

Lenovo CE0128TB/CE0128PB and CE0152TB/CE0152PB Switches

# Web GUI Reference

For Lenovo Campus NOS 8.4.3

**Lenovo**<sup>TM</sup>

**Note:** Before using this information and the product it supports, read [Appendix B, "Notices"](#) of this manual. Also read the the product *Warranty Information* document and the *Important Notices* document included with the product.

First Edition (March 2019)

© Copyright Lenovo 2019

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Lenovo and the Lenovo logo are trademarks of Lenovo in the United States, other countries, or both.

---

# Contents

<b>Preface</b> . . . . .	<b>.7</b>
Who Should Use This Guide . . . . .	8
What You'll Find in This Guide . . . . .	9
Additional References . . . . .	.10
Typographic Conventions . . . . .	.11
<b>Chapter 1. About Lenovo CE0128XB/CE0152XB Software Modules</b> . . . . .	<b>13</b>
<b>Chapter 2. Getting Started</b> . . . . .	<b>14</b>
Connecting the Switch to the Network . . . . .	.14
Booting the Switch . . . . .	.17
Understanding the User Interfaces . . . . .	.25
<b>Chapter 3. Getting Started with Stacking</b> . . . . .	<b>33</b>
Understanding Switch Stacks . . . . .	.33
Switch Stack Software Compatibility Recommendations . . . . .	.36
Incompatible Software and Stack Member Image Upgrades . . . . .	.37
Switch Stack Configuration Files . . . . .	.38
Switch Stack Management Connectivity . . . . .	.39
General Practices . . . . .	.40
Initial Installation and Power-up of a Stack . . . . .	.41
Removing a Unit from the Stack . . . . .	.42
Adding a Unit to an Operating Stack . . . . .	.43
Replacing the Stack Member with a New Unit . . . . .	.44
Renumbering Stack Members . . . . .	.45
Moving a Manager to a Different Unit in the Stack . . . . .	.46
Removing a Manager Unit from an Operating Stack . . . . .	.47
Initiating a Warm Failover of the Manager Unit . . . . .	.48
Merging Two Operational Stacks . . . . .	.49
Preconfiguration . . . . .	.50
<b>Chapter 4. Configuring System Information</b> . . . . .	<b>51</b>
Viewing the Dashboard . . . . .	.51
Viewing ARP Cache . . . . .	.53
Viewing Inventory Information . . . . .	.54
Viewing the System Firmware Status . . . . .	.56
Viewing System Resources . . . . .	.60
Defining General Device Information . . . . .	.62
Managing Logs . . . . .	.113
Configuring Email Alerts . . . . .	.122
Configuring and Viewing Device Slot Information . . . . .	.127
Configuring Power Over Ethernet (PoE) and PoE Statistics . . . . .	.131
Viewing Device Port Information . . . . .	.136
Configuring sFlow . . . . .	.151
Defining SNMP Parameters . . . . .	.159
Viewing System Statistics . . . . .	.171
Using System Utilities . . . . .	.184

Managing SNMP Traps . . . . .	198
Managing the DHCP Server . . . . .	201
Configuring Time Ranges . . . . .	209
Configuring DNS . . . . .	213
Configuring SNTP Settings . . . . .	217
Configuring the Time Zone . . . . .	224
Configuring and Viewing ISDP Information . . . . .	229
Link Dependency . . . . .	234
<b>Chapter 5. Configuring Switching Information . . . . .</b>	<b>236</b>
Managing VLANs . . . . .	236
Configuring UDLD . . . . .	246
MAC Based VLAN Status . . . . .	249
Double VLAN (DVLAN) Tunneling . . . . .	250
IP Subnet Based VLAN . . . . .	254
Protocol Based VLAN Configuration . . . . .	255
Private VLAN . . . . .	258
Voice VLAN Configuration . . . . .	264
Voice VLAN Interface . . . . .	265
Port Auto Recovery . . . . .	267
Creating MAC Filters . . . . .	270
Configuring Dynamic ARP Inspection . . . . .	272
GARP Configuration . . . . .	279
Configuring DHCP Snooping . . . . .	282
Configuring IGMP Snooping . . . . .	295
Configuring IGMP Snooping Querier . . . . .	303
Configuring MLD Snooping . . . . .	307
Configuring MLD Snooping Querier . . . . .	313
Creating Port Channels . . . . .	317
Viewing Multicast Forwarding Database Information . . . . .	322
Multicast VLAN Registration . . . . .	329
Configuring Protected Ports . . . . .	334
Configuring Spanning Tree Protocol . . . . .	335
Mapping 802.1p Priority . . . . .	352
Configuring Port Security . . . . .	354
Managing LLDP . . . . .	360
Loop Protection . . . . .	373
<b>Chapter 6. Configuring Routing . . . . .</b>	<b>376</b>
Configuring ARP . . . . .	377
Configuring Global IP Settings . . . . .	380
Router . . . . .	390
Configuring IPv6 Settings . . . . .	396
Configuring IPv6 Routes . . . . .	414
Configuring DHCPv6 . . . . .	418
Configuring Policy Based Routing . . . . .	428
<b>Chapter 7. Managing Device Security . . . . .</b>	<b>429</b>
Port Access Control . . . . .	429
RADIUS Settings . . . . .	439

