restoring the Backup Image from the CLI

The backup image can be restored using the CLI from local storage, flash and FTP server.

To restore the backup image from local storage and flash:

- 1 Locate the backup image from local storage and flash (if a flash device is inserted) using the `show upgrade` command. This command lists all upgrade files and backup image files.

```
EWC.extremenetworks.com# show upgrade
1: AC-MV-09.01.01.0123-1.rue
2: rue-08.31.01.0192-rescue-user.tgz
```



Note

Backup image files are identified based on the file name format.

- 2 Restore the backup image from the local storage or flash device using the `upgrade ac backup-image-name` command. Make sure that you do not specify a **bckto local** option.

```
EWC.extremenetworks.com# upgrade ac rue-08.31.01.0192-rescue-user.tgz
This command restores the system to the backup image selected.
```

To avoid typing the full image name, you can specify the image using the index returned by the `show upgrade` command.

For example, the command below will install the image with index 2 which, in this case, is

rue-08.31.01.0192-rescue-user.tgz.

```
EWC.extremenetworks.com# upgrade ac 2
```

To Restore the Local Image from the FTP or SCP Server:

- 3 Download the backup image from the FTP or SCP server by using the `copy upgrade server | user | dir | backup-file-name [scp scp password]` command.

In the following example, the CLI command states that the upgrade file will be downloaded from the SCP server to the Wireless Appliance local drive:

```
EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images AC-
MV-08.21.01.2222-1.rue scp TestPassword
```

- 4 Restore the backup image by using the `upgrade ac new-image-name` command.

```
EWC.extremenetworks.com# upgrade ac rue-08.31.01.0192-rescue-user.tgz
```

Restoring the Backup Image from Rescue Mode

To restore the backup image from rescue mode:

- 1 Connect to the console port. Do not use the ESA ports or the Admin management port. For more information, see [Using the Console Port](#) on page 55.
- 2 Reboot the system. The following menu is displayed during the reboot process:

```
-----
Controller
Controller rescue
-----
```

- 3 Use your cursor to highlight **Controller rescue**, and then press **[Enter]** to enter Rescue mode.

The following menu is displayed.

```
1) Force System Recovery
2) Create System Backup Image
3) Display Backup Images
4) FTP Menu
5) Network Interface Menu
```

```

6) Manually run File System Check Utility (fsck)
7) Restore Backup Image directly from the FTP server
8) Authentication Service Management Menu
9) Flash Menu
R) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the selected
image (either backup or factory).
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice:

```

- 4 Do one of the following:
 - If the backup image was backed up to the local drive of the ExtremeWireless Appliance, restore from the local drive.
 - If the backup image was backed up to a remote FTP server, restore from a remote FTP server.
 - If a USB device with the backup image on it is mounted on the ExtremeWireless Appliance, restore from the USB device.

Restoring from the Local Drive

To restore from the local drive:

- 1 On the **Rescue** menu, type 1.

The list of backup images on the local drive of the wireless controller are displayed.

```
Currently Stored Images
```

```
-----
```

```

1) AC-MV-09.01.01.0123-1.ruevps
2) rue-08.31.01.0192-rescue-user.tgz
B) Abort and go back to previous Menu

```

```
Please select which image to use for restoring:
```

Backup image names end in `-rescue-user.tgz` (see [Backing Up Image File Name](#) on page 12). Be careful not to select the upgrade image (AC-MV-09.01.01.0123-1.rue) when the backup image is needed.

Restoring to the upgrade image will restore the system to factory defaults and lose all of the configuration (see [Restoring to Factory Default](#) on page 25).

- 2 Type the sequence number of the backup image that you want to restore.

The following message is displayed:

```

Selected Restore Image is: rue-08.31.01.0192-rescue-user.tgz
This procedure is irreversible, do you wish to continue (Y/N)?

```

- 3 Type Y.

The wireless controller initiates the recovery process.

```
Performing System recovery, this may take a while...
```

```
Cleaning out normal mode partitions...
```

```
Cleaning Completed.
```

```
Mount normal mode main partition
```

```
Mounting rest of normal mode partitions...done.
```

```
Restoring from the backup image...
```

```
Restoration Completed!
```

```
Unmount normal mode partitions
```

```
System Recovery Complete!
```

```
Reboot the system for changes to take effect.
```

```
Proceed with reboot (y/n):
```

4 Type **y**.

The wireless controller will reboot. After the reboot, the wireless controller restores the backed up image with its original configuration.

Restoring from a Remote FTP Server

To restore from a remote FTP server:

1 On the **Rescue** menu, type 5.

The following menu is displayed:

- ```
1) Display Current Rescue Interface Info
2) Enter Interface Information
3) Change default gateway
4) Test interface by ICMP (ping)
B) Return back to the top menu
```

## 2 Configure the Network Interface. Type in the Network Interface menu, and then type the following:

- IP address of your wireless controller management port
  - IP mask
  - IP address of Gateway
- ```
Your choice> 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
Input: 192.168.1.201:255.255.255.0 192.168.1.1
Configuring interface ...
Setting up network interface ...Done!
```

3 Type **B** to return to the top menu.4 Type **4** in the top menu to configure the FTP settings.

The **FTP** menu is displayed.

- ```
1) Enter FTP Settings
2) Change FTP server IP address
3) Change FTP port
4) Change user name
5) Change password
6) Change FTP directory
7) Change file name
8) Display current FTP settings
9) Display locally stored images
10) Download image from FTP server
11) Upload image onto the FTP server
12) Remove locally stored images
B) Return back to the top menu
Your choice: 1
Command syntax: ftp://<user>:<password>@<ftp_ip>:<port>/<directory&file>
~port information is optional: the default value is 21~
Please enter ftp info:
```

## 5 Type the FTP information.

```
ftp://administrator:abc123@192.168.4.181/tester/v6/backup-rescue-user.tgz
```

6 Type **B** to return to the top menu.

- ```
1) Force system recovery
2) Create System Backup Image
3) Display Backup Images
4) FTP Menu
5) Network Interface Menu
6) Manually run File System Check Utility (fsck)
7) Restore Backup Image Directly From The FTP Server
```

- ```

8) Authentication Service Management Menu
9) Flash Menu
R) Reboot
Your choice:
7 Type 7.

The following message is displayed:
Your choice: 7
Make sure correct information is entered for Interface and FTP settings.
IP: 192.168.4.191 netmask 255.255.255.0 gateway:
FTP Settings: IP 192.168.4.181, port 21, user: administrator, password: abc123,
directory: /tester/v6/, file backup-rescue-user.tgz
This procedure is irreversible, do you wish to continue (Y/N)?
8 Type Y.

The wireless controller initiates the recovery process.
9 Reboot the wireless controller.

After the reboot, the wireless controller restores the backed up image with its original configuration.

```

## Restoring the Rescue Image

The rescue image resides on the wireless controller's hard disk in a separate partition called the rescue partition; the running software image is stored in the normal mode partition.

You can restore the rescue partition in the rare event that it becomes unavailable or corrupted (for example, because of a hardware disk hardware error or a power failure during upgrade). To restore the rescue partition, you must obtain a healthy rescue image and install it on the wireless controller.

A healthy rescue image is available from one of the following locations:

- The normal mode partition. A locally saved rescue image is delivered as part of the upgrade image and saved on the normal mode partition during the upgrade process.
- The Extreme Networks repository site. On the Extreme Networks repository site, one rescue image exists for each controller platform. The following table lists the file extension associated with each of the controller platforms. The file extension for the rescue image begins with the letter *r* to identify the file as a rescue image.

**Table 4: Rescue Image File Naming Conventions**

| Wireless Appliance Model | Rescue File Extension |
|--------------------------|-----------------------|
| C5110                    | .rtxe                 |
| C5210                    | .rrue                 |
| C4110                    | .rgxe                 |
| C25                      | .rpfe                 |
| C35                      | .rcwe                 |



**Table 4: Rescue Image File Naming Conventions (continued)**

| Wireless Appliance Model    | Rescue File Extension |
|-----------------------------|-----------------------|
| V2110 (VmWare platform)     | .rbge                 |
| V2110 (MS Hyper-V platform) | .rize                 |

**Note**

Use the restore procedure in an emergency only when the rescue partition is not accessible. Restore commands are available in the CLI to administrators only; these commands are not listed when you enter the help command.

To restore the rescue image:

- 1 Log into the CLI as administrator from the console or by using SSH.
- 2 List the locally saved rescue images by entering the command:

```
EWC.extremenetworks.com# show restore-rescue
1: rescue.rrue
```

If a rescue image exists, go to step 3; if no rescue images exist, skip to step 5.

- 3 To restore the rescue partition using the locally saved rescue image, enter the command: `restore-rescue local imagefilename`

For example, to restore from the locally saved rescue image, `rescue.rrue`, enter the command:

```
EWC.extremenetworks.com# restore-rescue local rescue.rrue
```

- 4 To restore the rescue partition from any repository site:
  - a Download the appropriate rescue image to the locally accessible FTP server. Make sure that the rescue image you download matches the main image (platform and version). [Table 4](#) on page 24 lists the platforms and the corresponding rescue image file extensions.
  - b Download the rescue image from the FTP server and install it into the controller by entering the following command:

```
restore-rescue ftp serverip | user | password | dir | imagefilename
```

For example, to download the rescue image for the model C5210 controller from the FTP site and, as the user `admin` with the password `abc123`, install the rescue image, `AC-MV-09.01.01.0183-1.rrue`, into the store directory, enter the following command:

```
EWC.extremenetworks.com# restore-rescue ftp 1.1.1.1 admin abc123 store/ AC-
MV-09.01.01.0183-1.rrue
```

## Restoring to Factory Default

To restore the system to a particular image with factory defaults, restore the system from rescue mode with the upgrade image as the restore image.

For example, if the system needs to be restored to factory default image `V10.01`, enter the rescue mode, follow the procedure to restore the backup image (as explained in [Restoring the Backup Image from Rescue Mode](#) on page 21) and, instead of selecting the backup image, provide the upgrade image

V10.01 (local, flash or download from FTP), and perform the restore. The system is restored to the V10.01 with factory default values.



**Caution**

Be aware that restoring a system to factory defaults means that the configuration is lost including the IP connectivity, certificates, and licenses. Restoring to factory default is possible only from rescue mode.

---

# 3 Backing Up and Restoring the Configuration

Backing Up the Wireless Controller Configuration

Uploading a Backup to a Server

Copying a Local Backup to Flash

Scheduling a Backup

Deleting a Backup

Restoring the Wireless Controller Configuration

Downloading a Backup File

## Backing Up the Wireless Controller Configuration

Backing up the wireless controller database and creating a software package backup are two different processes. Backing up the wireless database only involves creating a backup of specific content in the wireless database. For example, you can choose to backup configuration, logs, or audit information. To create a backup image of your operating system, use the backup and restore functionality of the system.



### Note

Configuration data for the wireless controller is saved in NVRAM (non-volatile memory).

When you backup the wireless database, you can choose to do the following:

- Back up the wireless database now
- Upload a backup to an FTP or SCP server or flash
- Schedule when a backup occurs
- Schedule a backup and copy it to an FTP or SCP server or flash



### Note

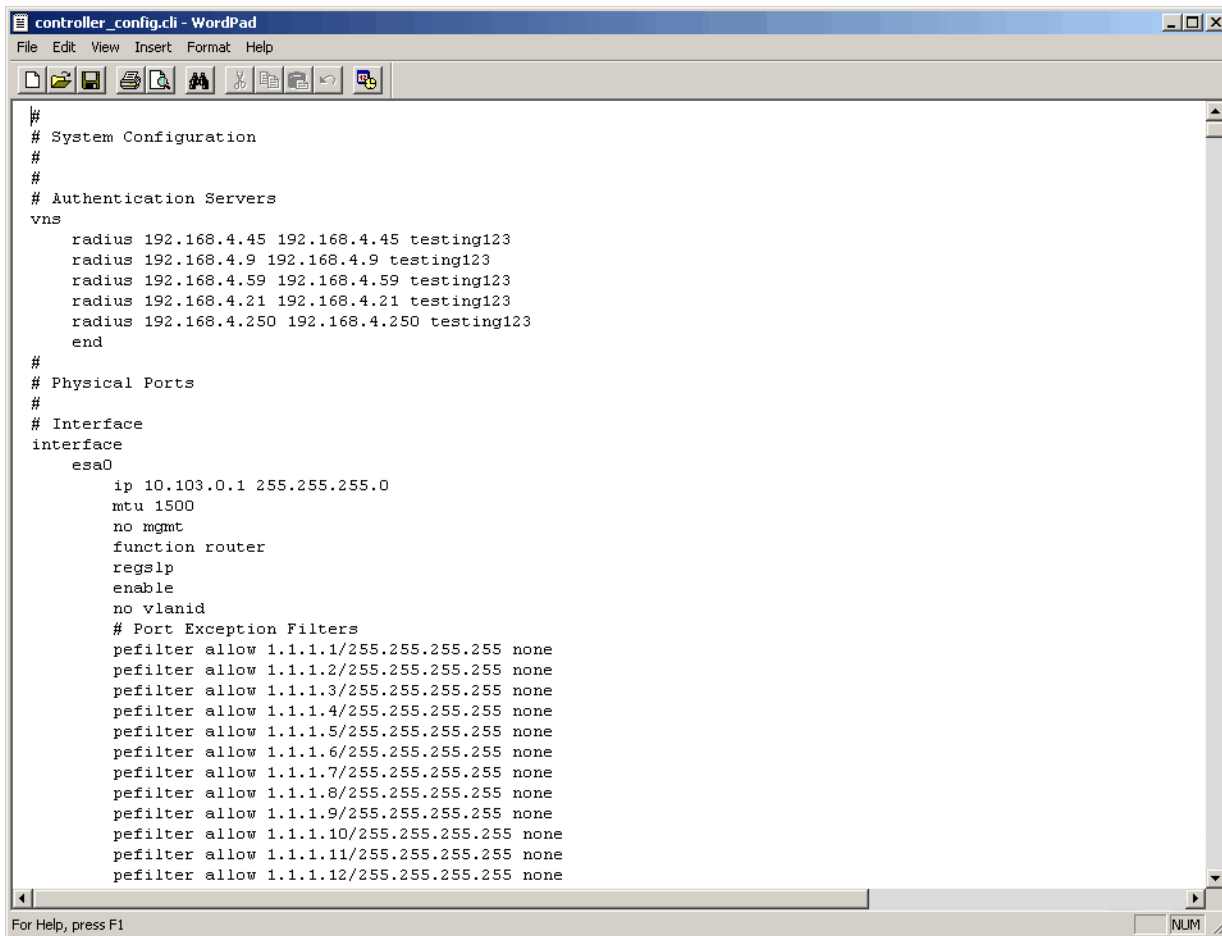
V2110 (MS Hyper-V platform) does not support flash functionality.

## Working with a Portable and Text Editable Backup

When the controller database backup is processed, a .zip file is created. The contents of the .zip file will vary depending on what type of database backup you process.

If you process a configuration information backup, one of the files included in the .zip file is a .cli file. When the .zip file is stored on a server or flash, the .zip file contents can be extracted and the .cli file can be edited.

This editable .cli file when imported to the controller will reproduce the identical configuration from which the original configuration was generated. This editable .cli file provides an easy method for replicating identical configurations on multiple controllers. Below is a sample .cli file. The .cli file contains CLI commands, which will replicate the configuration that the backup was based on when the file is imported.



```

controller_config.cli - WordPad
File Edit View Insert Format Help
#
System Configuration
#
#
Authentication Servers
vns
 radius 192.168.4.45 192.168.4.45 testing123
 radius 192.168.4.9 192.168.4.9 testing123
 radius 192.168.4.59 192.168.4.59 testing123
 radius 192.168.4.21 192.168.4.21 testing123
 radius 192.168.4.250 192.168.4.250 testing123
end
#
Physical Ports
#
Interface
interface
 esa0
 ip 10.103.0.1 255.255.255.0
 mtu 1500
 no mgmt
 function router
 regslp
 enable
 no vlanid
 # Port Exception Filters
 pefilter allow 1.1.1.1/255.255.255.255 none
 pefilter allow 1.1.1.2/255.255.255.255 none
 pefilter allow 1.1.1.3/255.255.255.255 none
 pefilter allow 1.1.1.4/255.255.255.255 none
 pefilter allow 1.1.1.5/255.255.255.255 none
 pefilter allow 1.1.1.6/255.255.255.255 none
 pefilter allow 1.1.1.7/255.255.255.255 none
 pefilter allow 1.1.1.8/255.255.255.255 none
 pefilter allow 1.1.1.9/255.255.255.255 none
 pefilter allow 1.1.1.10/255.255.255.255 none
 pefilter allow 1.1.1.11/255.255.255.255 none
 pefilter allow 1.1.1.12/255.255.255.255 none

```

For information on how to import a backup onto the controller, see [Restoring the Wireless Controller Configuration](#) on page 32.

#### Note

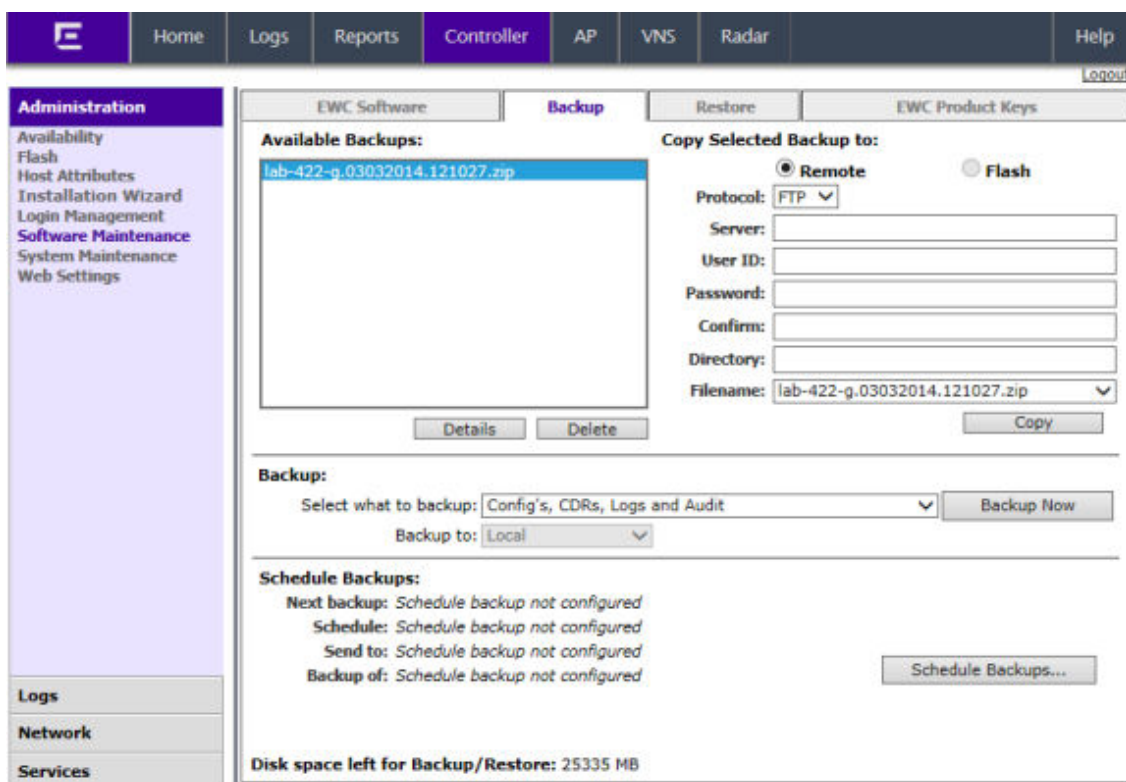


Backup configurations saved in local storage are deleted during the upgrade. To preserve your backed up configurations, upload them to an external FTP or SCP server, or flash before performing the upgrade.

To back up the wireless database using the GUI:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.

- 3 Click the **Backup** tab.



The **Available Backups** list displays items that have already been backed up and are available.

- 4 In the **Backup** section:
  - click an item from the **Select what to backup** drop-down list.
  - select Local or Flash from the **Backup to** drop-down list.
- 5 To launch the backup of the selected items, click **Backup Now**.

The **Software Maintenance** window is displayed, providing the status and results of the backup.

## Uploading a Backup to a Server

You can upload an existing backup file to a server using FTP (file transfer protocol) or SCP (secure copy protocol).

To upload an existing backup to a server using the GUI:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration** > **Software Maintenance**.
- 3 Click the **Backup** tab.
- 4 Select **Remote** in **Copy Selected Backup to**.

- 5 To upload a backup, do the following:
  - **Protocol** – Click the file transfer protocol you want to use to upload the backup file, SCP or FTP.
  - **Server** – Type the IP address of the server where the backup will be uploaded.
  - **User ID** – Type the user ID used to log into the server.
  - **Password** – Type the corresponding password for the user ID.
  - **Confirm** – Type the corresponding password for the user ID to confirm it was typed correctly.
  - **Directory** – Type the directory on the server where the backup file will be stored.
- 6 In the **Filename** drop-down list, click the backup you want to upload.
- 7 Click **Copy**.  
The **Software Maintenance** window is displayed, providing the status and results of the operation.

## Copying a Local Backup to Flash

You can copy an existing local backup file to a flash drive.

To copy an existing local backup to a flash using the GUI:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration** > **Software Maintenance**.
- 3 Click the **Backup** tab.
- 4 Select **Flash** in **Copy Selected Backup to**. Flash has to be mounted for this.
- 5 In the Filename drop-down list, select the local backup you want to copy.
- 6 Click **Copy**. The **Software Maintenance** window is displayed, providing the status and results of the operation.
- 7 The backup copy located on flash is going to be displayed in Available Backups list as well.