TACACS+ Settings . . . . .	449
Authentication Manager . . . . .	453
<b>Chapter 8. Configuring Quality of Service . . . . .</b>	<b>463</b>
Configuring Access Control Lists . . . . .	464
Configuring Class of Service . . . . .	481
Configuring DiffServ . . . . .	485
<b>Chapter 9. Configuring Stacking . . . . .</b>	<b>501</b>
Managing Stack Summary . . . . .	501
Configuring Stacking Unit . . . . .	504
Viewing Supported Switches . . . . .	506
Updating Firmware . . . . .	508
Synchronizing Firmware . . . . .	509
Configuring Stack Ports . . . . .	510
Viewing Port Statistics . . . . .	512
Viewing Port Diagnostics . . . . .	513
Configuring Nonstop Forwarding . . . . .	515
Viewing Nonstop Forwarding Checkpoint Statistics . . . . .	517
<b>Appendix A. Getting Help and Technical Assistance . . . . .</b>	<b>519</b>
<b>Appendix B. Notices . . . . .</b>	<b>521</b>
Trademarks . . . . .	523
Important Notes . . . . .	524
Open Source Information . . . . .	525
Recycling Information . . . . .	526
Particulate Contamination . . . . .	527
Telecommunication Regulatory Statement . . . . .	528
Electronic Emission Notices . . . . .	529



---

# Preface

This guide describes how to configure the Lenovo Campus NOS 8.4.3 software features by using the Web-based graphical user interface (GUI). The CE0128TB/CE0128PB and CE0152TB/CE0152PB architecture accommodates a variety of software modules so that a platform running CE0128TB/CE0128PB and CE0152TB/CE0152PB (referred to as CE0128XB/CE0152XB throughout this document) software can function as a Layer 2 switch in a basic network or a Layer 3 router in a large, complex network.

---

## Who Should Use This Guide

The information in this guide is intended for:

- System administrators who are responsible for configuring and operating a network using CE0128XB/CE0152XB software
- Software engineers who are integrating CE0128XB/CE0152XB software into a router or switch product
- Level 1 and/or Level 2 Support providers

To obtain the greatest benefit from this guide, you should have an understanding of the base software and should have read the specification for your networking device platform. You should also have basic knowledge of Ethernet and networking concepts.



---

## What You'll Find in This Guide

This guide will help you plan, implement, and administer Campus NOS software. Where possible, each section provides feature overviews, usage examples, and configuration instructions. The following material is included:

- Chapter 1, "About Lenovo CE0128XB/CE0152XB Software Modules"
- Chapter 2, "Getting Started", "
- Chapter 3, "Getting Started with Stacking"
- Chapter 4, "Configuring System Information"
- Chapter 5, "Configuring Switching Information"
- Chapter 6, "Configuring Routing"
- Chapter 7, "Managing Device Security"
- Chapter 8, "Configuring Quality of Service"
- Chapter 9, "Configuring Stacking"
- Appendix A, "Getting Help and Technical Assistance", describes where to get help with your product.
- Appendix B, "Notices", contains legal notices.

---

## Additional References

Additional information about installing and configuring the CE0128XB/CE0152XB is available in the following guides:

- *Lenovo CE0128TB/CE0128PB and CE0152TB/CE0152PB CLI Command Reference*
- *Lenovo CE0128TB/CE0128PB and CE0152TB/CE0152PB Quick Start Guide*

# Typographic Conventions

The following table describes the typographic styles used in this book.