To copy an existing local backup to a flash using the CLI:

- 8 Log into the system using SSH or console.

- 9 Transfer the backup file from the local storage to a flash using the following command:

```
copy configuration (to-local | to-flash | to-remote server user dir [ftp password | scp password]) (from-local filename | number | from-flash filename | number | from-remote server user dir file [ftp password | scp password])
```

For example, to transfer the backup file BAK.03122009.071327.zip from local storage to a flash:

```
EWC.extremenetworks.com#copy configuration to-flash from-local BAK.03122009.071327.zip
```

To see all backup files stored locally and on flash, use the show export command.

```
EWC.extremenetworks.com#show export
1: BAK.03122009.071327.zip
2: BAK.03122009.071327.zip(flash)
```

## Scheduling a Backup

When you schedule a backup, you can choose to upload the backup to a server, have the scheduled backup saved on your system or flash drive.

To schedule a backup:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.
- 3 Click the **Backup** tab.
- 4 Click **Schedule Backups**.

The **Software Maintenance** screen is displayed.

**Software Maintenance**

What to backup:  Send backup file to:

Schedule Task:   Flash  Local  Remote

Save Cancel

- 5 In the **What to backup** drop-down list, click what you want to backup:
  - Configs, CDRs, Logs and Audit
  - Configurations only
  - CDRs only
  - Logs only
  - Audit only
- 6 In the **Schedule task** drop-down list, click the frequency of the backup:
  - **Daily** – Click the **Start Time** and Recurrence for the backup.
  - **Weekly** – Click the **Start Time** and Recurrence for the backup.
  - **Monthly** – Click the **Start Time** and Recurrence for the backup.
  - **Never** – Click to disable schedule backup.
- 7 Under **Send backup file to**, select Flash, Local, or Remote.

- 8 If you select **Remote** (scheduling a backup to a remote server), specify a server to where the scheduled backup will be copied to. Do the following:
  - **Protocol** – Click the file transfer protocol you want to use to upload the backup file, SCP or FTP.
  - **Server** – Type the IP address of the server to where the scheduled backup will be copied to.

**Note**

The Server parameter supports both IPv4 and IPv6 addresses.

- **User ID** – Type the user ID used to log into the server.
  - **Password** – Type the corresponding password for the user ID.
  - **Confirm** – Type the corresponding password for the user ID to confirm it was typed correctly.
  - **Directory** – Type the directory on the server where the image file will be stored.
- 9 To save your changes, click **Save**.

## Deleting a Backup

You can delete a backup if it is no longer needed on your system or flash drive.

To delete a backup using the GUI:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.
- 3 Click the **Backup** tab.
- 4 In the **Available Backups** list, click the backup you want to delete.
- 5 Click **Delete**.
- 6 In the dialog box that is displayed, click **OK** to confirm the deletion.

The **Software Maintenance** window is displayed, providing the status and results of the deletion.

## Restoring the Wireless Controller Configuration

To restore the configuration using the GUI:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.
- 3 Click the **Restore** tab.
- 4 The **Available Backups** list displays available backup files for restore.
- 5 In the **Restore** section, Select a backup to restore.
- 6 To launch the restore of the selected item, click **Restore Now**.



- 7 The **Software Maintenance** window is displayed, providing the status and results of the restore.

To restore the configuration using the CLI:

- 8 Log into the CLI using SSH or console.
- 9 View all backup files in local storage by using the `show import` command.
- 10 Restore the configuration by using the `import filename | number` command.

```
EWC.extremenetworks.com#show import
1: EWC.03122009.071327.zip
```

For example, to restore the backup file shown in the example under step 1:

```
EWC.extremenetworks.com#import EWC.03122009.071327.zip
```

To avoid typing the full name of the backup file, you can use the index number returned by the show import command.

The restore can be run directly from an imported file stored on flash. In this case, the string “(flash)” must be suffixed to the end of the specified file name.

```
EWC.extremenetworks.com#import 1
```

The command will restore the controller configuration to the configuration in the backup file.

## Downloading a Backup File

You can download an existing backup file from a server using FTP (file transfer protocol) or SCP (secure copy protocol), or from flash to local storage.

To download an existing backup from a server using the GUI:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.
- 3 Click the **Restore** tab.
- 4 Select a Remote under **Copy Backup File From**.
- 5 Enter values for the following:
  - **Protocol** — Select the file transfer protocol you want to use to download the backup file (SCP or FTP).
  - **Server** — Type the IP address of the server from which the backup will be downloaded.

**Note**

The Server parameter supports both IPv4 and IPv6 addresses.

- **User ID** — Type the user ID used to log into the server.
  - **Password** — Type the corresponding password for the user ID.
  - **Confirm** — Type the corresponding password for the user ID to confirm it was typed correctly.
  - **Directory** — Type the directory on the server where the backup file is stored.
  - **Filename** — Enter the name of the backup file you want to download.
  - **Destination** — Define whether a file is transferred to local or flash from a remote server.
- 6 Click **Copy**.

The **Software Maintenance** window is displayed, providing the status and results of the download.

To download an existing backup from a server using the CLI:

- 7 Log into the system using SSH or console.
- 8 Download the backup file from the FTP or SCP server using the following command:  

```
EWC.extremenetworks.com#copy configuration (to-local | to-flash | to-remote serveruser dir [ftp password | scp password]) (from-local filename|number | from-flash filename|number | from-remote server user dir file [ftp password | scp password])
```

For example, to download the backup file EWC.03122009.071327.zip locally from an SCP server:

```
EWC.extremenetworks.com#copy configuration to-local from-remote 192.168.3.10 test
conf_bak_dir
EWC.03122009.071327.zip scp abc123
```

The command will download the file and store in the local storage.

To see all backup files stored in the local storage, use the show import command.

```
EWC.extremenetworks.com#show import
1: EWC.03122009.071327.zip
```

To copy an existing backup from a flash to local storage using the GUI:

- 9 From the top menu, click **Controller**.  
The **Wireless Controller Configuration** screen is displayed.
- 10 From the left pane, click **Administration > Software Maintenance**.  
The **EWC Software** tab is displayed.
- 11 Click the **Restore** tab.
- 12 Select a source Flash under **Copy Backup File From**. Flash has to be mounted for this.

13 In the **Filename** drop-down list, click the backup you want to transfer.

14 Click **Copy**.

The Software Maintenance window is displayed, providing the status and results of the operation.

The local backup copy is going to be displayed in Available Backups list as well.

To copy an existing backup from a flash to local storage using the CLI:

15 Log into the system using SSH or console.

16 Copy the backup file from the local storage to flash using the following command:

```
EWC.extremenetworks.com#copy configuration (to-local | to-flash | to-remote server user dir [ftp password | scp password]) (from-local filename|number | from-flash filename|number | from-remote server user dir file [ftp password | scp password])
```

For example, to copy the backup file BAK.03122009.071327.zip locally from a flash:

```
EWC.extremenetworks.com#copy configuration to-local from-flash BAK.03122009.071327.zip
```

To see all backup files stored locally and on flash, use the show import command.

```
EWC.extremenetworks.com#show import
1: BAK.03122009.071327.zip
2: BAK.03122009.071327.zip(flash)
```

# 4 Upgrading the Wireless Convergence Software

## Upgrading Process

Upgrading Using the GUI

Upgrading Using the CLI

Migrating the Platform Configuration

Upgrading Two Controllers in Availability Mode

Upgrading Two Controllers in Session Availability Mode

## Upgrading Process

During the upgrade process, the upgrade program does the following:

- Uninstalls the old version
- Installs the new version
- Preserves and migrates the configuration to the new version



### Note

V2110 (MS Hyper-V platform) does not support flash functionality.



### Note

When you upgrade the Wireless Controller Software, the previous SSL Configuration file is replaced by a new one. Consequently, the manual edits that were made in the previous SSL Configuration file are lost. If you have done manual edits to the SSL configuration file to install certificates for Captive Portal on the virtual interfaces, it is suggested to use EWC Captive Portal Certificate Configuration instead.

## Upgrading to V10

If you are running a software version earlier than V9.01, you must first upgrade to V9 before upgrading to V10.

## Upgrade Path Matrix to V9

Use the following matrix to determine the upgrade path to required version V9 that is appropriate for your wireless controller and the software running on it.

**Table 5: Upgrade Matrix**

| Platform | From                                                   | To                      |
|----------|--------------------------------------------------------|-------------------------|
| C5110    | V6R0                                                   | V6R1 FR5 (or higher FR) |
|          | V6R1 FR5 (or higher FR)                                | V7.41                   |
|          | V7.0, V7.11, V7.21, V7.31                              | V7.41                   |
|          | V7.41, V8.01, V8.11, V8.21, V8.31                      | V8.32                   |
|          | V8.32, V9.01, V9.12, V9.15                             | V9.21                   |
| C4110    | V6R1                                                   | V6R1 FR5 (or higher FR) |
|          | V6R1 FR5 (or higher FR)                                | V7.41                   |
|          | V7.0, V7.11, V7.21, V7.31                              | V7.41                   |
|          | V7.41, V8.01, V8.11, V8.21, V8.31                      | V8.32                   |
|          | V8.32, V9.01, V9.12, V9.15                             | V9.21                   |
| C25      | V7.41, V8.01, V8.11, V8.21, V8.31                      | V8.32                   |
|          | V8.32, V9.01, V9.12, V9.15                             | V9.21                   |
| V2110    | V8.01, V8.11, V8.21, V8.31, V8.32, V9.01, V9.12, V9.15 | V9.21                   |
| C5210    | V8.21, V8.31, V8.32, V9.01, V9.12, V9.15               | V9.21                   |

For information about migrating from one platform to another, see [Migrating the Platform Configuration](#) on page 45.

For information about upgrading controllers operating in “availability” mode, see [Upgrading Two Controllers in Availability Mode](#) on page 47.

## Upgrading the Image File Name

The format of the upgrade image file name is: `AC-MV-<version>-<revision>.<platf>`

- version — version number (for example 08.00.00.0174)
- revision — software release number
- platf — is one of the values from the table below

**Table 6: Upgrade File Name Extensions**

| Wireless Appliance models       | Platform |
|---------------------------------|----------|
| ExtremeWireless Appliance C5110 | .txe     |
| ExtremeWireless Appliance C5210 | .rue     |
| ExtremeWireless Appliance C4110 | .gxe     |
| ExtremeWireless Appliance C25   | .pfe     |
| ExtremeWireless Appliance C35   | .cwe     |

**Table 6: Upgrade File Name Extensions (continued)**

| Wireless Appliance models                                     | Platform |
|---------------------------------------------------------------|----------|
| ExtremeWireless Virtual Appliance V2110 (VmWare platform)     | .bge     |
| ExtremeWireless Virtual Appliance V2110 (MS Hyper-V platform) | .ize     |

## Upgrading Using the GUI

Use the following procedure if you are upgrading using the GUI.



### Note

You should always backup the existing software image during the upgrade process. Backing up provides you the option of restoring your wireless controller to its previous configuration. For more information, see [Restoring the Backup Image from the GUI](#) on page 18.

The wireless software provides two upgrade options:

- **Local** – Upgrades the wireless software by using the image file that is located either on the local drive or USB device. This is the preferred method of upgrade.



### Note

Before starting the local upgrade, the image file needs to be downloaded to the local drive or a flash device has to be provided with the image file.

- **Remote** – Upgrades the wireless software by using an image file that is located on an external FTP server. The upgrade program downloads the image file from the FTP server, unpacks it and installs it directly on the system without retaining a local copy of the image file.



### Note

The Wireless Assistant GUI displays Remote as the upgrade option for upgrade from a remote FTP server.

## Upgrading Locally

When you upgrade locally, the upgrade program upgrades the wireless software by using the image file that is located either on the local drive or USB device.

To perform a local upgrade of the wireless software:

- 1 From the top menu, click **Controller**.

- 2 From the left pane, click **Administration > Software Maintenance**.

- 3 Select **Local**, and then click the image file you want to use from the list of upgrade files.

#### Note



Multiple images may be listed: image files on the local drive, image files on the flash device (if a flash device is inserted), and image backup files (end with -rescue-user.tgz) if they exist on the local drive or flash device. Select the desired image. Image files use the AC-MV-<version>-<revision>.<platf> name format, as explained in [Upgrading the Image File Name](#) on page 37.

#### Note



Regardless of whether the upgrade image file is on the local drive or flash device, the wireless controller displays it in the list of upgrade files.

#### Caution



You should always backup the existing software image during the upgrade process. Backing up provides you the option of restoring your wireless controller to its previous configuration if needed. For more information, see [Restoring the Backup Image from the GUI](#) on page 18.

- 4 Select one of the following upgrade options:
  - To schedule a software upgrade, select the Schedule upgrade for option. The earliest you can schedule an upgrade is 5 minutes into the future.

Use the Month, Day, Hour, and Minute drop-down lists to schedule the upgrade and then click **Schedule upgrade**.

Review the upgrade settings in the dialog box, and then click **OK** to confirm the upgrade settings. The **EWC Software** tab fields gray out.

**Note**

A scheduled upgrade is not a recurring event. The wireless controller allows only one **Scheduled upgrade** to be configured at a time.

---

- To upgrade the software immediately, select the **Upgrade now** option.

Click the **Upgrade now** button.

Review the upgrade settings in the dialog box, and then click **OK** to confirm the upgrade settings. A window displays the upgrade status.

The wireless controller reboots after the upgrade process is completed.

### *Downloading the Remote Image File to the Local Drive or USB Device*

To download the Remote Image File to the local drive or USB device:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.



3 Select **Remote**.

The FTP/SCP server boxes are displayed.

The screenshot shows the 'EWC Software' upgrade configuration page. The 'Select upgrade:' section has three radio buttons: 'Local', 'Remote' (selected), and 'Flash'. Below 'Remote' are fields for Protocol (FTP), Server (134.141.120.74), User ID (test), Password (masked), Confirm, Directory (new/ac/rpm/build09.01.01.0174/), and Filename (AC-MV-09.01.01.0174-1.gxe). The 'Destination' dropdown is set to 'Local'. A 'Get Image now' button is present. The 'Backup system image to:' checkbox is checked, with 'Local' selected under it. The 'Upgrade now' radio button is selected, and 'Schedule upgrade for:' is unselected. The current controller time is shown as [Mon Mar 3 14:51 2014]. A 'Disk space left for images: 1727 MB' indicator is at the bottom. A navigation sidebar on the left includes 'Administration', 'Logs', 'Network', and 'Services'.

## 4 Type the following:

- **Protocol** – FTP or SCP.
- **Server** – The IP address of the server to retrieve the image file from.
- **User ID** – The user ID used to log into the server.
- **Password** – The password for the user ID.
- **Confirm** – The password to log on to the server. This field is to confirm you have typed the correct password.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** – The name of the image file to retrieve.

5 In the **Destination** drop-down list, click **Local** or **Flash** to specify where the image is downloaded to.6 Click **Get Image now**.

The **Download Image** window is displayed, providing the status and results of the download. The image is downloaded onto your system and added to the **Select upgrade** list.

**Note**

SCP can only be used to download an image and cannot be used to start remote upgrade. The Upgrade now button is disabled when SCP is selected from the drop-down list.

## Upgrading Remotely

When you upgrade the wireless software remotely, the upgrade program upgrades the software image by using the image file that is located on an external FTP server. The upgrade program downloads the image file from the FTP server, unpacks it and installs it directly on the system without retaining a local copy of the image file. The Wireless Assistant GUI displays Remote as the upgrade option for upgrade from a remote FTP server with FTP selected as the protocol.



### Note

SCP can only be used to download an image and cannot be used to start remote upgrade. The Upgrade now button is disabled when SCP is selected from the drop-down list.



### Caution

You should always backup the existing software image during the upgrade process. Backing up provides you the option of restoring your controller to its previous configuration if needed. For more information, see [Restoring the Backup Image from the GUI](#) on page 18.

### Running the Upgrade from the FTP Server

To run the upgrade from the FTP Server via the Wireless Assistant GUI:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.
- 3 Select **Remote**.

The FTP server boxes are displayed.

The screenshot shows the 'EWC Software' configuration page in the Wireless Assistant GUI. The 'Controller' menu item is selected in the top navigation bar. The left sidebar shows 'Administration' > 'Software Maintenance' selected. The main content area is titled 'EWC Software' and has tabs for 'Backup', 'Restore', and 'EWC Product Keys'. The 'Select upgrade:' section has three radio buttons: 'Local', 'Remote' (selected), and 'Flash'. The 'Backup system image to:' section has three radio buttons: 'Flash', 'Local' (selected), and 'Remote'. The 'Flash' option is also selected. The 'Get Image now' button is disabled. The 'Upgrade now' button is visible at the bottom right. The current controller time is displayed as 'Mon Mar 3 14:51 2014'. The disk space left for images is 1727 MB.

- 4 Type the following:
  - **Protocol** – FTP.
  - **Server** – The IP address of the FTP server to retrieve the image file from.
  - **User ID** – The user ID used to log into the FTP server.
  - **Password** – The password for the user ID.
  - **Confirm** – The password to log on to the FTP server. This field is to confirm you have typed the correct password.
  - **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
  - **Filename** – The name of the image file to retrieve.
- 5 To schedule a software upgrade, select the **Schedule upgrade for** option. The earliest you can schedule an upgrade is five minutes into the future.
  - a Use the Month, Day, Hour, and Minute drop-down lists to schedule the upgrade.
  - b Click **Schedule upgrade**.
  - c Review the upgrade settings in the dialog box, and then click **OK** to confirm the upgrade settings. The **EWC Software** tab fields gray out.



#### Note

A scheduled upgrade is not a recurring event. The wireless controller only allows one scheduled upgrade to be configured at a time.

- 6 To upgrade the software immediately, select the **Upgrade now** option.
  - a Click the **Upgrade now** button.
  - b Review the upgrade settings in the dialog box, and then click **OK** to confirm the upgrade settings. A window displays the upgrade status.

The wireless controller reboots after the upgrade process is completed.

## Modifying a Scheduled Software Upgrade

To modify a scheduled software upgrade, first cancel the existing scheduled upgrade, then reschedule a new upgrade.

To modify a scheduled software upgrade:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.
- 3 Click **Cancel upgrade**.
- 4 In the dialog box that is displayed, click **OK** to confirm the cancellation of the upgrade. The scheduled software upgrade is cancelled and the **EWC Software** tab fields become available for scheduling a new software upgrade.

## Deleting a Software Image

It is OK to delete a software image if it is no longer needed on your system.

To delete a software upgrade:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > Software Maintenance**.
- 3 In the **Select upgrade** list, click the software upgrade you want to delete.
- 4 Click **Delete selected**.
- 5 In the dialog box that is displayed, click **OK** to confirm the deletion of the upgrade. The **Software Maintenance** window is displayed, providing the status and results of the deletion.

## Upgrading Using the CLI



### Note

The first step to upgrade the software is to backup the image of the existing software release. For more information, see [Backing Up and Restoring the Image](#) on page 11.

To upgrade the wireless software locally:

- 1 Use the `copy upgrade server | user | dir | file [dest] [scp scp password]` command to download the software upgrade bundle from the remote FTP or SCP server.
  - If you want to download the file on the controller flash device, type flash for **dest** option in the `copy upgrade server | user | dir | file [dest]` syntax.
  - If you want to download the file on the controller local drive, leave out the [dest] option in the `copy upgrade server | user | dir | file [dest]` syntax.
  - If you want to download the file from the SCP server, provide the corresponding SCP server, user, dir and file appended with `scp scp password`.
  - If you want to download the file from the FTP server do not specify `scp scp password` at the end, where server, user, dir and file will specify FTP server parameters.

**Example 1** – In the following example, the CLI command states that the upgrade file will be downloaded from the FTP server to the flash card.

```
EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images/ AC-
MV-08.00.01.0003-1.pfe flash
```

**Example 2** – In the following example, the CLI command states that the upgrade file will be downloaded from the FTP server to the controller local drive.

```
EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images/ AC-
MV-08.00.00.0123-1.pfe
```

**Example 3** – In the following example, the CLI command states that the upgrade file will be downloaded from the SCP server to the flash card.

```
EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images AC-
MV-08.31.01.0200-1.rue flash scp TestPassword
```

**Example 4** – In the following example, the CLI command states that the upgrade file will be downloaded from the SCP server to the controller local drive.

```
EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images AC-
MV-08.31.01.0200-1.rue scp TestPassword
```

- 2 Use the `show upgrade` command to confirm the upgrade file was downloaded successfully.

```
EWC.extremenetworks.com# show upgrade
1: AC-MV-08.00.00.0123-1.pfe
```

- 3 Upgrade the software by running `upgrade ac file name` command. Type `Yes` to the `Do you wish to continue?` prompt.

```
EWC.extremenetworks.com# upgrade ac AC-MV-08.00.00.0123-1.pfe bckto local
```

This command makes a local backup image of the running system and installs the selected upgrade image.

To avoid typing the image name, you can specify the image using the index returned by the `show upgrade` command.

For example, the command below will install the image with index 1 which, in this case, is AC-MV-08.00.00.0123-1.pfe: `upgrade ac 1 bckto local`

To upgrade the wireless software remotely:

- 4 Set up the FTP server from which you are downloading the file.

```
upgrade_image_src 192.168.4.10 test abc123 system/images AC-
MV-08.00.00.0123-1.pfe
```

- 5 Start the upgrade with `upgrade ac ftp bckto local` command.