**Table 1.** *Typographic Conventions*

Typeface or Symbol	Meaning	Example
ABC123	This type is used for names of commands, files, and directories used within the text.  It also depicts on-screen computer output and prompts.	View the readme.txt file.  Main#
<b>ABC123</b>	This bold type appears in command examples. It shows text that must be typed in exactly as shown.	Main# <b>sys</b>
<ABC123>	This italicized type appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.  This also shows book titles, special terms, or words to be emphasized.	To establish a Telnet session, enter: host# <b>telnet</b> <IP address>  Read your <i>User's Guide</i> thoroughly.
[ ]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	host# <b>ls</b> [-a]
	The vertical bar ( ) is used in command examples to separate choices where multiple options exist. Select only one of the listed options. Do not type the vertical bar.	host# <b>set left right</b>
<b>AaBbCc1 23</b>	This block type depicts menus, buttons, and other controls that appear in Web browsers and other graphical interfaces.	Click the <b>Save</b> button.



---

# Chapter 1. About Lenovo CE0128XB/CE0152XB Software Modules

The CE0128XB/CE0152XB software suite includes the following modules:

- Switching (Layer 2)
- Routing (Layer 3)
- IPv4-IPv6 routing
- Multicast
- Quality of Service
- IPv4-IPv6 Management (CLI, Web UI, SNMP)
- Stacking
- Secure Management

---

## Chapter 2. Getting Started

This section describes how to start the switch and access the user interface.

---

### Connecting the Switch to the Network

To enable remote management of the switch through telnet, a Web browser, or SNMP, you must connect the switch to the network. By default, the switch has no IP address assigned and DHCP is enabled on the service port.

To access the switch over a network you must first configure it with network information (an IP address, subnet mask, and default gateway). You can configure the IP information using any of the following:

- BOOTP
- DHCP
- Terminal interface via the EIA-232 port

After you configure network information, such as the IP address and subnet mask, and the switch is physically and logically connected to the network, you can manage and monitor the switch remotely through SSH, telnet, a Web browser, or an SNMP-based network management system. You can also continue to manage the switch through the terminal interface via the EIA-232 port.

The CE0128XB/CE0152XB switch supports a Service port located on the front panel next to the EIA-232 port. The Service port is an Ethernet port dedicated to switch management. The Service port does not switch or route packets to or from the other front panel Ethernet ports. Because the Service port is assigned an IP address, it appears in the Routing table.

**Note:** Do NOT assign the default routing gateway to the Service port.

After you perform the physical hardware installation, you need to make a serial connection to the switch so that you can do one of the following:

- Manually configure network information for the management interface, or
- Enable the management interface as a DHCP or BootP client on your network (if not already enabled) and then view the network information after it is assigned by the DHCP server.

To connect to the switch and configure or view network information, use the following steps:

1. Using a straight-through modem cable, connect a VT100/ANSI terminal or a workstation to the console (serial) port.

If you attached a PC, Apple, or UNIX workstation, start a terminal-emulation program, such as HyperTerminal or TeraTerm.

2. Configure the terminal-emulation program to use the following settings:
  - Baud rate: 115,200 bps
  - Data bits: 8
  - Parity: none
  - Stop bit: 1
  - Flow control: none
3. Power on the switch.

For information about the boot process, including how to access the utility menu, see [“Booting the Switch” on page 17](#).
4. Press the return key, and the `User :` prompt appears.

Enter `admin` as the user name. The default password is `admin`.

After a successful login, the screen shows the system prompt, for example `(switch)>`.
5. At the `(switch)>` prompt, enter `enable` to enter the Privileged EXEC command mode. There is no default password to enter Privileged EXEC mode.

The command prompt changes to `(switch)#`.

## 6. Configure network information.

- To have the service port address assigned through DHCP:  
By default, the port is configured as a DHCP client. If your network has a DHCP server, then you need only to connect the switch to your network.