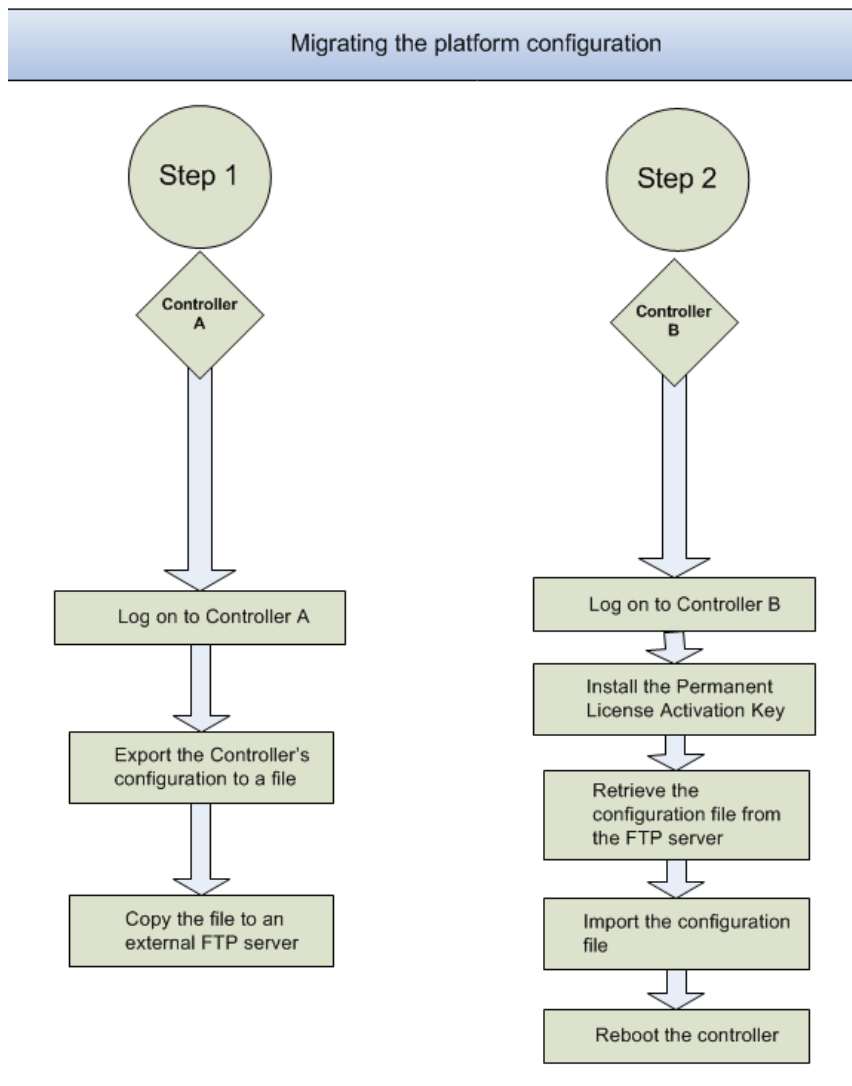
This command first makes a local backup image of the running system, downloads the upgrade image in temporary directory, and installs the image. No local copy of the image exists after the upgrade.

## Migrating the Platform Configuration

You can migrate a configuration from one model of wireless controller to another model. [Table 7](#) provides information on the pairs of wireless controller models that support configuration migration from one another. [Figure 1](#) on page 46, displays the steps to migrate a configuration between platforms.

**Table 7: Configuration Migration Table**

| From                                                        | To                                            |
|-------------------------------------------------------------|-----------------------------------------------|
| C25, running V9.01/V9.12/V9.15/V9.21/V10.01/V10.11          | C25, C35, C4110, C5110, V2110, running V10.21 |
| V2110, running V9.01/V9.12/9.15/V9.21/V10.01/V10.11         | C4110, C5110, C5210, running V10.21           |
| C4110, C5110, running V9.01/V9.12/V9.15/V9.21/V10.01/V10.11 | C5210, running V10.21                         |
| C35, running V9.21/V10.01/V10.11                            | C5210, running V10.21                         |



**Figure 1: Sequential Steps for Migrating a Configuration**

## To Migrate a Platform Configuration

To migrate a platform configuration, both the Source controller model and software and the Destination controller model and software must support the migration as described in [Table 7](#) on page 45.

- 1 Log on to the Source controller.
- 2 Export the controller configuration to a file by running the following CLI command.

```

EWC.extremenetworks.com# export configuration
Filename (EWC.extremenetworks.com.13062007.132046):
Comment: <enter a comment here - optional>
Please wait...
Creating EWC.extremenetworks.com.13062007.132046...
Backup/Export complete.

```

- 3 Use the `show export` command to list the current set of backup files.

- Copy the file to an external FTP or SCP server by running the `copy configuration` command.

```
EWC.extremenetworks.com#copy configuration to-remote server IP
username destination directory [ftp password
| scp password] from-local filename
```

- Log on to the Destination controller.
- Install the Permanent License Activation key.
- Retrieve the configuration file from the external FTP or SCP server by running the `copy configuration` command.

```
EWC.extremenetworks.com#copy configuration to-remote server IP
username destination directory [ftp
password | scp password]
from-local filename
```

- Type the password.
- Use the `show import` command to list the current set of backup files, which will include the retrieved configuration file.
- Import the configuration by running the `import filename` command.  
After the import process is completed, the wireless controller will reboot.



#### Note

The Management IP address will be identical to that of the controller from where the configuration is migrated.

## Upgrading Two Controllers in Availability Mode

This section, which describes how to upgrade the software version on two controllers in availability mode, is applicable if the availability pair is made of one of the following combinations:

**Table 8: Availability Pairs**

| Controller 1 | Controller 2 |
|--------------|--------------|
| C25          | C25          |
| C35          | C35          |
| C4110        | C4110        |
| C5110        | C5110        |
| C5210        | C5210        |
| V2110        | V2110        |



#### Note

The two wireless controllers in an 'availability' pair must be running the identical version of the software.

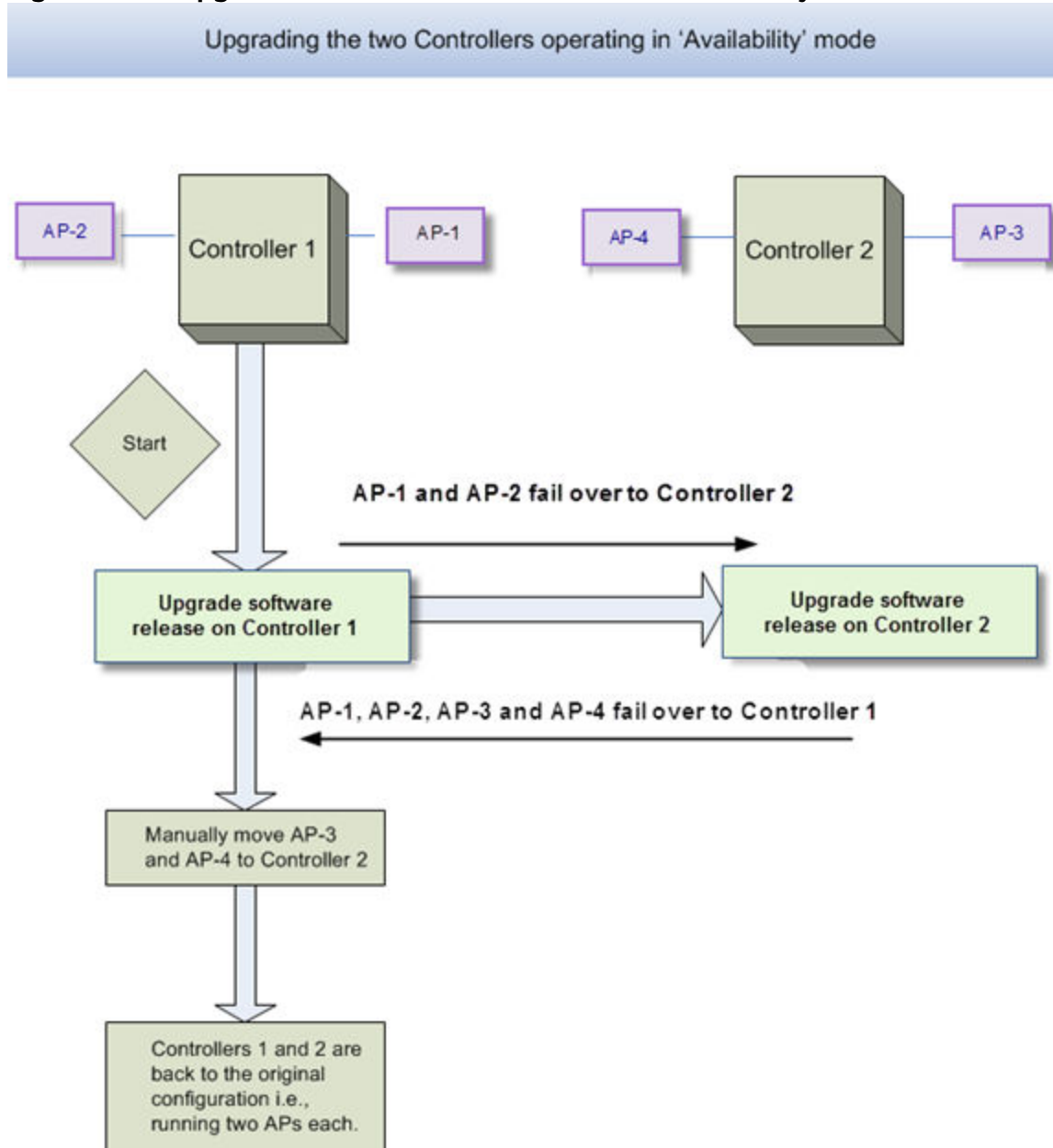
For the ease of understanding, this section is explained with the help of the following hypothetical scenario:

- The upgrade is to be carried out on the two controllers — EWC-1 and EWC-2.
- Both the controllers are operating in 'availability' mode.

- Both controllers are running the previous software release, and they need to be upgraded to the next software release.
- Each controller has two APs. EWC-1 has AP-1 and AP2, whereas EWC-2 has AP-3 and AP-4.
- AP-1 and AP-2 are configured as 'Local' on EWC-1 and 'Foreign' on EWC-2.
- AP-3 and AP-4 are configured as 'Local' on EWC-2 and 'Foreign' on EWC-1.

The following figure depicts the hypothetical upgrade process:

**Figure 2: The Upgrade Process for Two Controllers in Availability Mode**





## Upgrading Software on Controller 1

---



### Note

If you upgraded the software on the two controllers in session availability mode, you must perform a controlled upgrade on the wireless APs. For more information, see [Maintaining the Wireless AP Software](#) on page 99.

---

Use the standard procedures via the Wireless Assistant GUI or CLI commands to upgrade the software.

When you upgrade the software version on Controller 1, it will reboot. Consequently, the 'availability' feature automatically moves both AP-1 and AP-2 from Controller 1 to Controller 2. All clients registered with these two APs get disconnected. They re-connect automatically (if configured to do so) either to a different AP or to the same one after the service is restored.

After Controller 1 reboots, all 4 APs connect to Controller 2, which is still running the older software. Controller 1 is now upgraded to the new software release and has the same prior configuration. All 4 APs are running the older software.

## Upgrading Software on Controller 2

Use the standard procedures via the Wireless Assistant GUI or CLI commands to upgrade the software.

When you upgrade the software version on Controller 2, it will reboot. Consequently, the "Availability" feature will automatically move all 4 APs from Controller 2 to Controller 1. Because Controller 1 was upgraded to the newer software version, all the 4 APs are upgraded as well. This causes a short disruption of service.

All clients on all the four APs get disconnected. They re-connect automatically (if configured to do so) after the service is restored.

After Controller 2 reboots, all the four APs are associated with Controller 1. Both controllers are now upgraded to the new software release and have the same prior configuration. All the four APs are also upgraded to the new software release.

## Manually Moving APs Back to Local Controller

Manually move AP-3 and AP-4 from Controller 1 to Controller 2, where they were configured as 'Local' APs. After you manually move the APs, the network is back to its original configuration with each controller running two APs.

## Upgrading Two Controllers in Session Availability Mode

---

The process for upgrading two wireless controllers in session availability mode is identical to upgrading two controllers in availability mode. For more information, see [Upgrading Two Controllers in Availability Mode](#) on page 47.

# 5 Working with External Storage Devices

Working with an External Storage Device  
Mounting a Flash Device on the Wireless Controller  
Un-mounting a Flash Device from the Controller  
Deleting Files from a Flash Device



## Note

In this chapter, the term “flash device” applies to all external storage devices that can be used with the controllers.

## Working with an External Storage Device



## Note

V2110 (MS Hyper-V platform) does not support flash functionality (upgrade, backup, restore, storage, etc.).

You can use a USB device to do the following maintenance tasks:

- **Installing and upgrading the software:** You can install or upgrade the wireless software from a USB device.
- **Backing up the system:** You can store the existing image of the wireless software on a USB device as a backup while upgrading the software.
- **Restoring the software:** You can restore the backed up wireless software from a USB device.
- **Storing configuration backup files:** You can export and import configuration backup to/from flash, as well as transfer configuration backup file between flash, local storage and remote servers.
- **Storing exception traffic files:** You can store captured exception traffic on the USB device. For example, DHCP, OSPF, TFTP traffic.

The USB device is automatically made available to the GUI/CLI (mounted) by the controller when inserted in the device slot. After the flash device is mounted, the GUI/CLI shows the content of the flash device for the related operation, such as backup and upgrade. To manually unmount or remount an already inserted flash device, use the controller GUI:

- **Mount the flash device** – By mounting the flash device, you make the flash device that has been inserted into the controller available for use.

- **Unmount the flash device** – By unmounting the flash device, you make the flash device that has been inserted into the controller unavailable for use.

**Caution**

You must always unmount the flash device via the controller GUI before removing it from the controller. Failure to do so may corrupt the files on the flash device. Always wear an ESD wristband when inserting or removing a flash device.

- **Delete files stored on the flash device** – You can also delete files stored on a USB device. By deleting the files, you can create space on the USB device. For more information, see [Deleting Files from a Flash Device](#) on page 54.

## Flash Device File System Format

All flash devices used with the controller must be formatted in FAT32. Only the first partition of the flash device is used by the controller.

Controller software can operate (backup, restore, delete, etc.) only with files located in the root directory on the flash drives. In other words, it cannot operate with files located under directories.

Wireless controllers equipped with multiple USB connectors support only one USB device at a time, regardless of what USB connector the device is connected to. If you connect a second USB device while the first is already connected, the system will return an error.

**Warning**

Ensure all flash devices used with the controller are formatted to be non-bootable. Otherwise, the controller may experience difficulties when rebooting if connected to a bootable formatted flash device.

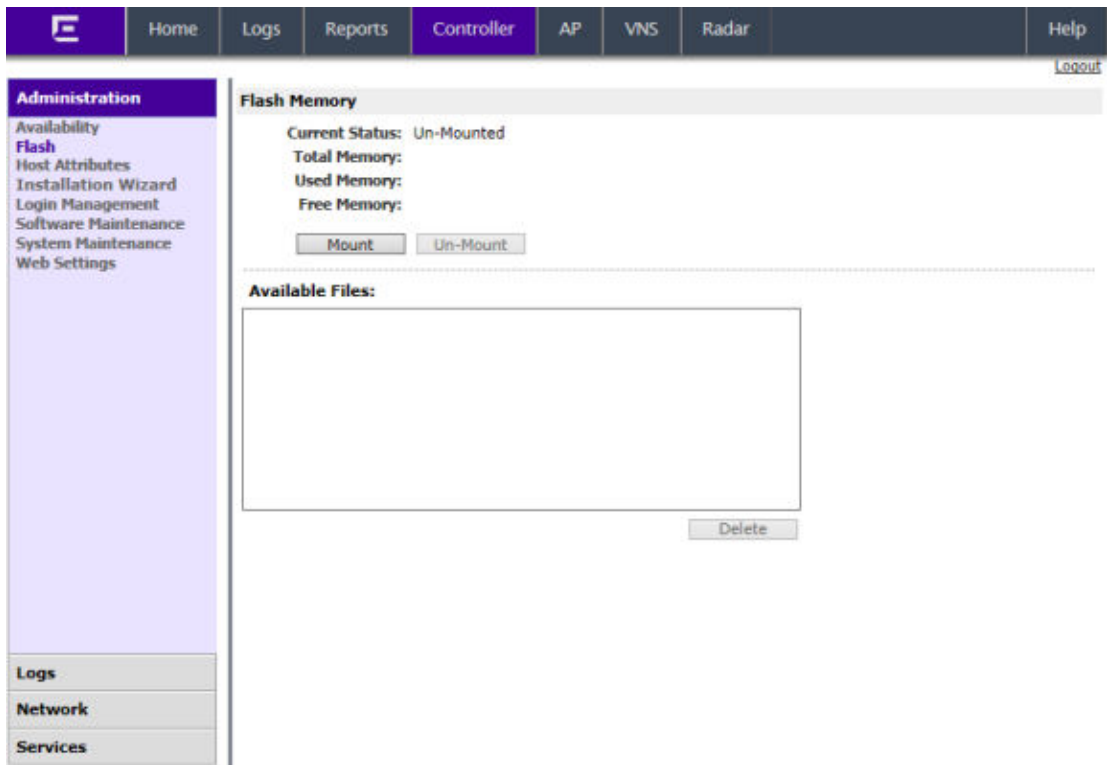
---

## Mounting a Flash Device on the Wireless Controller

To mount a flash device on the controller:

- 1 From the top menu, click **Controller**.

- From the left pane, click **Administration** > **Flash**.



**Figure 3: Flash Memory Screen**

- Click **Mount**, and then click **OK** to confirm the flash device mount. Once the mounting process is complete, the flash memory space is displayed and the files contained on the flash device are listed in the **Available Files** box.

When you mount the flash device, the F icon in the footer changes from red to green.



#### Note

If a flash device was already mounted (previously inserted), the screen shows the status as Mounted as well as all available files on the flash device.

The screenshot shows the 'Flash Memory' section of the Controller interface. The 'Current Status' is 'Mounted'. The memory statistics are: Total Memory: 1.9G, Used Memory: 1.4G, and Free Memory: 579M. There are 'Mount' and 'Un-Mount' buttons. Below, the 'Available Files' list includes: AC-MV-07.00.00.0088-1.txe, HWC-txe-V6R1.10209.0-rescue-user.tgz, Recovery Manager, bootmenu.exe, bootmenu.xml, bootwiz.cfg, bootwiz.sys, bzImage, bzImage.1, bzImage.orig, and c1.png. A 'Delete' button is located at the bottom right of the file list.

**Figure 4: Available Files**

## Un-mounting a Flash Device from the Controller

To un-mount a flash device from the controller:

- From the top menu, click **Controller**.
- From the left pane, click **Administration > Flash**.

The mounted flash memory space is displayed and the Available Files box displays any files located on the flash device.

- Click **Un-Mount**, and then click **OK** to confirm the flash device unmount.

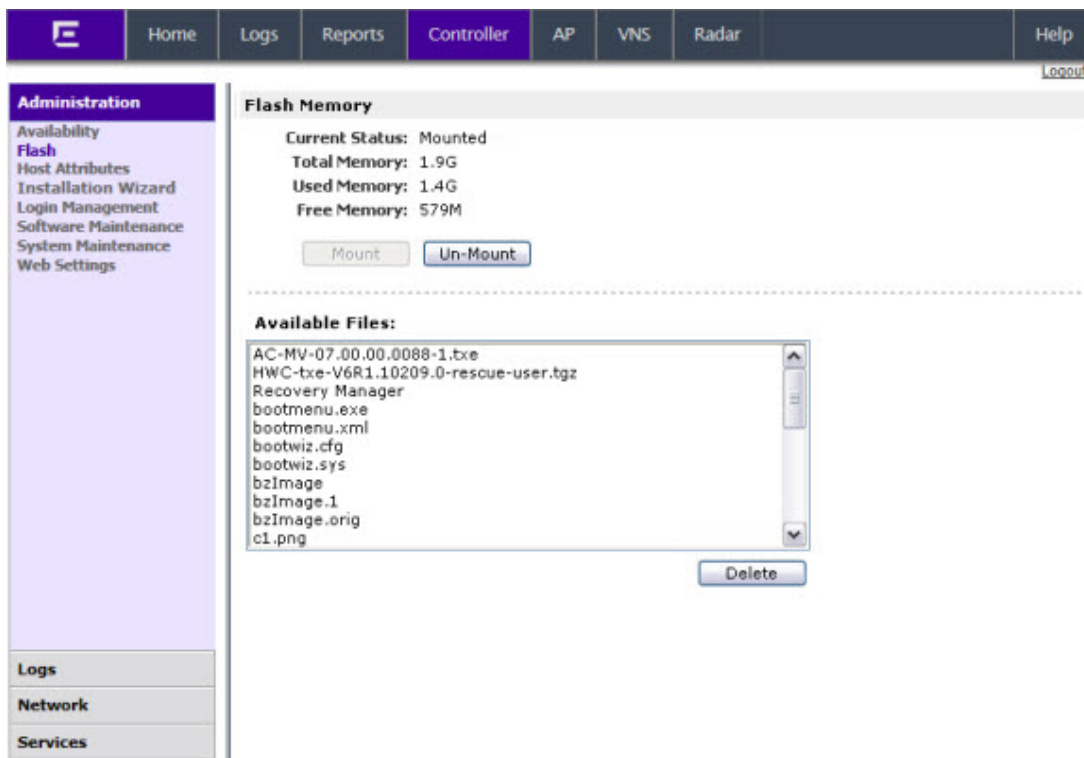
Once the un-mounting process is complete, the **Flash Memory** screen is refreshed and no longer displays any of the flash memory information. When you un-mount the flash device, the F icon in the footer changes from green to red.

## Deleting Files from a Flash Device

To delete files from a flash device:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration** > **Flash**.

The **Flash Memory** screen is displayed. The mounted flash memory space is displayed and the **Available Files** box displays any files located on the flash device.



**Figure 5: Deleting Files**

- 3 In the **Available Files** box, click the file you want to delete, and then click **Delete**.
- 4 To confirm the file deletion from the flash device, click **OK**. The file is deleted.

# 6 Using the Console Port

---

Using the Console Port in the Wireless Controller Models C25, C35, C4110, C5110, and C5210

Using the Console Port for the V2110

## Using the Console Port in the Wireless Controller Models C25, C35, C4110, C5110, and C5210

---

### Entering Rescue Mode on the Wireless Controller C25, C4110, and C5110

To get into Rescue mode, you must connect your laptop to the controller's RS232 serial console port via the Null Modem DB9 F- F (Female to Female) cable.

The serial port settings on the laptop should be the following:

- Speed — 115200
- Databits — 8
- Parity — None
- Stop Bits — 1
- Flow Control — None

If your laptop has a USB port instead of a serial port, you must use the USB 2.0 To RS232 Serial Adapter to connect the Null Model DB9 F-F cable to the laptop.

### Entering Rescue Mode on the Wireless Controller C35, and C5210

To get into Rescue mode, you must connect your laptop to the controller's console port using a Serial RJ45 to DB9 Female cable. For more information on the location of the console port for the C5210, see [Maintaining the C5210 Controller](#) on page 95. For more information on the location of the console port for the C35, see [Maintaining the C35 Controller](#) on page 86.

## Using the Console Port for the V2110

---

To get into Rescue mode in the V2110 Virtual Wireless Appliance, you must connect your laptop to the VMware server's serial port via the Null Modem DB9 F- F (Female to Female) cable.

The serial port settings on the laptop should be the following:

- Speed — 115200
- Databits — 8

- Parity — None
- Stop Bits — 1
- Flow Control — None



# 7 Performing System Maintenance

---

Changing Log Levels, Syslog Event Reporting, and AP Log Management  
Enabling or Disabling the Poll Timer  
Shutting Down the System  
Resetting Your System Configuration  
Resetting Wireless APs to Factory Default Settings  
Replacing the CMOS Battery

---

## Note



Syslog event reporting uses the syslog protocol to relay event messages to a centralized event server on your enterprise network. In the protocol a device generates messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

---

## Changing Log Levels, Syslog Event Reporting, and AP Log Management

---

This section provides procedural information related to log management and event reporting.

## Changing Log Levels

- 1 From the top menu, click **Controller**. From the left pane, click **Logs**. The **Logs Configuration** screen is displayed.

The screenshot shows the 'Logs Configuration' interface. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar has 'Administration' (with 'Logs' selected), 'Network', and 'Services'. The main content area is titled 'Logs Configuration' and is divided into two sections: 'System Log Level' and 'Syslog'. In the 'System Log Level' section, 'Wireless Controller Log Level' and 'Wireless AP Log Level' are both set to 'Information'. Three checkboxes are checked: 'Report station events on controller', 'Send station session events to NetSight', and 'Forward station session events as traps'. The 'Syslog' section has three 'Syslog Server IP' entries, each with a 'Port#' of 514. The first entry is '192.168.14.9'. There are also checkboxes for 'Include all service messages', 'Include audit messages', and 'Include station event messages' (checked). Under 'Facilities', there are four dropdown menus: 'Application Logs' (local.0), 'Service Logs' (local.3), 'Audit Logs' (local.6), and 'Station Logs' (local.1). An 'Apply' button is located at the bottom right of the configuration area.

### Note



Syslog event reporting uses the syslog protocol to relay event messages to a centralized event server on your enterprise network. In the protocol a device generates messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

### Note



The log statements **Low water mark level was reached** and **Incoming message dropped, because of the rate limiting mechanism** indicate that there is a burst of log messages coming to the event server and the processing speed is slower than the incoming rate of log messages. These messages do not indicate that the system is impaired in any way.

- 2 In the **System Log Level** section:
  - From the **Wireless Controller Log Level** drop-down list, select the least severe log level for the controller that you want to receive: Information, Minor, Major, Critical.  
  
For example, if you select **Minor**, you receive all Minor, Major and Critical messages. If you select **Major** you receive all Major and Critical messages. The default is Minor.
  - From the **Wireless AP Log Level** drop-down list, select the least severe log level for the AP that you want to receive: Information, Minor, Major, Critical.  
  
For example, if you select **Major** you receive all Major and Critical messages. The default is Major.
  - Click **Report station events on controller** to collect and display station session events on the controller station events log.
  - Click **Send station session events to NetSight** to forward station session events to NetSight for monitoring. Event information will not be sent to NetSight unless this checkbox is selected.
  - Click **Forward station session events as traps** to forward station events as SNMP traps.
- 3 Click **Apply**.

## Enabling and Defining Parameters for Syslog

To enable and define parameters for Syslog:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Logs**.
- 3 In the **Syslog** section, to enable the **Syslog** function for up to three syslog servers, select the appropriate checkboxes.
- 4 For each enabled syslog server, in the **IP** box, type a valid IP address for the server on the network. In the **Port #** box, the default port for syslog (514) is displayed.
- 5 To include all system messages, select the **Include all service messages** checkbox. If the box is not selected, only component messages (logs and traces) are relayed. This setting applies to all three servers. The additional service message is: **DHCP messages reporting users receiving IP addresses**.
- 6 To include audit messages, select the **Include audit messages** checkbox.
- 7 To include station session event messages, select the **Include station event messages** checkbox.
- 8 In the **Application Logs** drop-down list, click the log level (local.0 - local.6) to be sent to the syslog server. This setting applies to all three servers.
- 9 If the **Include all service messages** checkbox is selected, the **Service Logs** drop-down list becomes available. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies to all three servers.
- 10 If you select the **Include audit messages** checkbox, the **Audit Logs** drop-down list becomes available. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies to all three servers.
- 11 If you select the **Include station event messages** checkbox, the **Station Logs** drop-down list becomes available. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies to all three servers.

12 To apply your changes, click **Apply**.



#### Note

The syslog daemon must be running on both the controller and on the remote syslog server before the logs can be synchronized. If you change the log level on the controller, you must also modify the appropriate setting in the syslog configuration on remote syslog server.

**Table 9: Syslog and Controller Event Log Mapping**

| Syslog Event | Controller Event |
|--------------|------------------|
| LOG_CRIT     | Critical         |
| LOG_ERR      | Major            |
| LOG_WARNING  | Minor            |
| LOG_INFO     | Information      |

## Enabling AP Log Management

To enable AP Log Management:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Logs > AP Log Management > AP Log Collection**.

The screenshot shows the 'AP Log Collection' configuration page. The top navigation bar includes Home, Logs, Reports, Controller (selected), AP, VNS, Radar, and Help. The left sidebar shows Administration > Logs > AP Log Management > Logs Configuration. The main content area has a checked 'AP Log Collection' checkbox, a search bar, and a 'Select APs' dropdown menu. Below this is a table of wireless APs with columns for Name, Platform, and Home. The table lists five APs with their respective IDs and names. To the right of the table are configuration options for 'Times Per Day' (set to 1) and 'Destination' (set to Local).

| Wireless APs                              | Name                  | Platform | Home  |
|-------------------------------------------|-----------------------|----------|-------|
| <input type="checkbox"/> 111111111137152  | 3715e                 | AP3715   | Local |
| <input type="checkbox"/> 111111111138251  | 3825i                 | AP3825   | Local |
| <input type="checkbox"/> 11111111113935e  | 3935e                 | AP3935   | Local |
| <input type="checkbox"/> 11111111113935i  | 3935i                 | AP3935   | Local |
| <input type="checkbox"/> 13310619085D0000 | name-13310619085D0000 | AP3715   | Local |

- 3 To specify which APs will be included, do one of the following:
  - Search for a specific AP by entering the AP in the search bar and clicking (🔍).
  - For a specific AP, select the corresponding checkbox.
  - For APs by category, click one of the **Select APs** options:
    - “---” option - Selected APs will be cleared from the AP Logs search.
    - Local APs - Select active or inactive local configured APs.
    - Foreign APs - Select active or inactive foreign configured APs.
- 4 To clear your AP selections, click **Deselect All**.
- 5 To set the frequency of the collection, under **Times Per Day**, select 1 (default), 2, 4, or 6 times per day.
- 6 To set the destination of the AP logs, under **Destination**, select **Local**, **Flash**, or **Remote**.

- 7 Click **Save**.

## Copying AP Logs

- 1 From the **AP Log Management** dialog, click **Copy AP Logs** to transfer locally collected logs. The **Copy AP Logs** dialog is displayed.

**Copy AP Logs** ? X

Copy AP Logs to:  Remote  Flash

Protocol: FTP ▾

Server:

User ID:

Password:

Confirm:

Directory:

Copy Cancel

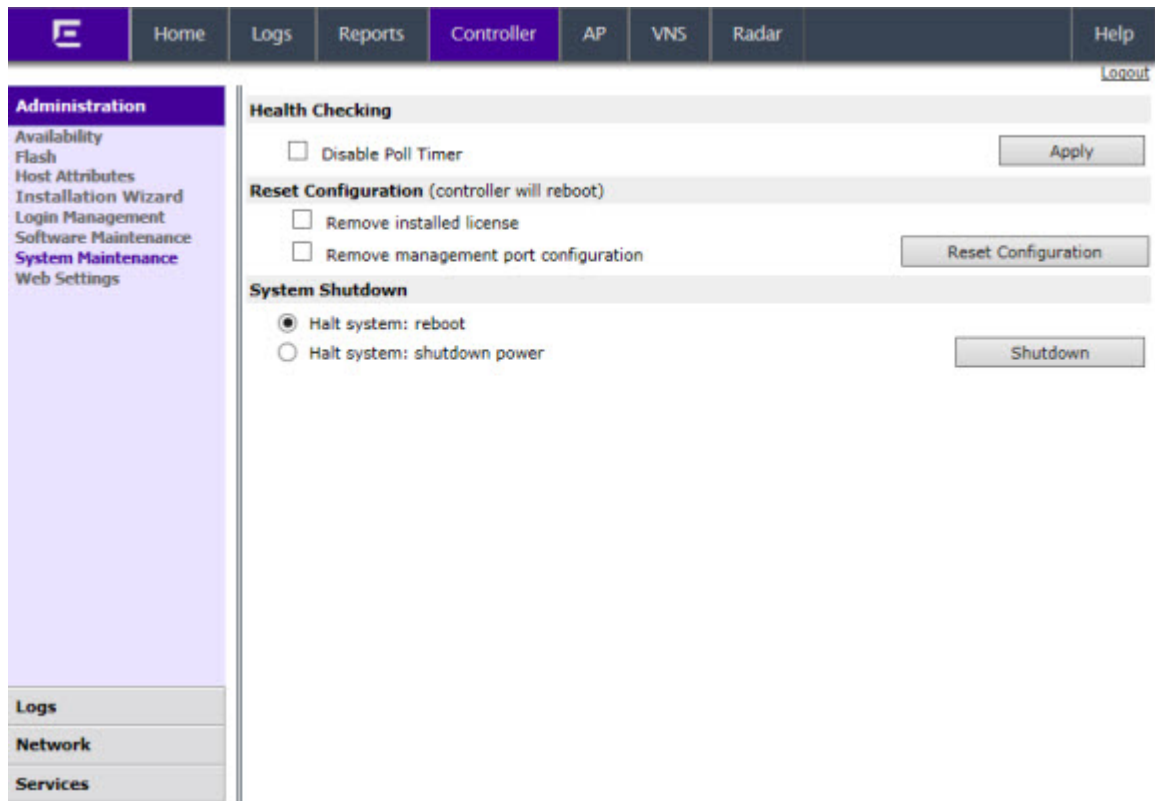
- 2 Set the location of the AP Logs by selecting either **Remote** or **Flash**. The Flash button is disabled when flash is not mounted.
- 3 When Remote is selected, do the following:
  - Under Protocol, select SCP or FTP to select the file transfer protocol you want to use to upload the AP Log file.
  - Under Server, type the IP address of the server where the AP Logs will be uploaded.
  - Under User ID, enter the user ID used to log into the server.
  - Under Password, enter the corresponding password for the user ID.
  - Under Confirm, enter the corresponding password for the user ID to confirm it was typed correctly.
  - Under Directory, enter the directory on the server where the AP Log file will be stored.
- 4 Click **Copy** to copy the logs.

## Enabling or Disabling the Poll Timer

To enable or disable the Poll Timer:

- 1 From the top menu, click **Controller**.

- From the left pane, click **Administration > System Maintenance**.



- Do one of the following:
  - To disable the poll timer, select the **Disable Poll Timer** checkbox in the **Health Checking** section.
  - To enable the poll timer, clear the **Disable Poll Timer** checkbox in the **Health Checking** section.
- Click **Apply**.

#### Related Links

[Resetting Your System Configuration](#) on page 63

[Shutting Down the System](#) on page 62

## Shutting Down the System

An alternative method of stopping the software operation is to use CLI commands. For more information, see the *CLI Reference Guide*.



#### Warning

Do not power off the controller by using the power switches only. Instead, carry out the entire procedure as described in this section. Failure to do so may corrupt the data on the hard disk drive.

To shut down the system:

- From the top menu, click **Controller**.
- From the left pane, click **Administration > System Maintenance**.

- 3 In the **System Shutdown** section, select the appropriate shut down option:
  - Halt system: reboot – The system shuts down, then reboots.
  - Halt system: Shutdown power – The system enters the halted state, which stops all functional services and the application. To restart the system, the power to the system must be reset.
- 4 To shut down the system including associated wireless APs, click **Shutdown**.  
A warning message is displayed, asking you to confirm your shutdown selection.
- 5 Click **Yes** to continue. Your system shuts down.

## Resetting Your System Configuration

To reset your system configuration:

- 1 From the top menu, click **Controller**.
- 2 From the left pane, click **Administration > System Maintenance**.
- 3 In the **Reset Configuration** section, select the appropriate configuration reset options:
  - Remove installed license – The system reboots and restores all aspects of the system configuration to the initial settings and the license key is removed. However, the Management IP address is preserved. This permits administrators to remain connected through the Management interface.
  - Remove management port configuration – The system reboots and resets the entire system configuration to the factory shipping state. The Management IP address reverts to 192.168.10.1.
- 4 Click **Reset Configuration**.
  - Depending on the configuration reset options you select, a warning message is displayed asking you to confirm your selection.



- If the Remove installed license option is selected, the warning message also displays the license activation key and optional features license keys.



### Warning

Copy the license key information displayed in the warning message in order to reuse these keys after the controller resets to its factory defaults.

- 5 The system reboots and the configuration is reset to its factory defaults.

## Resetting Wireless APs to Factory Default Settings

The AP boot-up sequence includes a random delay interval, followed by a vulnerable time interval. During the vulnerable time interval (2 seconds), the LEDs flash in a particular sequence to indicate that the controller is in the vulnerable time interval. For more information, see the *Wireless User Guide*.

If you power up the AP and interrupt the power during the vulnerable time interval three consecutive times, the next time the AP reboots, it will restore its factory defaults including the user password and the default IP settings.

**Caution**

The restoration of factory default settings does not erase the non-volatile log.

---

## Resetting APs to Factory Defaults

- 1 Switch off, and then switch on the wireless AP. The wireless AP reboots.
- 2 Switch off, and then switch on the wireless AP during the vulnerable time interval.

Refer to the wireless AP's LED pattern to determine the vulnerable period. For more information, see the *ExtremeWireless User Guide*.

- 3 Repeat Step 2 two more times.

When the wireless AP reboots for the fourth time, after having its power supply interrupted three consecutive times, it restores its factory default settings. The wireless AP then reboots again to put the default settings into effect.

Refer to the wireless AP's LED pattern to confirm that the wireless AP is set to its factory defaults. For more information, see the *ExtremeWireless User Guide*.

## Using the Reset Button (Hardware)

All wireless APs have a reset button, but they are located in different places on the AP chassis. Use it to reset the AP to its factory default settings by pressing and holding the reset button for at least six seconds.

**Note**

If you press the reset button and do not hold it longer than six seconds, the wireless AP simply reboots, and does not reset to its factory defaults.

---

The AP installation documentation is available at: <https://extranet.extremenetworks.com/downloads>

### *AP37xx Series Reset*

Figure 6 illustrates the location of the reset button on the WS-AP3705i.



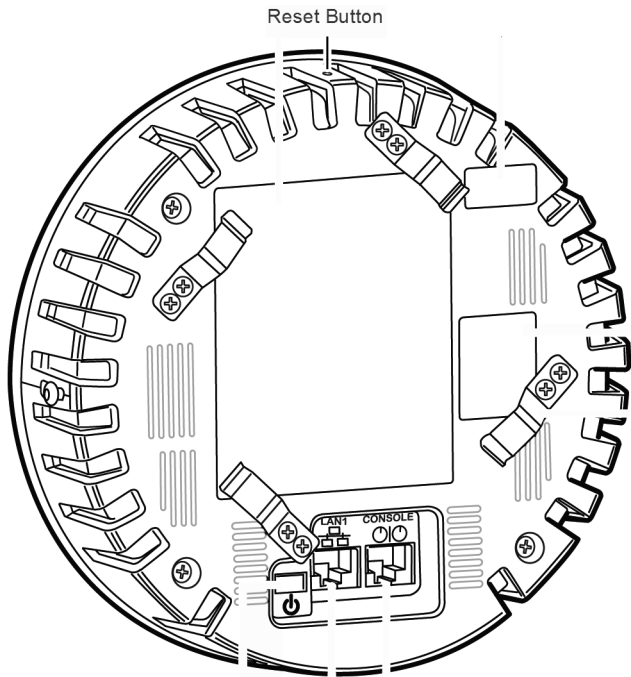
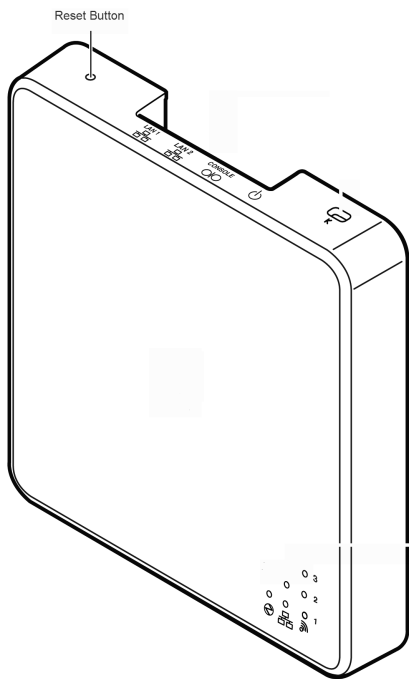


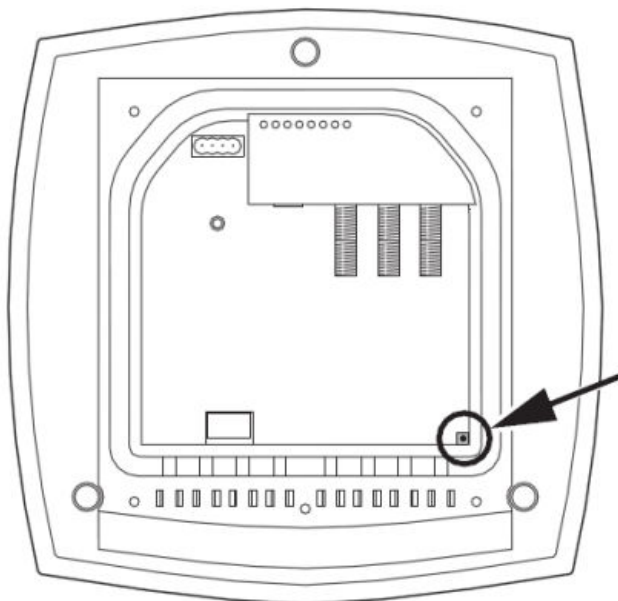
Figure 7 illustrates the location of the reset button on the WS-AP3710.

**Figure 6: Position of the Reset Button on the AP3705i (rear view)**



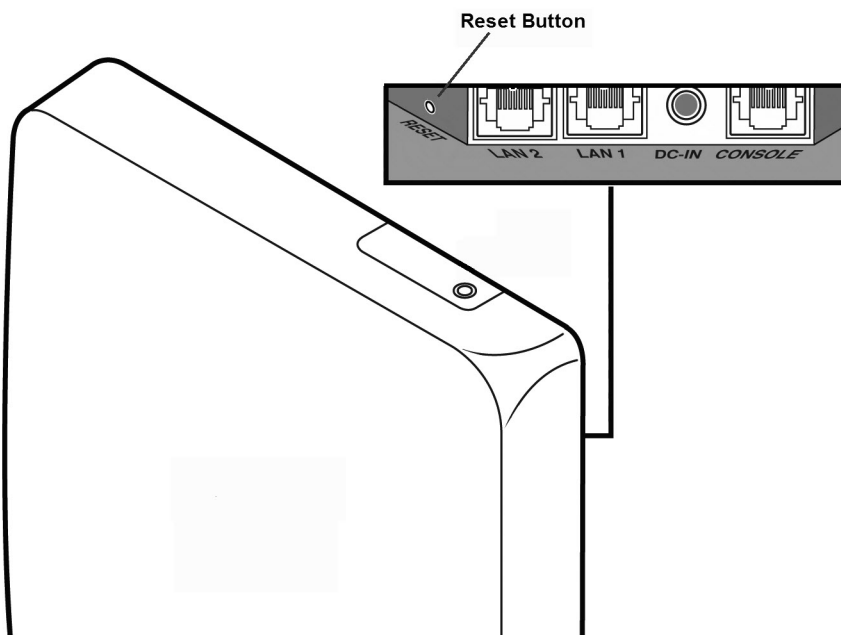
**Figure 7: Position of the Reset Button on the AP3710**

Figure 8 illustrates the location of the reset button on the WS-AP3765/3767.



**Figure 8: Position of the Reset Button on the AP3765/67 (rear view, with cover removed)**

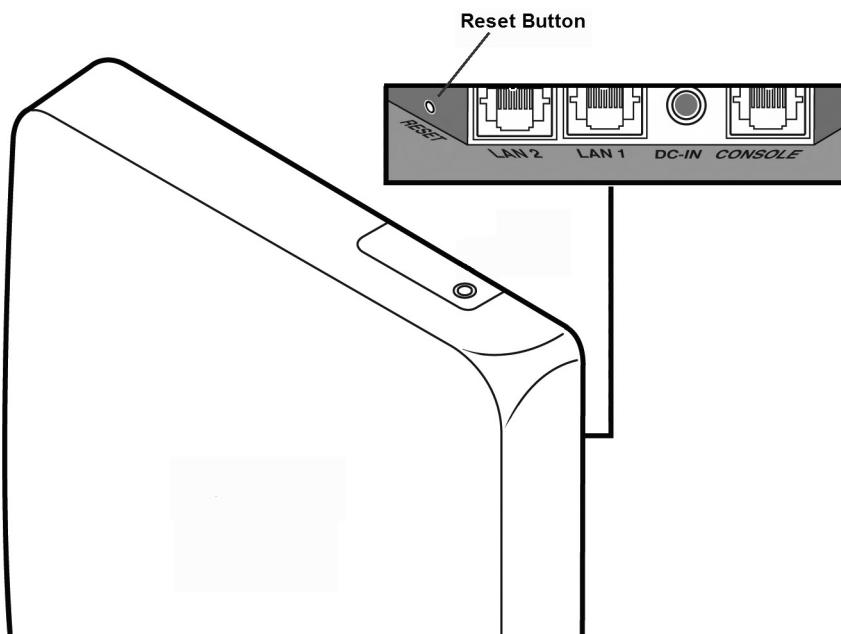
Figure 9 illustrates the location of the reset button on the WS-AP3715.



**Figure 9: Position of the Reset Button on the AP3715**

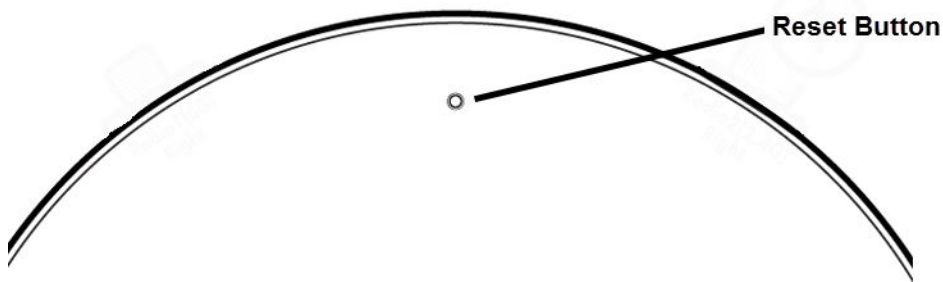
*AP38XX Series Reset*

Figure 10 illustrates the location of the reset button on the WS-AP3825i.



**Figure 10: Position of the Reset Button on the AP3825**

Figure 11 illustrates the location of the reset button on the WS-AP3805 and WSAP3801.

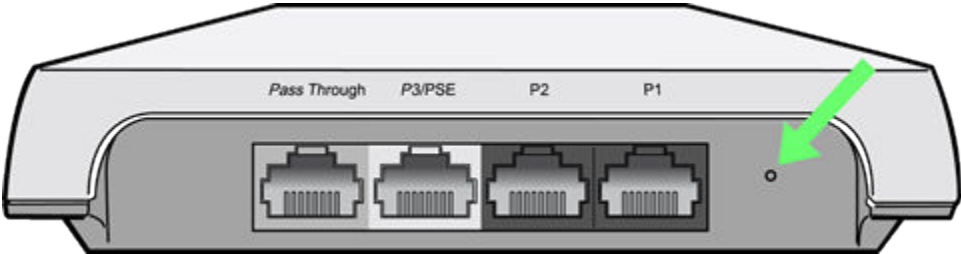


**Figure 11: Position of the Reset Button on the AP3805 and AP3801**

*AP39xx Series Reset*

**AP3912 Reset**

Figure 12 illustrates the reset button on the AP3912 access points.



**Figure 12: Position of the Reset Button on the AP3912**

**AP3935 Reset**

Figure 13 illustrates the reset button on the AP3935 access points.

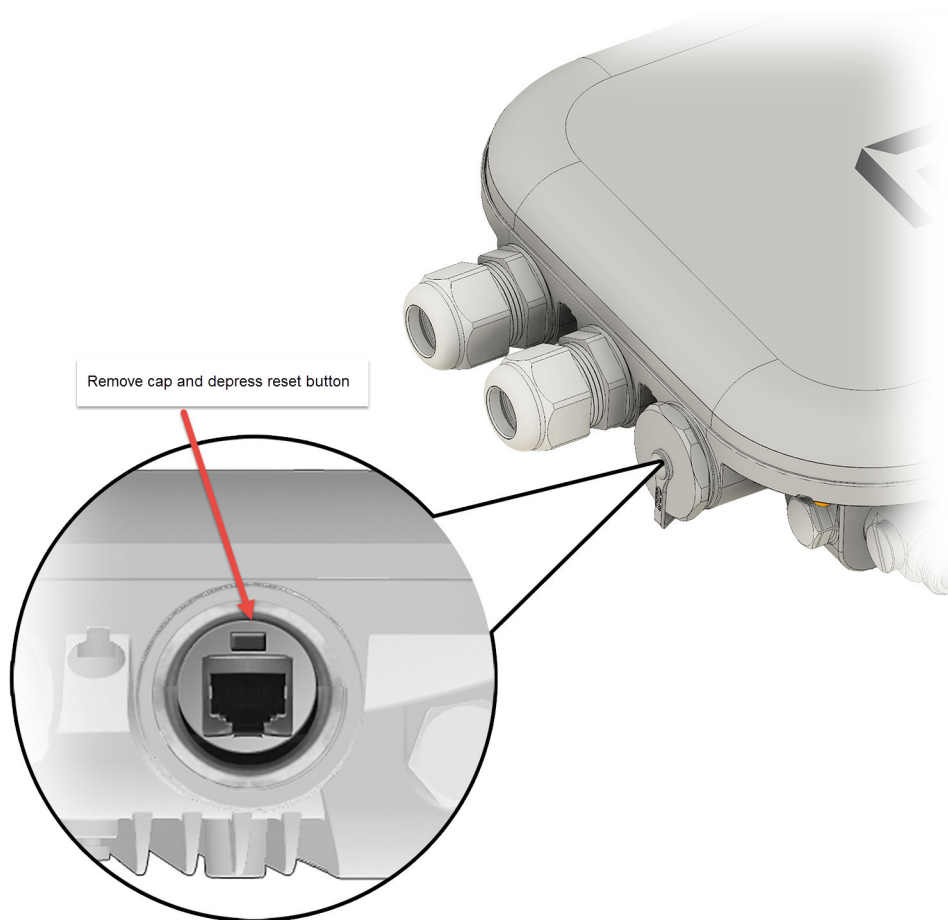


**Figure 13: Position of the Reset Button on the AP3935**

**AP3965 Reset**

Figure 14 illustrates the reset button on the AP3965 access points. Remove the console cap and use a non-corrosive probe to depress the black reset button.





**Figure 14: AP3965 Reset Button**

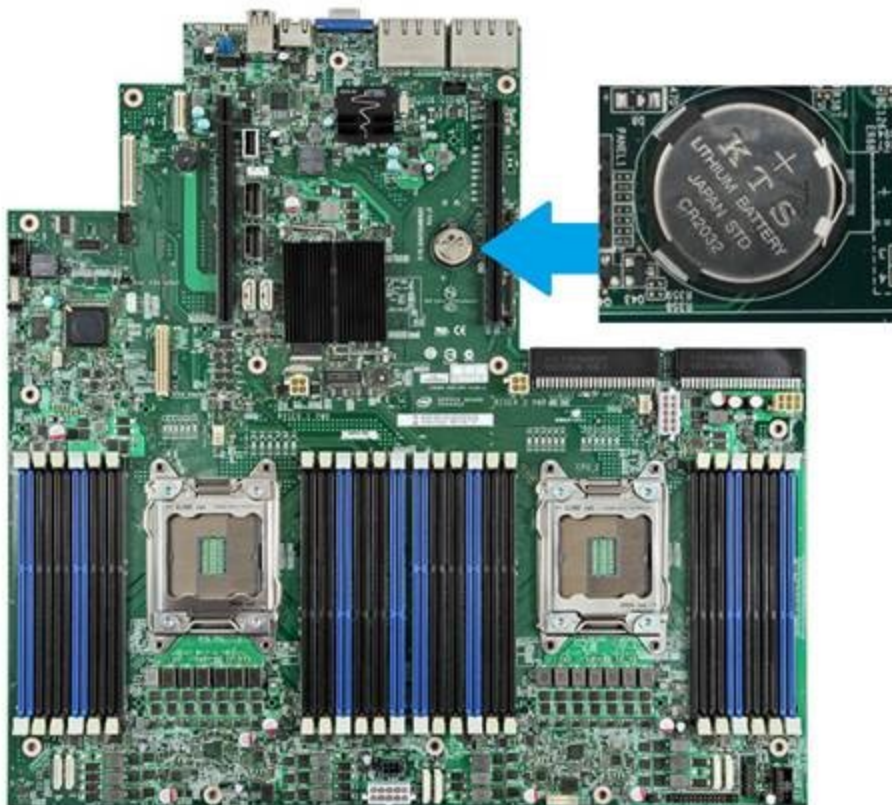
## Replacing the CMOS Battery



**Note**

This procedure applies to the wireless controller model C5210.

All wireless controllers contain a CMOS battery that retains BIOS information when the controller is powered off. The battery is located on the server board as shown in [the figure below](#). See [Table 10](#) for battery details.



**Figure 15: CMOS Battery Location**

**Table 10: Battery Details**

| Specification | Detail    |
|---------------|-----------|
| Part Number   | CR2032    |
| Battery Type  | Lithium   |
| Voltage       | 3.3 Volts |
| Diameter      | 20 mm     |
| Thickness     | 0.1 mm    |

## Removing the Discharged Battery

- 1 Power off the controller.
- 2 Remove the power cables attached to the controller.
- 3 Remove the controller cover.



### Warning

Make sure the controller is powered off and unplugged before removing the chassis cover.

- 4 Discharge the controller from static electricity by touching it with a metallic object and making sure all controller board LEDs are off.

- 5 Locate the battery as shown in [Figure 15](#) on page 70. The positive pole of the battery should be visible.
- 6 Gently press the spring clip to eject the battery from the socket.
- 7 Remove the battery.

## Installing the New Battery

- 1 Insert the new battery into the socket with the text on the battery facing up as shown in [Figure 15](#) on page 70.



### Note

Verify that the battery is placed correctly (firmly) in the slot location.

- 2 Replace the controller cover.
- 3 Install the power cable on the controller.
- 4 Power on the controller.

## Verifying BIOS Data and Resetting the Controller Clock

Once the operation complete, it is important to re-configure the BIOS settings on the controller.

- 1 Connect a PC to the controller.
- 2 Power up the controller and enter the BIOS by pressing **[F2]** during POST.
- 3 Modify the date and time as needed.
- 4 Press **[F9]** to load the Extreme Default settings
- 5 Press **[F10]** to Save and quit BIOS.

# 8 Using Controller Utilities

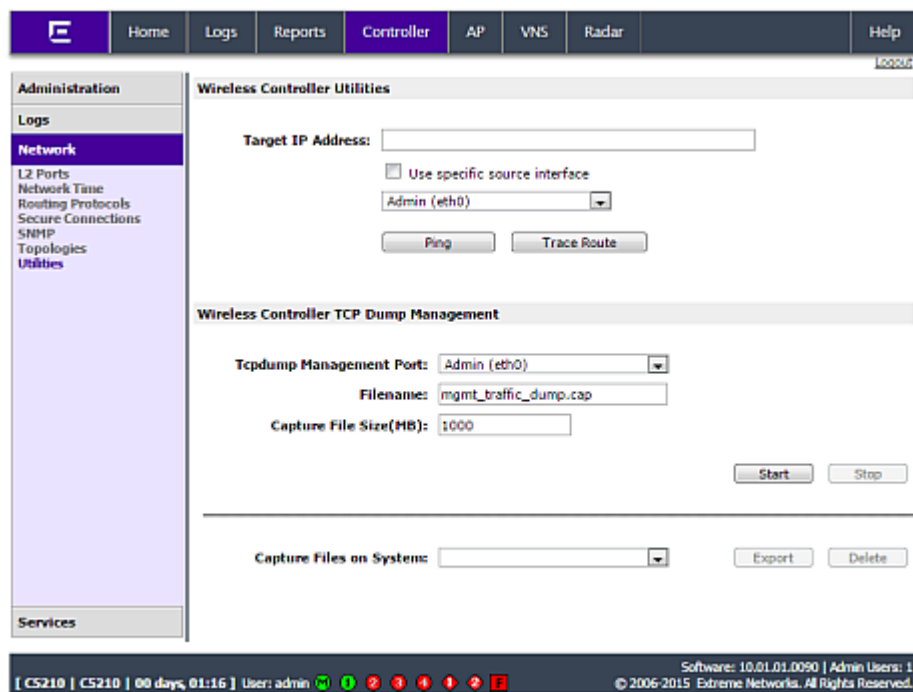
## Using Controller Utilities Enabling SNMP

### Using Controller Utilities

You can use wireless controller utilities to test a connection to the target IP address and record the route through the Internet between your computer and the target IP address. In addition, you can also use controller utilities to capture exception traffic, which can be useful for network administrators when debugging network problems.

To test or record IP address connections:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network > Utilities**.



**Figure 16: Wireless Controller Utilities Screen**

- 3 In the **Target IP Address** box, type the IP address of the destination computer.



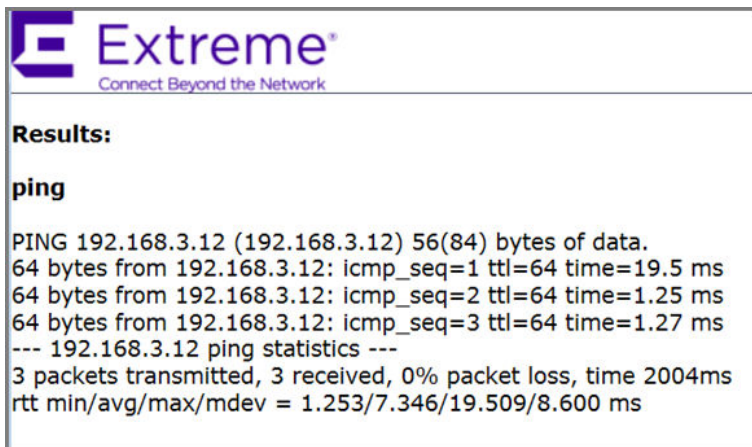
#### Note

The Target IP address supports both IPv4 and IPv6 addresses.



- 4 To test a connection to the target IP address, click **Ping**.

A window displays with the ping results. The following is an example:



```
Extreme®
Connect Beyond the Network

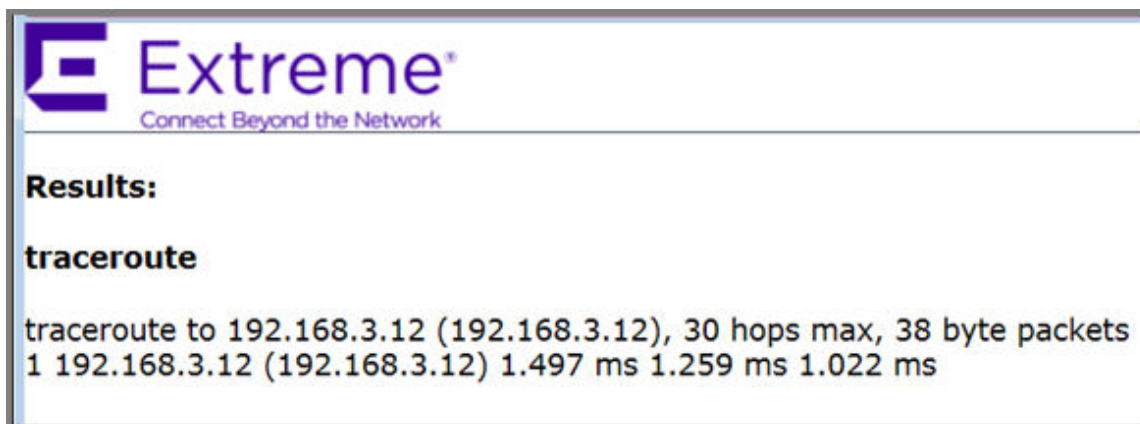
Results:

ping

PING 192.168.3.12 (192.168.3.12) 56(84) bytes of data.
64 bytes from 192.168.3.12: icmp_seq=1 ttl=64 time=19.5 ms
64 bytes from 192.168.3.12: icmp_seq=2 ttl=64 time=1.25 ms
64 bytes from 192.168.3.12: icmp_seq=3 ttl=64 time=1.27 ms
--- 192.168.3.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.253/7.346/19.509/8.600 ms
```

- To record the route through the Internet between your computer and the target IP address, click **Trace Route**.

The following is an example of trace results.



**Figure 17: Wireless Controller TCP Dump Management**

The wireless controller TCP dump management allows you to capture exception traffic that is sent to the management plane. Exception traffic is defined as traffic that is sent to the management plane from the data/control plane for special handling. For example, exception traffic can include DHCP, OSPF, and TFTP traffic.

When capturing exception traffic, you define the following:

- The physical or virtual VNS port on which the captured exception traffic travels
- The name and size of the captured traffic file
  - When naming the file, the file name extension must be .cap.
  - 10 MB is the minimum and 1 GB is the maximum size of the captured traffic file.
- The location where the captured TCP dump file is saved

The captured traffic file is stored in a binary tcpdump-format file on the controller or flash card. The captured traffic file can then be exported to a local machine for packet analysis and opened with a traffic analysis tool. For example, Wireshark.

The controller can only store one captured traffic file locally. Alternately, if you choose to save the captured traffic file on a flash card, the available space on the flash card will dictate how many captured traffic files you can save.

## Capturing Exception Traffic

- From the top menu, click **Controller**.
- In the left pane, click **Network > Utilities**.  
The **Wireless Controller Utilities** screen is displayed.
- In the **Tcpdump Management Port** drop-down list, click the port on which the exception traffic travels that you want to capture.
- In the **Filename** box, type the name for the captured traffic file. The default name is **mgmt\_traffic\_dump.cap**.

- 5 In the **Capture File Size (MB)** box, type the maximum size for the captured traffic file. 10 MB is the minimum and 1 GB is the maximum size of the captured traffic file.
- 6 If applicable, in the **Destination** drop-down list, select one of the following:
  - Flash – Click to save the file on the flash card.
  - Local – Click to save the file locally on the controller.

**Note**

The Destination drop-down list is only available if the controller has a mounted flash device. For more information, see [Working with an External Storage Device](#) on page 50.

- 7 Click **Start**. A dialog is displayed informing you the previously captured file will be removed.
- 8 To continue with the exception traffic capture, click **OK**. A dialog is displayed informing you the capture has started.

If applicable, to stop the capture before it is completed, click Stop.

To export an Exception Traffic Capture File:

- 9 From the top menu, click **Controller**.
- 10 In the left pane, click **Network > Utilities**.  
The **Wireless Controller Utilities** screen is displayed.
- 11 In the **Capture Files on System** drop-down list, click the capture file you want to export, and then click **Export**.  
A **File Download** dialog is displayed asking you where you want to save the file.
- 12 Click **Save**.
- 13 Navigate to the location on your network where you want to save the file, and then click **Save**.

## Enabling SNMP

The Wireless Controller, Access Points and Convergence Software system supports Simple Network Management Protocol (SNMP), Version 1 and 2c and Version 3.

**Note**

Due to the lack of a standard .11n MIB, the SNMP protocol does not provide full support for Wireless 802.11n AP attributes.

## MIB Support

The wireless controller software accepts SNMP get commands and generates Trap messages for the following set of MIBs:

- SNMPv2-MIB
- IF-MIB
- IEEE802dot11-MIB
- RFC1213-MIB

The Siemens Enterprise MIB includes:

- HIPATH-WIRELESS-EWC-MIB
- HIPATH-WIRELESS-PRODUCTS-MIB
- HIPATH-WIRELESS-SMI.my
- HIPATH-WIRELESS-DOT11-EXTNS-MIB
- HIPATH-WIRELESS-BRANCH-OFFICE-MIB

The MIB is provided for compilation into an external NMS. No support has been provided for automatic device discovery by an external NMS.

The controller is the only point of SNMP access for the entire system. In effect, the controller proxies sets, gets, and alarms from the associated wireless APs.

### *NetSight Suite Integration*

The Wireless Controller, Access Points and Convergence Software system now support get and set for a number of proprietary MIBs that are listed below. By using the Netsight Suite and the following MIBs, you can configure the controller to create and manage policy, VNS, VLAN; backup and restore configurations.

- set support
  - EXTREME-CONFIGURATIONMANAGEMENT-MIB
  - EXTREME-RADIUS-ACCT-CLIENT-EXT-MIB ('set' supported for this MIB except scalar elements)
  - EXTREME-RADIUS-AUTH-CLIENT-MIB ('set' supported for this MIB except scalar elements)
  - EXTREME-POLICY-PROFILE-MIB (not all tables supported)
  - EXTREME-CLASS-OF-SERVICE-MIB (not all tables supported)
  - Q-BRIDGE-MIB (dot1qVlanStaticTable only)
- get support
  - BRIDGE-MIB (dot1dBasePortTable)

Use these MIBs to perform controller hardware and software resets, including backing up and restoring controller configurations via the NetSight Suite. SNMP must be enabled on the controller for NetSight Suite integration.

For more information on NetSight suite integration, see the *Wireless Software User Guide* and documentation.

## Enabling SNMPv1/v2c on the Wireless Controller

You can enable SNMPv1/v2c or SNMPv3 on the wireless controller to retrieve statistics and configuration information.

For information on editing or deleting SNMPv3 user accounts, see [Editing SNMPv3 User Accounts](#) on page 80 and [Deleting SNMPv3 User Accounts](#) on page 82.

To enable SNMPv1/v2c parameters:

- 1 From the top menu, click **Controller**.

- 2 In the left pane, click **Network > SNMP**.  
The **SNMP Common Settings** screen is displayed.

The screenshot shows the 'SNMP Common Settings' configuration page. The left navigation pane is expanded to 'Network > SNMP'. The main content area has a title bar 'SNMP Common Settings' and a 'Logout' link. Below the title bar, there are three radio buttons for 'Mode': 'No SNMP', 'SNMPv1/v2c' (which is selected), and 'SNMPv3'. Below the mode selection, there are several input fields: 'Contact Name' (Lucy), 'Location' (lab-422), 'SNMP Port' (162), 'Forward Traps' (Informational), and 'Publish AP as interface of controller' (Enabled). Below these fields, there are two tabs: 'SNMPv1/v2c' (selected) and 'SNMPv3'. Under the 'SNMPv1/v2c' tab, there are four input fields: 'Read Community Name' (public), 'Read/Write Community Name' (private), 'Manager A' (136.157.233.176), and 'Manager B' (192.168.3.100). A 'Save' button is located at the bottom right of the form.

- 3 To enable SNMP, select the **SNMPv1/v2c Mode** option.
- 4 Type the following information:
  - **Contact Name** – Specifies the name of the SNMP administrator.
  - **Location** – Specifies the location of the SNMP administration.
  - **SNMP Trap Port** – Specifies the destination port for SNMP traps. The industry standard is 162. If left blank, no traps are generated.
- 5 In the **Forward Traps** drop-down list, click the security level of the traps to be forwarded: **Informational**, **Minor**, **Major**, or **Critical**.
- 6 In the **Publish AP as interface of controller** drop-down list, click to enable or disable publishing the wireless AP and their interfaces as interfaces of the controller. By default this option is enabled.

When this option is enabled, all wireless APs and their interfaces are published as interfaces of the controller when you retrieve topology statistics and configuration information using SNMP.

Topology statistics and configuration information on wireless APs are retrievable using both proprietary and standard MIBs. The Publish AP as interface of controller option only affects information retrieved through standard MIBs, i.e. IF-MIB, RFC1213. All information that is retrieved through proprietary MIBs is not affected. If the Publish AP as interface of controller option is disabled, the wireless APs' interfaces are not considered interfaces of the controller.

For example, if the Publish AP as interface of controller option is disabled, querying the ifTable would return information on the controller physical interfaces, plus all VNSs that are configured on that controller. If enabled, querying the same table would return the above information, in addition to information on each wireless APs' interfaces.

- 7 In the **SNMP v1/v2c** section, type the following:
- **Read Community Name** – Specifies the community name password for users with read privileges.
  - **Read/Write Community Name** – Specifies the community name password for users with read and write privileges.
  - **Manager A** – Specifies the IP address of the server on the network where the SNMP traps are monitored.
  - **Manager B** – Specifies the IP address of a second server on the network where the SNMP traps are monitored.



#### Warning

For security purposes, it is recommended that you immediately change the Read Community Name (public) and the Read/Write Community Name (private) passwords to names that are less obvious and more secure.

- 8 To save your changes, click **Save**.

### Enabling SNMPv3

To enable SNMPv3 parameters:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network** > **SNMP**.

The **SNMP Common Settings** screen is displayed.

The screenshot shows the 'SNMP Common Settings' configuration page. The 'Mode' is set to 'SNMPv1/v2c'. The 'Contact Name' is 'John Doe', 'Location' is 'lab-765', and 'SNMP Port' is '162'. 'Forward Traps' is set to 'Informational' and 'Publish AP as interface of controller' is 'Enabled'. Below, the 'SNMPv3' tab is active, showing a table of user accounts. The table has columns for User Name, Security Level, Authentication Protocol, Privacy Protocol, and Account Enabled. One user is listed with Security Level 'authPriv', Authentication Protocol 'MD5', Privacy Protocol 'DES', and Account Enabled 'X'. There are buttons for 'Delete Selected User', 'Add User Account', and 'Edit Selected User'. At the bottom, there are two 'Trap' configuration sections, each with 'Destination IP' and 'User Name' fields. A 'Save' button is at the bottom right.

| User Name | Security Level | Authentication Protocol | Privacy Protocol | Account Enabled |
|-----------|----------------|-------------------------|------------------|-----------------|
|           | authPriv       | MD5                     | DES              | X               |

- 3 To enable SNMP, select the **SNMPv3 Mode** option.

- 4 Type the following information:
  - **Contact Name** – Specifies the name of the SNMP administrator.
  - **Location** – Specifies the location of the SNMP administration.
  - **SNMP Trap Port** – Specifies the destination port for SNMP traps. The industry standard is 162. If left blank, no traps are generated.
- 5 In the **Forward Traps** drop-down list, click the security level of the traps to be forwarded: **Informational**, **Minor**, **Major**, or **Critical**.
- 6 In the **Publish AP as interface of controller** drop-down list, click to enable or disable publishing the wireless AP and their interfaces as interfaces of the controller. By default this option is enabled.  
When this option is enabled, all wireless APs and their interfaces are published as interfaces of the controller when you retrieve topology statistics and configuration information using SNMP.

Topology statistics and configuration information on wireless APs are retrievable using both proprietary and standard MIBs. The Publish AP as interface of controller option only affects information retrieved through standard MIBs, i.e. IF-MIB, RFC1213. All information that is retrieved through proprietary MIBs is not affected. If the Publish AP as interface of controller option is disabled, the wireless APs' interfaces are not considered interfaces of the controller.

For example, if the Publish AP as interface of controller option is disabled, querying the ifTable would return information on the controller physical interfaces, plus all VNSs that are configured on that controller. If enabled, querying the same table would return the above information, in addition to information on each wireless APs' interfaces.

- 7 In the **SNMP v3** section, type the SNMP engine ID in **Engine ID**. The SNMP engine ID is a 5 - 32 character ID for the **EWC** SNMP agent. Do not use spaces, control characters, or tabs.

- 8 Add user accounts.
  - a Click **Add User Account**.  
The Add SNMPv3 User Account screen is displayed.

**Add SNMPv3 User Account**

Enabled:

User Name:

Security Level:

Authentication Protocol:

Authentication Password:

Privacy Protocol:

Privacy Password:

- b Select **Enabled** to enable the user.
  - c In User Name, type a user name.
  - d In the Security Level drop-down list, select the appropriate security level for the user: authPriv, authNoPriv, NoAuthNoPriv.  
If NoAuthNoPriv is selected, click **OK** and go to the next step.
  - e In the Authentication Protocol drop-down list, select the authentication protocol: None, MD5, SHA.
  - f In Authentication Password, type the password, which must be at least eight characters long. If desired, click Unmask to display the password in plain text.  
If authNoPriv is the selected security level, click **OK** and go to the next step.
  - g In the Privacy Protocol drop-down list, select the encryption protocol: None, DES.
  - h In Privacy Password, type the password, which must be at least eight characters long. If desired, click Unmask to display the password in plain text.
  - i Click **OK** to save the user account information. The **SNMP Common Settings** screen is displayed.
- 9 In **Trap 1 Destination IP** and **Trap 2 Destination IP**, type the IP addresses of the servers on the network where the SNMP traps are monitored.
- 10 In the **Trap 1 User Name** and **Trap 2 User Name** drop-down lists, select the user name associated with the Trap 1 and Trap 2 destination servers. Only enabled users appear in these drop-down lists.
- 11 To save your changes, click **Save**.

### *Editing SNMPv3 User Accounts*

To edit SNMPv3 user accounts:

- 1 From the top menu, click **Controller**.



- In the left pane, click **Network > SNMP**.  
The **SNMP Common Settings** screen is displayed.

The screenshot shows the 'SNMP Common Settings' configuration page. The left navigation pane is expanded to 'Network > SNMP'. The main content area includes the following fields and sections:

- Mode:** Radio buttons for 'No SNMP', 'SNMPv1/v2c' (selected), and 'SNMPv3'.
- Contact Name:** Text input field containing 'John Doe'.
- Location:** Text input field containing 'lab-765'.
- SNMP Port:** Text input field containing '162'.
- Forward Traps:** Dropdown menu set to 'Informational'.
- Publish AP as interface of controller:** Dropdown menu set to 'Enabled'.
- SNMPv1/v2c / SNMPv3:** Two tabs, with 'SNMPv3' currently selected.
- Context String:** Text input field.
- Engine ID:** Text input field containing 'controller\_000C29C2C71A'.
- RFC3411 Compliant:** Checked checkbox.
- User Accounts Table:**

| User Name | Security Level | Authentication Protocol | Privacy Protocol | Account Enabled |
|-----------|----------------|-------------------------|------------------|-----------------|
|           | authPriv       | MD5                     | DES              | X               |
- Buttons:** 'Delete Selected User', 'Add User Account', and 'Edit Selected User'.
- Trap Configuration:** Two sections for 'Trap 1' and 'Trap 2', each with 'Destination IP' and 'User Name' input fields.
- Save:** A 'Save' button at the bottom right.

- In the **SNMP v3** section, select a user account.
- Click **Edit Selected User**.  
The **Edit SNMPv3 User Account** screen is displayed.

The 'Edit SNMPv3 User Account' dialog box contains the following configuration options:

- Enabled:** Unchecked checkbox.
- User Name:** Text input field containing 'User1'.
- Security Level:** Dropdown menu set to 'authPriv'.
- Authentication Protocol:** Dropdown menu set to 'MD5'.
- Authentication Password:** Masked text input field with an 'Unmask' button.
- Privacy Protocol:** Dropdown menu set to 'DES'.
- Privacy Password:** Masked text input field with an 'Unmask' button.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

You can change the setting of the Authentication Protocol, Authentication Password, Privacy Protocol, and Privacy Password, depending upon how the user account's security level is set.

- In the **Authentication Protocol** drop-down list, select the authentication protocol: **MD5, SHA**.
- In **Authentication Password**, type the password, which must be at least eight characters long. If desired, click **Unmask** to display the password in plain text.

- 7 In the **Privacy Protocol** drop-down list, select the encryption protocol: **DES**.
- 8 In **Privacy Password**, type the password, which must be at least eight characters long. If desired, click **Unmask** to display the password in plain text.
- 9 Click **OK** to save the user account information.
- 10 To save your changes, click **Save**.

### *Deleting SNMPv3 User Accounts*

To delete SNMPv3 user accounts:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network > SNMP**.
- 3 In the **SNMP v3** section, select a user account.
- 4 Click **Delete Selected User**.

A warning is displayed.



- 5 Click **OK** to delete the user account.
- 6 To save your changes, click **Save**.

# 9 Recovering the Wireless Controller

## Rescue Mode Authentication Service Management Menu Recovering the Wireless Controller from File System Corruption

### Rescue Mode Authentication Service Management Menu

Use Rescue mode's Authentication Service Management menu to do the following on the wireless controller:

- Set login mode to local
- Reset accounts and passwords to factory default
- Change administrator password

To use Rescue Mode's Authentication Service Management menu:

- 1 Connect to the console port. Do not use the ESA ports or the Admin management port. For more information, see [Using the Console Port](#) on page 55.

- 2 Reboot the system.

The following menu appears during the reboot process.

```

Controller
Controller Rescue

```

- 3 Select the **Rescue Mode**, and then press **[Enter]**.

The **Rescue Start-up Menu** appears.

Rescue Start-up Menu. Use with extreme caution.

- ```
1) Force System Recovery  
2) Create System Backup Image  
3) Display Backup Images  
4) FTP Menu  
5) Network Interface Menu  
6) Manually run File System Check Utility (fsck)  
7) Restore Backup Image directly from the FTP server  
8) Authentication Service Management Menu  
9) Flash Menu  
R) Reboot
```

WARNING! - Forcing system recovery will erase all files, and reinstall the selected image (either backup or factory).

Reboot will restart the system back into Normal mode.

If you have any questions about these options, please contact Support.

Your choice:

- 4 Type 8.

The **Authentication Service Management** menu displays.

```
Authentication Service Management Menu  
=====
```

```
1) Set Login Mode to Local  
2) Reset Accounts and Passwords to Factory Default  
3) Change administrator password  
B) Return back to main menu  
Please enter your choice:
```

- 5 Type the sequence number of the appropriate option, given in the **Authentication Service Management** menu.
 - Set Login Mode to Local – Type 1 if the login authentication mode was set to RADIUS-based authentication, and you want to revert to the local login authentication mode.
 - Reset Accounts and Passwords to Factory Default – Type 2 if you want to reset the login accounts and password to factory defaults.
 - Change administrator password – Type 3 if you want to change the administrator’s password.
 - Return back to main menu – Type B if you want to return to the main menu.
- 6 After you have used any of the first three options in the **Authentication Service Management** menu, type B to return to the main menu.

Rescue Start-up Menu. Use with extreme caution.

- 1) Force System Recovery
- 2) Create System Backup Image
- 3) Display Backup Images
- 4) FTP Menu
- 5) Network Interface Menu
- 6) Manually run File System Check Utility (fsck)
- 7) Restore Backup Image directly from the FTP server
- 8) Authentication Service Management Menu
- 9) Flash Menu
- R) Reboot

WARNING! - Forcing system recovery will erase all files, and reinstall the selected image (either backup or factory).

Reboot will restart the system back into Normal mode.

- 7 Type R. The system restarts into normal mode.

Recovering the Wireless Controller from File System Corruption

A power outage can, in rare cases cause file system corruption to the wireless controller. If file system corruption occurs, the controller might not be able to start up and provide service. This section describes how to recover the controller in such a situation.

To recover the controller from file system corruption:

- 1 Connect to the console port. Do not use the ESA ports or the Admin port. For more information, see [Using the Console Port](#) on page 55.
- 2 Monitor the console output of the system startup. In case there are file system corruptions, you will see similar output containing unexpected file system inconsistency with a request for the manual actions.

```
INIT: version 2.86 booting
Starting the hotplug events dispatcher: udevd.
Synthesizing the initial hotplug events...done.
Waiting for /dev to be fully populated...done.
Mounting readonly root filesystem...done.
Checking root file system...fsck 1.40 (29-Jun-2007)
/dev/hda2 has gone 14817 days without being checked, check forced.
Inodes that were part of a corrupted orphan linked list found.
/dev/hda2: UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY.(i.e., without -a or -p options)
fsck failed (exit code 4). Please repair manually and reboot.
Please note that the root file system is currently mounted read-only.
To remount it read-write:
# mount -n -o remount,rw /
CONTROL-D will exit from this shell and REBOOT the system.
Give root password for maintenance
(or type Control-D to continue):
```

- 3 Type the main admin password to log into the wireless controller.
The command prompt displays.
- 4 Use the `fsck.ext3` command to recover the file system partition, where `/dev/hda2` is a problematic partition name from the output above.

```
bash-3.00# fsck.ext3 -fyv /dev/hda2
```

- 5 After the recovery completes, use the `reboot` command to reboot the system.

```
e2fsck 1.40 (29-Jun-2007)
Checking for bad blocks (read-only test): done
Pass 1: Checking inodes, blocks, and sizes
Inodes that were part of a corrupted orphan linked list found. Fix? yes
Inode 17765 was part of the orphaned inode list. FIXED.
Inode 17786 was part of the orphaned inode list. FIXED.
Inode 64432 was part of the orphaned inode list. FIXED.
Inode 64433 was part of the orphaned inode list. FIXED.
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/hda2: ***** FILE SYSTEM WAS MODIFIED *****
/dev/hda2: ***** REBOOT LINUX *****
12087 inodes used (15.61%)
83 non-contiguous inodes (0.7%)
# of inodes with ind/dind/tind blocks: 636/5/0
83316 blocks used (53.88%)
0 bad blocks
0 large files
10967 regular files
742 directories
2 character device files
0 block device files
6 fifos
1418 links
359 symbolic links (359 fast symbolic links)
2 sockets
-----
13496 files
bash-3.00# reboot
```

Following the reboot, the wireless controller should proceed with the normal startup.

10 Maintaining the Wireless Controller

- Maintaining the C35 Controller
- Maintaining the C25 Controller
- Maintaining the C5110 Controller
- Maintaining the C5210 Controller
- Maintaining the C4110 Controller

Maintaining the C35 Controller

This topic outlines the features of the C35 controller.

Related Links

- [C35 Front Panel Features](#) on page 86
- [C35 Back Panel Features](#) on page 87

C35 Front Panel Features

The figure below depicts the chassis front panel of the C35. [C35 System Status LEDs](#) describes the C35 system status LED functions.

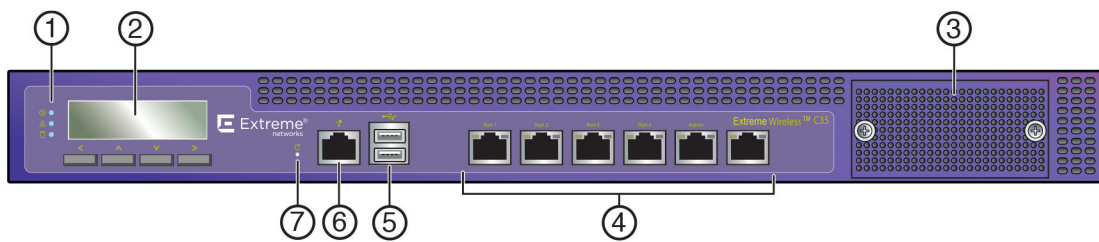


Figure 18: C35 Front Panel Features

1	System Status LEDs	5	USB Port
2	LCD Panel	6	Console Port
3	Not Used	7	Reset Switch
4	Ethernet Ports (see Figure 19)		

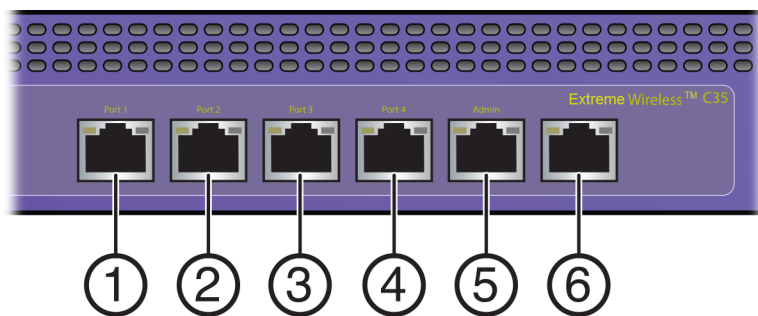


Figure 19: C35 Ethernet Ports

1	Data Port 1: 1GbE (esa0)	4	Data Port 4: 1GbE (esa3)
2	Data Port 2: 1GbE (esa1)	5	Mgmt Port: 1GbE (eth0)
3	Data Port 3: 1GbE (esa2)	6	Not used, plugged

Table 11: C35 System Status LEDs

LED	Function
	Power: When this LED is on, it indicates power is supplied to the WS-C35 power supply unit. This LED should be illuminated when the system is operating
	Status: When lit Green, it indicates operational state is normal. When lit Red, it indicates a system malfunction.
	Hardisk (HDD): When this LED flashes, it indicates hard drive activity. Otherwise, the LED remains off.

C35 Back Panel Features

The following figure depicts the C35 back panel. [C35 Management and Data Port LEDs](#) describes the management and data port LED functions.

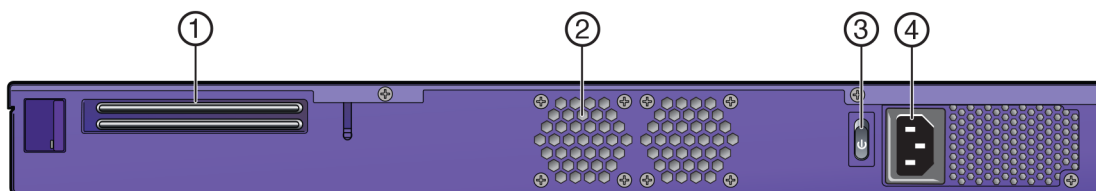


Figure 20: C35 Back Panel Features

1	Not Used	3	Power Switch
2	CPU-Fan	4	AC Power Socket

Table 12: C35 Management and Data Port LEDs

Port	LED	Function
Management	Network speed	Off = 10Mbps
		Green = 100Mbps
		Amber = 1000Mbps
Management	Activity/Link	Off = No Link
		Green = Active Link
		Blinking Amber = Network Activity

Maintaining the C25 Controller

This topic outlines the features of the C25 controller.

Related Links

[C25 Front Panel Features](#) on page 88

[C25 Back Panel Features](#) on page 89

C25 Front Panel Features

The figure below depicts the chassis front panel of the C25. Table 13 on page 89 describes the C25 system status LED functions.

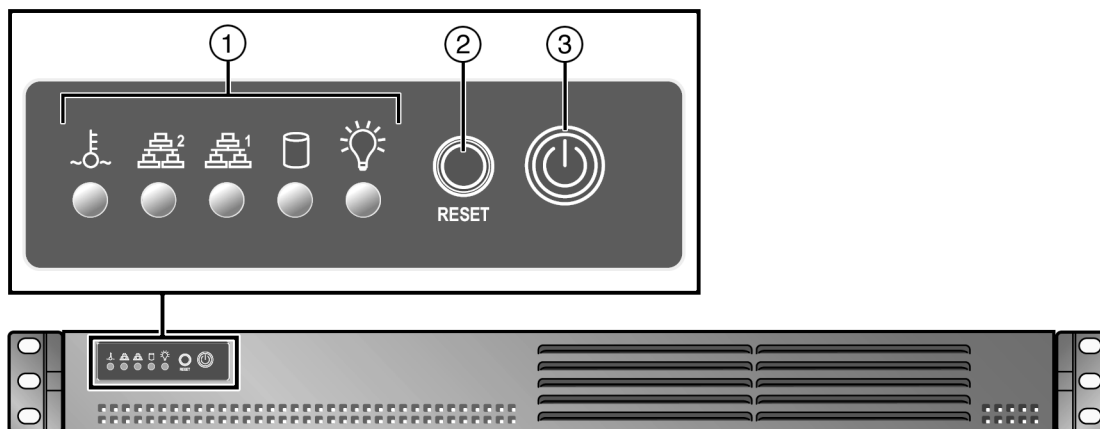






Figure 21: C25 Front Panel Features

1	System Status LEDs	3	Power button
2	Reset button		

Table 13: C25 System Status LEDs

LED	Function
	Overheat/Fan Fail: When this LED flashes it indicates a fan failure. When continuously on, it indicates an overheat condition.
	Gb1 & Gb2 (Data ports): When these LEDs flash, they indicate network activity on Gb1 and Gb2.
	Hardisk: When this LED flashes, it indicates hard drive activity.
	Power: When this LED is on, it indicates power is supplied to the C25 power supply unit. This LED should be illuminated when the system is operating.

C25 Back Panel Features

The following table depicts the C25 back panel. Table 14 on page 89 describes the management and data port LED functions.

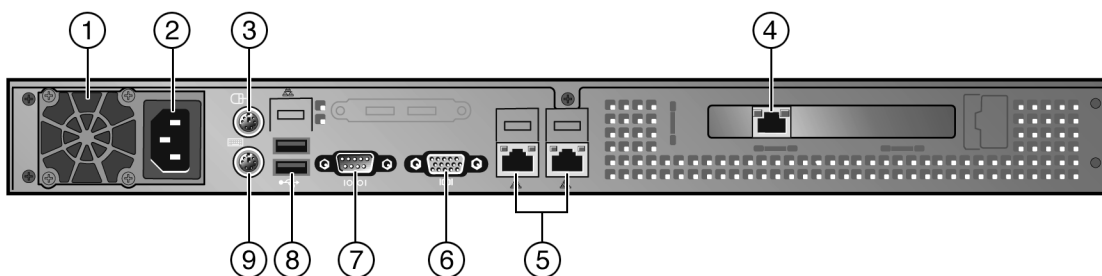


Figure 22: C25 Back Panel Features

1	AC fan	6	VGA connector (not used)
2	AC Power supply	7	Serial connector (console port)
3	Mouse connector (not used)	8	USB connector (2 x USB 2.0)
4	Management port (1 x GbE)	9	Keyboard connector (not used)
5	Data port (2 x 1GbE), RJ45		

Table 14: C25 Management and Data Port LEDs

Port	LED	Function
Management	(left) Network speed	Off = 10Mbps
		Green = 100Mbps
		Yellow = 1000Mbps

Table 14: C25 Management and Data Port LEDs (continued)

Port	LED	Function
Management	(right) Activity/Link	Off = No Link
		Green = Active Link
		Blinking Green = Network Activity
Data	(left) Network speed	Off = No connection or 10Mbps
		Green = 100Mbps
		Amber = 1000Mbps
Data	(right) Activity/Link	Off = 10Mbps
		Yellow = Active Link
		Blinking Yellow = Data Traffic

Maintaining the C5110 Controller

This topic outlines the features of the C5110 controller.

Related Links

- [C5110 Front Panel Features](#) on page 90
- [C5110 Back Panel Features](#) on page 91
- [Opening and Closing the C5110](#) on page 94
- [Attaching the Front Bezel](#) on page 93
- [Inside the System](#) on page 92

C5110 Front Panel Features

The following figure depicts the front panel of the C5110. Table 15 depicts the features and functions of the C5110 front panel.



Figure 23: C5110 Front Panel Features

Table 15: C5110 Front Panel Features

Callout	Feature	Function
1	Power-on indicator	The power button controls the DC power supply output to the system.
2	NMI button	Not used in the current release.
3	System Identification button	The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of the buttons is pushed, the blue system status indicator on the front and back blinks until one of the buttons is pushed again.
4	LCD display	Provides system ID, status information and system error messages. The LCD display lights during normal system operation. Both the systems management software and the identification buttons located on the front and back of the system can cause the LCD to flash blue to identify a particular system. The LCD display lights amber when the system needs attention due to a problem with power supplies, fans, system temperature or hard drives. Note: : If the system is connected to AC power and an error has been detected, the LCD display amber lights regardless of whether the system has been powered on.
5	USB connectors	Connects USB 2.0-compliant devices to the system. For more information, see the Note below.
6	Video connector	Not used in the current release.
7	Hard drive	One 3.5 inch SATA 250 GB drives.
8	Optical drive	Not used in the current release.

Note



The C5110 is equipped with four USB connectors — two on each front and back panel. However, the controller is capable of supporting only one USB device at a time, regardless of what USB connector the device is connected to. If you connect a second USB device while the first is already connected, the system will return an error.

C5110 Back Panel Features

The following figure displays back panel features of the C5110. Table 16 depicts the features and functions of the C5110 back panel.

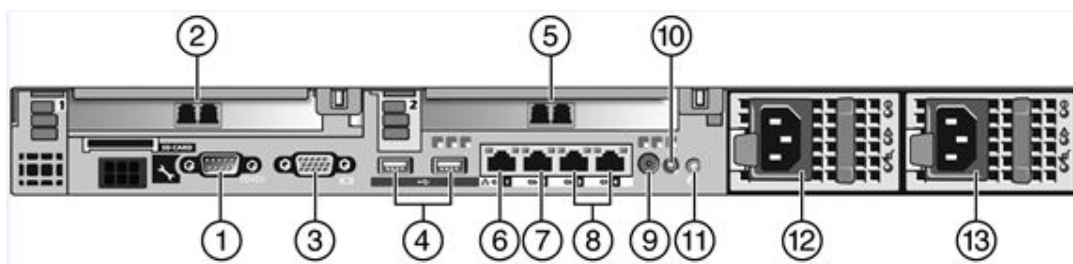


Figure 24: C5110 Back Panel Features

Table 16: C5110 Back Panel Features

Callout	Feature	Function
1	Serial port connector	Console Port – Used to get into Rescue mode.
2	PCIe1 fiber optic connector	Data port – esa1
3	Video connector	Not used in the current release
4	USB connector (2)	Connects USB 2.0-compliant devices to the system. For more information, see the Note below.
5	PCIe2 fiber optic connector	Data port – esa2
6	NIC1 connector	Management port – eth0
7	NIC2 connector	Data port – esa0
8	Remote Access Controller	Not used in the current release.
9	System status indicator connector	Not used in the current release.
10	System status indicator	The blue-colored system status indicator blinks to indicate the location of a particular system within a rack. The indicator continues to blink until one of the system identification button is pushed again.
11	System identification button	The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pushed, the blue system status indicator on the front and back blinks until one of the buttons is pushed again.
12	AC Power Supply 1	AC Power Supply 1 and 2 combine to make a redundant power supply.
13	AC Power Supply 2	

Note

The PCIe and PCIe2 ports are fiber optic ports. If your infrastructure does not allow the fiber optic connection, you must get a Gigabit Media Converter to convert the fiber optic connection to a copper Gigabit connection. For example, use a converter that receives the fiber optic connection and outputs traffic via the RJ45 copper port (Unshielded Twister Pair – UTP).

Inside the System

In [the figure below](#), the bezel, system cover, and memory cooling shroud are removed to provide an interior view of the system.

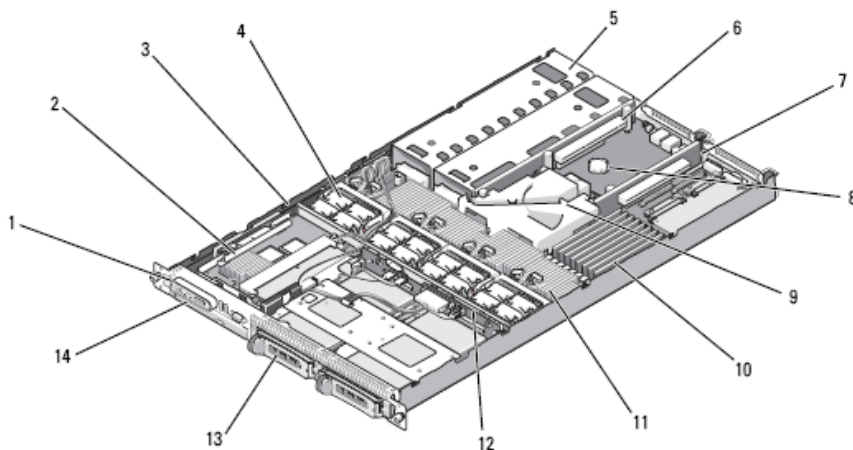


Figure 25: Internal Components of the C5110

1	Control Panel	8	Battery
2	SAS/SATA RAID Controller	9	System board cooling shroud
3	Sideplane	10	Memory modules
4	Cooling fan modules	11	Heatsink/microprocessor (2)
5	Power supply bays	12	Backplane
6	Left riser (slot 2)	13	Hard drive bays (2)
7	Center riser (slot 1)	14	Optical slimline drive

Attaching the Front Bezel

The C5110 comes with an optional front panel bezel (see [Figure 26](#)), which can be attached to the front of the chassis by snapping it on the chassis handles. A key lock allows you to lock the bezel in place so that the controls on the front panel cannot be used. You can monitor the system status indicators with the bezel in place.

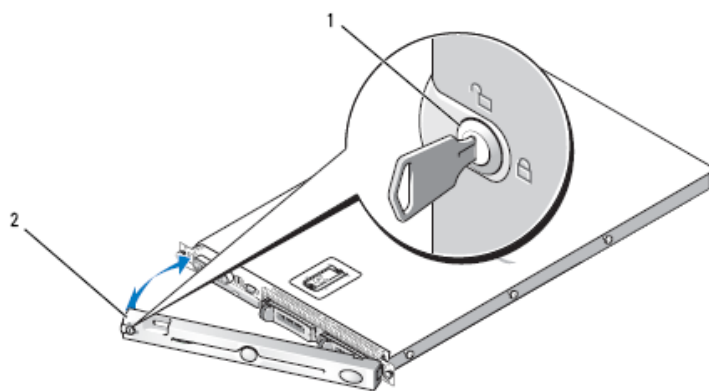




Figure 26: Attaching the Bezel to the Front of the C5110

1	Key lock	2	Bezel cover
---	----------	---	-------------

Opening and Closing the C5110

Caution
 Only trained service technicians are authorized to remove the system cover and access any of the components inside the system. See the Product Information Guide for complete information on safety precautions, working inside the computer, and protecting against electrostatic discharge.

Caution
 Whenever you need to lift the system, get others to assist you. To avoid injury, do not attempt to lift the system by yourself.

Opening the C5110

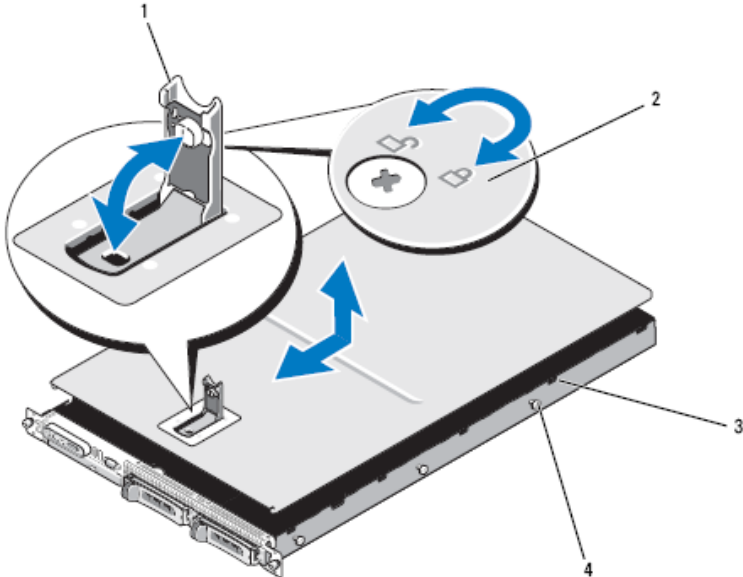


Figure 27: Removing the Cover from the C5110

1	Latch	3	Alignment J hooks
2	Latch release lock	4	Chassis tabs

- 1 Turn off the system and attached peripherals, and disconnect the system from the electrical outlet and peripherals.
- 2 Remove the bezel.
- 3 To remove the system cover, rotate the latch release lock on the latch in a counterclockwise direction to the unlocked position (see [Figure 27](#) on page 94).
- 4 Lift up on the latch on top of the system to guide it back and into an offset position (see [Figure 27](#) on page 94).



- 5 Grasp the cover on both sides and carefully lift the cover away from the system.

Closing the C5110

To Close the System:

- 1 Lift up the latch on the cover.
- 2 Place the cover on top of the system and offset the cover slightly back so that it clears the chassis J hooks and lays flat on the system chassis (see [Figure 27](#) on page 94)
- 3 Lower the cover into the closed position aligning it with the J hooks and push down on the latch to guide the cover into place.
- 4 Rotate the latch release lock in a clockwise direction to secure the cover.

Maintaining the C5210 Controller

This topic outlines the features of the C5210 controller.

Related Links

- [C5210 Front Panel Features](#) on page 95
- [C5210 Front Control Panel Features](#) on page 96
- [C5210 Back Panel Features](#) on page 97

C5210 Front Panel Features

[Figure 28](#) depicts the front panel of the C5210. [Table 17](#) depicts the features and functions of the C5210 front panel.

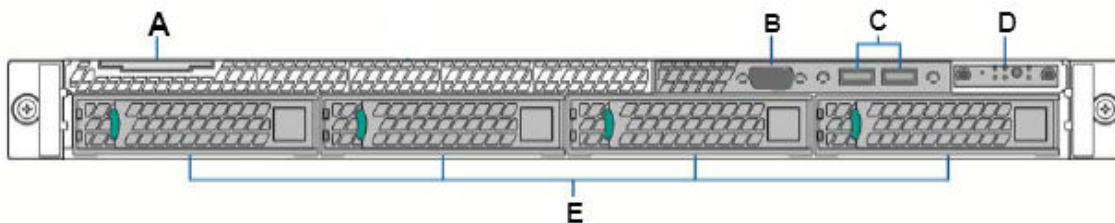


Figure 28: C5210 Front Panel Features

Table 17: C5210 Front Panel Features

Callout	Feature	Function
A	System Label Pull-out	
B	Not used	
C	USB Ports	Connects USB 2.0-compliant devices to the system. For more information, see the Note below.



Table 17: C5210 Front Panel Features (continued)

Callout	Feature	Function
D	Front Control Panel	For more information, see Figure 29 on page 96.
E	Hard Disk Drive Bays	Only left one used.

Note



The C5210 is equipped with 5 USB connectors—2 on the front panel and 3 on the back panel. However, the controller is capable of supporting only one USB device at a time, regardless of what USB connector the device is connected to. If you connect a second USB device while the first is already connected, the system will return an error.

C5210 Front Control Panel Features

This section highlights the control panel features on the front of the C5210. See callout D in [Table 17](#) on page 95. See [Table 18](#) for a description of each control.

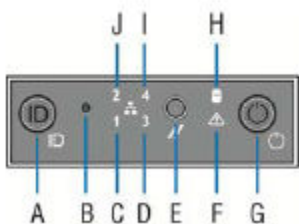


Figure 29: C5210 Front Control Panel Features

Table 18: C5210 Front Control Panel Features

Callout	Feature	Function
A	System ID Button w/Integrated LED	The identification buttons on the front panel can be used to locate a particular system within a rack. When one of the buttons is pushed, the blue system status indicator on the front and back blinks until one of the buttons is pushed again.
B	NMI Button	Not used
C	Mgmt Port Activity LED	For more information, see Table 19 on page 97.
D	Data Port 2 Activity LED	For more information, see Table 19 on page 97.
E	System Cold Reset Button	
F	System Status LED	The blue-colored system status indicator blinks to indicate the location of a particular system within a rack. The indicator continues to blink until one of the system identification button is pushed again.
G	Power Button w/Integrated LED	The power button controls the DC power supply output to the system.
H	Hard Drive Activity LED	LED Off - Power on and drive spinning up or spinning down/No access or no faults



Table 18: C5210 Front Control Panel Features (continued)

Callout	Feature	Function
		Blinking Green - Power on with drive activity
		Solid Amber - Hard drive fault has occurred
I	Data Port 4 Activity LED	Not used
J	Data Port 1 Activity LED	For more information, see the following table .

Table 19: RJ45 Port LEDs (Management Port, Data Port 1, Data Port 2)

LED Type	LED Pattern	Status Indication
Network Speed (Right)	Off	10 Mbps
	Amber	100 Mbps
	Green	1000 Mbps
Link Activity (Left)	Off	No link
	Solid Green	Active link
	Blinking Green	Data traffic activity
LED Type	LED Pattern	Status Indication

C5210 Back Panel Features

Figure 30 displays back panel features of the C5210. Table 20 depicts the features and functions of the C5210 back panel.

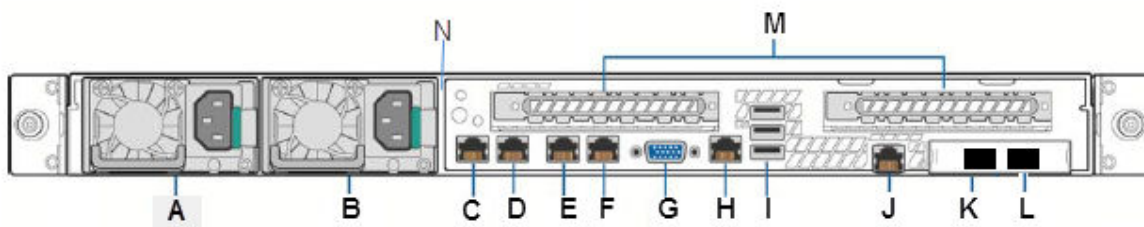


Figure 30: C5210 Back Panel Features

Table 20: C5210 Back Panel Features

Callout	Feature	Function
A	AC Power Supply 1	AC Power Supply 1 and 2 combine to make a redundant power supply.
B	AC Power Supply 2	
C	1GbE RJ45	Management port - eth0
D	1GbE RJ45	Data port 1 - esa0
E	1GbE RJ45	Data port 2 - esa1

Table 20: C5210 Back Panel Features (continued)

Callout	Feature	Function
F	Port 4	Not used
G	Video Connector	Used to see POST BIOS information during controller boot up
H	Serial-A Port RJ45	Console Port - Used to get into Rescue mode.
I	USB Ports	Connects USB 2.0-compliant devices to the system. For more information, see the Note below.
J	RMM4 NIC Port	Not used, plugged
K	1/10GbE SFP+	Data port 4 - esa3
L	1/10GbE SFP+	Data port 3 - esa2
M	Expansion slots.	Not used
N	Chassis tab	Used for optional cable bracket.

Note

The C5210 is equipped with 5 USB connectors — 2 on the front panel and 3 on the back panel. However, the controller is capable of supporting only one USB device at a time, regardless of what USB connector the device is connected to. If you connect a second USB device while the first is already connected, the system will return an error.

Maintaining the C4110 Controller

For information on the C4110 hardware, see the *Wireless Controller C4110 Quick Reference* guide.

11 Maintaining the Wireless AP Software

Maintaining a List of Current Software Images

Deleting a Software Image

Downloading a New Software Image

Defining Parameters for a Software Upgrade

Maintaining a List of Current Software Images

To maintain a list of current wireless AP software images:

- 1 From the top menu, click **AP**.

- From the left pane, click **Global > Maintenance**.

AP Software Maintenance | **Controlled Upgrade** | **AP Maintenance Cycle**

AP Images for Platform:

AP3935

AP3935-10.11.01.0194.img (Default)

Set as default | Delete

Download AP Images:

FTP Server:

User ID:

Password:

Confirm:

Directory:

Filename:

Platform: AP3935

Download

Upgrade Behavior:

Upgrade when AP connects using settings from Controlled Upgrade

Always upgrade AP to default image (overrides Controlled Upgrade settings)

Disk space left for images: 13016 MB

Save

- In the **AP Images for Platform** drop-down list, click the appropriate platform.
- To select an image to be the default image for a software upgrade, click it in the list, and then click **Set as default**.
- In the **Upgrade Behavior** section, select one of the following:
 - Upgrade when AP connects using settings from Controlled Upgrade – The **Controlled Upgrade** tab is displayed. Controlled upgrade allows you to individually select and control the state of an AP image upgrade: which APs to upgrade, when to upgrade, how to upgrade, and to which image the upgrade or downgrade should be done. Administrators decide on the levels of software releases that the equipment should be running.
 - Always upgrade AP to default image (overrides Controlled Upgrade settings) – Selected by default. Allows for the selection of a default revision level (firmware image) for all APs in the domain. As the AP registers with the controller, the firmware version is verified. If it does not match the same value as defined for the default-image, the AP is automatically requested to upgrade to the default-image.
- To save your changes, click **Save**.

Deleting a Software Image

To delete a wireless AP software image:

- 1 From the top menu, click **AP**.
- 2 From the left pane, click **Global > Maintenance**.
- 3 In the **AP Images for Platform** drop-down list, click the appropriate platform.
- 4 In the **AP Images** list, click the image you want to delete.
- 5 Click **Delete**. The image is deleted.

Downloading a New Software Image

To download a new wireless AP software image:

- 1 From the top menu, click **AP**.
- 2 From the left pane, click **Global > Maintenance**.
- 3 In the **Download AP Images** list, type the following:
 - **FTP Server** – The IP address of the FTP server to retrieve the image file from.



Note

The FTP Server supports both IPv4 and IPv6 addresses.

- **User ID** – The user ID that the controller should use when it attempts to log into the FTP server.
 - **Password** – The corresponding password for the user ID.
 - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
 - **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
 - **Filename** – The name of the image file to retrieve.
 - **Platform** – The AP hardware type to which the image applies. There are several types of APs and they require different images.
- 4 Click **Download**. The new software image is downloaded.

Defining Parameters for a Software Upgrade

To define parameters for a Wireless AP controlled software upgrade:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Maintenance**.
- 3 Under upgrade behavior, select **Upgrade when AP connects using settings from Controlled Upgrade**. The **Controlled Upgrade** tab displays.

- 4 Click the **Controlled Upgrade** tab.

AP Software Maintenance
Controlled Upgrade

Step 1: Select AP Platform:

Step 2: Select an image to use:

Step 3: Apply the AP image from Step 2 to the selected APs below:

	Wireless APs	Current version	Upgrade to
<input type="checkbox"/>	3705i	10.11.01.0190T	

Step 4: Repeat Steps 1 - 3 as necessary

Step 5: Save this upgrade strategy for later, or upgrade the APs now:



Note

The **Controlled Upgrade** tab is displayed only when the Upgrade Behavior is set to Upgrade when AP connects using settings from Controlled Upgrade on the **AP Software Maintenance** tab.

- 5 In the **Select AP Platform** drop-down list, click the type of AP you want to upgrade.
- 6 In the **Select an image to use** drop-down list, click the software image you want to use for the upgrade.
- 7 In the list of registered **Wireless APs**, select the checkbox for each AP to be upgraded with the selected software image.
- 8 Click **Apply AP image version**. The selected software image is displayed in the **Upgrade To** column of the list.
- 9 To save the software upgrade strategy to be run later, click **Save for later**.
- 10 To run the software upgrade immediately, click **Upgrade Now**. The selected AP reboots, and the new software version is loaded.



Note

The Always upgrade AP to default image checkbox on the **AP Software Maintenance** tab overrides the Controlled Upgrade settings.

12 Performing Wireless AP Diagnostics

Performing Wireless AP Diagnostics Using SSH

Performing Wireless AP Diagnostics Using SSH



Caution

For security reasons, SSH is disabled by default. SSH should only be enabled to perform diagnostic sessions. When completed, SSH should always be disabled.

As a support tool to perform diagnostic debugging of the wireless AP, the capability to access the wireless AP by SSH has been provided. Normally, SSH are disabled and should be disabled again after diagnostics. This process should only be used by support services.

To configure the password for SSH access:

- 1 From the top menu, click **AP**.
- 2 From the left pane, click **Global > Registration**.

Wireless AP Registration

Security Mode:

- Allow all Wireless APs to connect
 Allow only approved Wireless APs to connect

Discovery Timers:

Number of retries: (1 - 255)

Delay between retries: (1 - 10 seconds)

SSH Access:

Password:

Confirm password:

Secure Cluster:

Cluster Shared Secret:

Use Cluster Encryption

Figure 31: Wireless AP Registration Screen

- 3 If using SSH, in the **SSH Access** area, in the **Password** box, type the password for SSH access.

- 4 To confirm the password, in the **Confirm Password** box, re-type the password.

**Note**

When the controller ships from the factory it is configured with a default password to assign to the wireless APs that register with it. The default password is new2day. The password is sent to the wireless AP after it has registered. The administrator can override this password using the wireless AP Registration page in the GUI. For more information, see the *User Guide*.

- 5 To send the password information to all registered wireless APs, click **Save**.

**Note**

The admin password is modified in the wireless AP when a new password is saved for SSH access. SSH to wireless APs works via the console port only.

Enabling SSH on a Selected Wireless AP

To enable SSH on a selected wireless AP:

- 1 From the top menu, click **AP**.
- 2 From the left pane, click **APs**.
- 3 Click the appropriate wireless AP in the list (not the checkbox). The **AP** dashboard displays.

- 4 Click **Configure**. The **AP Properties** tab displays.

AP Properties	WLAN Assignment	Radio 1	Radio 2	Static Configuration	80
Serial #:	14160242085A0000				
Host Name:	AP3825e-14160242085A0000				
Name:	C5110 - ap3 - AP3825e				
Location:	MU7 - C5110				▶
Zone:					▶
Description:					
Topology:	esa0				
AP Environment¹:	Indoor ▼				
	¹ Change of Environment will cause interruption of service				
Hardware Type:	Wireless AP3825e External				
Application Version:	10.11.01.0196				
Status:	Approved				
Active Clients:	0				
Role:	Traffic forwarder (AP)				
Country²:	United States ▼				
	² Change of Country may cause AP to reboot.				
				Professional install	Advanced...

- 5 Click **Advanced**.
- 6 Click the **Enable SSH Access** check box.
- 7 Click **Save**. This wireless AP is enabled for an SSH session.

Disabling SSH Access on a Selected AP

To disable SSH access:

- 1 From the top menu, click **AP**.
- 2 From the left pane, click **APs**.
- 3 Click the appropriate wireless AP in the list (not the checkbox). The **AP** dashboard displays.
- 4 Click **Configure**. The **AP Properties** tab displays.
- 5 Click **Advanced**, then clear the **Enable SSH Access** check box.
- 6 Click **Save**.

The wireless AP is disabled for the SSH sessions.



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 plan).

secondary port

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

segment

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

server certificate

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

sFlow

sFlow allows you to monitor network traffic by statistically sampling the network packets and periodically gathering the statistics. The sFlow monitoring system consists of an sFlow agent

(embedded in a switch, router, or stand-alone probe) and an external central data collector, or sFlow analyzer.

SFP

Small form-factor pluggable. These transceivers offer high speed and physical compactness.

slow path

This term refers to the data path for packets that must be processed by the switch CPU, whether these packets are generated by the CPU, removed from the network by the CPU, or simply forwarded by the CPU.

SLP

Service Location Protocol. A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network.

Using SLP, networking applications can discover the existence, location and configuration of networked devices.

With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.

For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.

(SLP version 2, RFC2608, updating RFC2165)

SMF

Single-mode fiber. SMF is a laser-driven optical fiber with a core diameter small enough to limit transmission to a single bound mode. SMF is commonly used in long distance transmission of more than three miles; it sends one transmission at a time.

SMI

Structure of Management Information. A hierarchical tree structure for information that underlies Management Information Bases (MIBs), and is used by the SNMP protocol. Defined in RFC 1155 and RFC 1442 (SNMPv2).

SMON

Switch Network Monitoring Management (MIB) system defined by the IETF document RFC 2613. SMON is a set of MIB extensions for RMON that allows monitoring of switching equipment from a SNMP Manager in greater detail.

SMT

Station Management. The object class in the 802.11 MIB that provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network. The four branches of the 802.11 MIB are:

- dot11smt—objects related to station management and local configuration
- dot11mac—objects that report/configure on the status of various MAC parameters
- dot11res—objects that describe available resources
- dot11phy—objects that report on various physical items

SNMP

Simple Network Management Protocol. SNMP is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multivendor environment, and the agent uses MIBs, which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

SNTP

Simple Network Time Protocol. SNTP is used to synchronize the system clocks throughout the network. An extension of the Network Time Protocol, SNTP can usually operate with a single server and allows for IPv6 addressing.

SSH

Secure Shell, sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol of securely gaining access to a remote computer. With SSH commands, both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. At Extreme Networks, the SSH is a separate software module, which must be downloaded separately. (SSH is bundled with SSL in the software module.)

SSID

Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the Basic Service Set (BSSs). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS.

In 802.11 networks, each access point (AP) advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named access point, it sends an associate request frame containing the desired SSID. The AP replies with an associate response frame, also containing the SSID. Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.

SSL

Secure Sockets Layer. SSL is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

spoofing

Hijacking a server's IP address or hostname so that requests to the server are redirected to another server. Certificate validation is used to detect and prevent this.

standard mode

Use ESRP standard mode if your network contains switches running ExtremeWare and switches running ExtremeXOS, both participating in ESRP.

STP

Spanning Tree Protocol. STP is a protocol, defined in IEEE 802.1d, used to eliminate redundant data paths and to increase network efficiency. STP allows a network to have a topology that contains physical loops; it operates in bridges and switches. STP opens certain paths to create a tree topology, thereby preventing packets from looping endlessly on the network. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the STP topology and re-establishes the link by activating the standby path.

STPD

Spanning Tree Domain. An STPD is an STP instance that contains one or more VLANs. The switch can run multiple STPDs, and each STPD has its own root bridge and active path. In the Extreme Networks implementation of STPD, each domain has a carrier VLAN (for carrying STP information) and one or more protected VLANs (for carrying the data).

STPD mode

The mode of operation for the STPD. The two modes of operation are:

- 802.1d—Compatible with legacy STP and other devices using the IEEE 802.1d standard.
- 802.1w—Compatible with Rapid Spanning Tree (RSTP).

stub areas

In **OSPF**, a stub area is connected to only one other area (which can be the backbone area). External route information is not distributed to stub areas.

subnet mask

See [netmask](#).

subnets

Portions of networks that share the same common address format. A subnet in a TCP/IP network uses the same first three sets of numbers (such as 198.63.45.xxx), leaving the fourth set to identify devices on the subnet. A subnet can be used to increase the bandwidth on the network by breaking the network up into segments.

superloop

In [EAPS](#), a superloop occurs if the common link between two EAPS domains goes down and the master nodes of both domains enter the failed state putting their respective secondary ports into the forwarding state. If there is a data VLAN spanning both EAPS domains, this action forms a loop between the EAPS domains.

SVP

SpectraLink Voice Protocol, a protocol developed by SpectraLink to be implemented on access points to facilitate voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.

syslog

A protocol used for the transmission of [event](#) notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

system health check

The primary responsibility of the system health checker is to monitor and poll error registers. In addition, the system health checker can be enabled to periodically send diagnostic packets. System health check errors are reported to the syslog.

T

TACACS+

Terminal Access Controller Access Control System. Often run on UNIX systems, the TACAS+ protocol provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and

accounting services. User passwords are administered in a central database rather than in individual routers, providing easily scalable network security solutions.

tagged VLAN

You identify packets as belonging to the same tagged VLAN by putting a value into the 12-bit (4 octet) VLAN ID field that is part of the IEEE 802.1Q field of the header. Using this 12-bit field, you can configure up to 4096 individual VLAN addresses (usually some are reserved for system VLANs such as management and default VLANs); these tagged VLANs can exist across multiple devices. The tagged VLAN can be associated with both tagged and untagged ports.

TCN

Topology change notification. The TCN is a timer used in [RSTP](#) that signals a change in the topology of the network.

TCP / IP

Transmission Control Protocol. Together with Internet Protocol (IP), TCP is one of the core protocols underlying the Internet. The two protocols are usually referred to as a group, by the term TCP/IP. TCP provides a reliable connection, which means that each end of the session is guaranteed to receive all of the data transmitted by the other end of the connection, in the same order that it was originally transmitted without receiving duplicates.

TFTP

Trivial File Transfer Protocol. TFTP is an Internet utility used to transfer files, which does not provide security or directory listing. It relies on [UDP](#).

TKIP

Temporal Key Integrity Protocol (TKIP) is an enhancement to the WEP encryption technique that uses a set of algorithms that rotates the session keys. The protocol's enhanced encryption includes a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. The encryption keys are changed (re-keyed) automatically and authenticated between devices after the re-key interval (either a specified period of time, or after a specified number of packets has been transmitted).

TLS

Transport Layer Security. See [SSL](#).

ToS / DSCP

ToS (Type of Service) / DSCP (Diffserv Codepoint). The ToS/DSCP box contained in the IP header of a frame is used by applications to indicate the priority and [Quality of Service](#) for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-

delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service.

transit node

In **EAPS**, the transit node is a switch, or node, that is not designated a master in the EAPS domain ring.

truststore

A repository containing trusted certificates, used to validate an incoming certificate. A truststore usually contains CA certificates, which represent certificate authorities that are trusted to sign certificates, and can also contain copies of server or client certificates that are to be trusted when seen.

TSN

Transition Security Network. A subset of Robust Security Network (RSN), which provides an enhanced security solution for legacy hardware. The Wi-Fi Alliance has adopted a solution called Wireless Protected Access (WPA), based on TSN. RSN and TSN both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

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

tunnelling

Tunnelling (or encapsulation) is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating packets of a network protocol within packets carried by the second network. The receiving device then decapsulates the packets and forwards them in their original format.

U

U-NII

Unlicensed National Information Infrastructure. Designated to provide short-range, high-speed wireless networking communication at low cost, U-NII consists of three frequency bands of 100 MHz each in the 5 GHz band: 5.15-5.25GHz (for indoor use only), 5.25-5.35 GHz and 5.725-5.825GHz. The three frequency bands were set aside by the FCC in 1997 initially to help schools connect to the Internet without the need for hard wiring. U-NII devices do not require licensing.

UDP

User Datagram Protocol. This is an efficient but unreliable, connectionless protocol that is layered over IP (as is [TCP](#)). Application programs must supplement the protocol to provide error processing and retransmitting data. UDP is an OSI Layer 4 protocol.

unicast

A unicast packet is communication between a single sender and a single receiver over a network.

untagged VLAN

A VLAN remains untagged unless you specifically configure the IEEE 802.1Q value on the packet. A port cannot belong to more than one untagged VLAN using the same protocol.

USM

User-based security model. In SNMPv3, USM uses the traditional SNMP concept of user names to associate with security levels to support secure network management.

V

virtual router

In the Extreme Networks implementations, virtual routers allow a single physical switch to be split into multiple virtual routers. Each virtual router has its own IP address and maintains a separate logical forwarding table. Each virtual router also serves as a configuration domain. The identity of the virtual router you are working in currently displays in the prompt line of the CLI. The virtual routers discussed in relation to Extreme Networks switches themselves are not the same as the virtual router in VRRP.

In VRRP, the virtual router is identified by a virtual router (VRID) and an IP address. A router running VRRP can participate in one or more virtual routers. The VRRP virtual router spans more than one physical router, which allows multiple routers to provide redundant services to users.

VEPA

Virtual Ethernet Port Aggregator. This is a Virtual Machine (VM) server feature that works with the ExtremeXOS Direct Attach Feature to support communications between VMs.

virtual link

In [OSPF](#), when a new area is introduced that does not have a direct physical attachment to the backbone, a virtual link is used. Virtual links are also used to repair a discontinuous backbone area.

virtual router

In the Extreme Networks implementations, virtual routers allow a single physical switch to be split into multiple virtual routers. Each virtual router has its own IP address and maintains a separate logical forwarding table. Each virtual router also serves as a configuration domain. The identity of the virtual router you are working in currently displays in the prompt line of the CLI. The virtual routers discussed in relation to Extreme Networks switches themselves are not the same as the virtual router in VRRP.

In VRRP, the virtual router is identified by a virtual router (VRID) and an IP address. A router running VRRP can participate in one or more virtual routers. The VRRP virtual router spans more than one physical router, which allows multiple routers to provide redundant services to users.

virtual router MAC address

In VRRP, RFC 2338 assigns a static MAC address for the first five octets of the VRRP virtual router. These octets are set to 00-00-5E-00-01. When you configure the VRRP VRID, the last octet of the MAC address is dynamically assigned the VRID number.

VLAN

Virtual LAN. The term VLAN is used to refer to a collection of devices that communicate as if they are on the same physical LAN. Any set of ports (including all ports on the switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the CLI.

VLSM

Variable-length subnet masks. In [OSPF](#), VLSMs provide subnets of different sizes within a single IP block.

VM

Virtual Machine. A VM is a logical machine that runs on a VM server, which can host multiple VMs.

VMAN

Virtual MAN. In ExtremeXOS software, VMANs are a bi-directional virtual data connection that creates a private path through the public network. One VMAN is completely isolated from other VMANs; the encapsulation allows the VMAN traffic to be switched over Layer 2 infrastructure. You implement VMAN using an additional 892.1Q tag and a configurable EtherType; this feature is also known as Q-in-Q switching.

VNS

Virtual Network Services. An Extreme Networks-specific technique that provides a means of mapping wireless networks to a wired topology.

VoIP

Voice over Internet Protocol is an Internet telephony technique. With VoIP, a voice transmission is cut into multiple packets, takes the most efficient path along the Internet, and is reassembled when it reaches the destination.

VPN

Virtual private network. A VPN is a private network that uses the public network (Internet) to connect remote sites and users. The VPN uses virtual connections routed through the Internet from a private network to remote sites or users. There are different kinds of VPNs, which all serve this purpose. VPNs also enhance security.

VR-Control

This virtual router (VR) is part of the embedded system in Extreme Networks switches. VR-Control is used for internal communications between all the modules and subsystems in the switch. It has no ports, and you cannot assign any ports to it. It also cannot be associated with VLANs or routing protocols. (Referred to as VR-1 in earlier ExtremeXOS software versions.)

VR-Default

This VR is part of the embedded system in Extreme Networks switches. VR-Default is the default VR on the system. All data ports in the switch are assigned to this VR by default; you can add and delete ports from this VR. Likewise, VR-Default contains the default VLAN. Although you cannot delete the default VLAN from VR-Default, you can add and delete any user-created VLANs. One instance of each routing protocol is spawned for this VR, and they cannot be deleted. (Referred to as VR-2 in earlier ExtremeXOS software versions.)

VR-Mgmt

This VR is part of the embedded system in Extreme Networks switches. VR-Mgmt enables remote management stations to access the switch through Telnet, SSH, or SNMP sessions; and it owns the management port. The management port cannot be deleted from this VR, and no other ports can be added. The Mgmt VLAN is created VR-Mgmt, and it cannot be deleted; you cannot add or delete any other VLANs or any routing protocols to this VR. (Referred to as VR-0 in earlier ExtremeXOS software versions.)

VRID

In VRRP, the VRID identifies the VRRP virtual router. Each VRRP virtual router is given a unique VRID. All the VRRP routers that participate in the VRRP virtual router are assigned the same VRID.

VRRP

Virtual Router Redundancy Protocol. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the master router, and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility

should the master router become unavailable. In case the master router fails, the virtual IP address is mapped to a backup router's IP address; this backup becomes the master router. This allows any of the virtual router IP addresses on the LAN to be used as the default first-hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every host. VRRP is defined in RFC 2338.

VRRP router

Any router that is running VRRP. A VRRP router can participate in one or more virtual routers with VRRP; a VRRP router can be a backup router for one or more master routers.

VSA

Vendor Specific Attribute. An attribute for a RADIUS server defined by the manufacturer.(compared to the RADIUS attributes defined in the original RADIUS protocol RFC 2865). A VSA attribute is defined in order that it can be returned from the RADIUS server in the Access Granted packet to the Radius Client.

W

walled garden

A restricted subset of network content that wireless devices can access.

WEP

Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

WINS

Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer, called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS supports dynamic addressing (DHCP) by maintaining a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.

WLAN

Wireless Local Area Network.

WMM

Wi-Fi Multimedia (WMM), a Wi-Fi Alliance certified standard that provides multimedia enhancements for Wi-Fi networks that improve the user experience for audio, video, and voice applications. This

standard is compliant with the IEEE 802.11e [Quality of Service](#) extensions for 802.11 networks. WMM provides prioritized media access by shortening the time between transmitting packets for higher priority traffic. WMM is based on the Enhanced Distributed Channel Access (EDCA) method.

WPA

Wireless Protected Access, or Wi-Fi Protected Access is a security solution adopted by the Wi-Fi Alliance that adds authentication to WEP's basic encryption. For authentication, WPA specifies IEEE 802.1x authentication with Extensible Authentication Protocol (EAP). For encryption, WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet. [Certificate Authentication](#) (CA) can also be used. Also part of the encryption mechanism are 802.1x for dynamic key distribution and Message Integrity Check (MIC) a.k.a. Michael.

WPA requires that all computers and devices have WPA software.

WPA-PSK

Wi-Fi Protected Access with Pre-Shared Key, a special mode of WPA for users without an enterprise authentication server. Instead, for authentication, a Pre-Shared Key is used. The PSK is a shared secret (passphrase) that must be entered in both the AP or router and the WPA clients.

This pre-shared key should be a random sequence of characters at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. After the initial shared secret, the Temporal Key Integrity Protocol (TKIP) handles the encryption and automatic re-keying.

X

XENPAK

Pluggable optics that contain a 10 Gigabit Ethernet module. The XENPAKs conform to the IEEE 802.3ae standard.

XNV

Extreme Network Virtualization. This ExtremeXOS feature enables the software to support VM port movement, port configuration, and inventory on network switches.