- To use BootP, change the protocol by entering:

**serviceport protocol bootp**

- To disable DHCP/BootP and manually assign an IPv4 address, enter:

**serviceport protocol none**

**serviceport ip** <ipaddress> <netmask> [<gateway>]

For example:

serviceport ip 192.168.2.23 255.255.255.0 192.168.2.1

- To disable DHCP/BootP and manually assign an IPv6 address and (optionally) default gateway, enter:

**serviceport protocol none**

**serviceport ipv6 address** <address>/<prefix-length> [eui64]

**serviceport ipv6 gateway** <gateway>

- To view the assigned or configured network address, enter:

**show serviceport**

### To enable switch management via the front panel ports:

- To use a DHCP server to obtain the IP address, subnet mask, and default gateway information, enter:

**network protocol dhcp**

- To use a BootP server to obtain the IP address, subnet mask, and default gateway information, enter:

**network protocol bootp**

- To manually configure the IPv4 address, subnet mask, and (optionally) default gateway, enter:

**network parms** <ipaddress> <netmask> [<gateway>]

For example:

network parms 192.168.2.23 255.255.255.0 192.168.2.1

- To manually configure the IPv6 address, subnet mask, and (optionally) default gateway, enter:

**network ipv6 address** <address>/<prefix-length> [eui64]

**network ipv6 gateway** <gateway>

- To view the network information, enter **show network**.

- To save these changes so they are retained during a switch reset, enter the following command:

**copy system:running-config nvram:startup-config**

After the switch is connected to the network, you can use the IP address for remote access to the switch by using a Web browser or through SSH.



---

## Booting the Switch

When the power is turned on with the local terminal already connected, the switch goes through Power-On Self-Test (POST). POST runs every time the switch is initialized and checks hardware components to determine if the switch is fully operational before completely booting.

If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM.

POST messages are displayed on the terminal and indicate test success or failure.

To boot the switch, perform the following steps:

1. Make sure that the serial cable is connected to the terminal.
2. Connect the power supply to the switch.
3. Power on the switch.

As the switch boots, the bootup test first counts the switch memory availability and then continues to boot.

4. During boot, you can use the Utility menu, if necessary, to run special procedures. To enter the Utility menu, press **2** within the first three seconds after the following message appears.

```
Lenovo Campus NOS Startup Rev: 8.4.3
Select startup mode. If no selection is made within 3 seconds,
the Lenovo Campus NOS Application will start automatically...
```

```
Lenovo Campus NOS Startup -- Main Menu
```

```
1 - Start Lenovo Campus NOS Application
2 - Display Utility Menu
Select (1, 2): 2
```

For information about the Utility menu, see [“Utility Menu Functions” on page 17](#).

5. If you do not start the Utility menu, the operational code continues to load.

After the switch boots successfully, the User login prompt appears and you can use the local terminal to begin configuring the switch. However, before configuring the switch, make sure that the software version installed on the switch is the latest version. If it is not the latest version, download and install the latest version. See [“AutoInstall” on page 58](#).

## Utility Menu Functions

You can perform many configuration tasks through the Utility menu, which can be invoked after the first part of the POST is completed.

Use the following procedures to display the Utility menu:

1. During the boot process, press **2** within three seconds after the following message displays:

```
Lenovo Campus NOS Startup Rev: 8.4.3
```

Select startup mode. If no selection is made within 3 seconds, the Lenovo Campus NOS Application will start automatically...

Lenovo Campus NOS Startup -- Main Menu

- 1 - Start Lenovo Campus NOS Application
- 2 - Display Utility Menu

Select (1, 2): 2

Lenovo Campus NOS Startup Rev: 8.4.3

Lenovo Campus NOS Startup -- Utility Menu

- 1 - Start Lenovo Campus NOS Application
- 2 - Load Code Update Package
- 3 - Load Configuration
- 4 - Select Serial Speed
- 5 - Retrieve Error Log
- 6 - Erase Current Configuration
- 7 - Erase Permanent Storage
- 8 - Select Boot Method
- 9 - Activate Backup Image
- 10 - Start Diagnostic Application
- 11 - Reboot
- 12 - Erase All Configuration Files

Q - Quit from Lenovo Campus NOS Startup

Select any of above (options or Q):

The following sections describe the Utility menu options.

## *Start Lenovo Campus NOS 8.4.3 Application*

Use option 1 to resume loading the Lenovo Campus NOS 8.4.3 Application code.

To relaunch the boot process from the Utility menu:

1. On the **Utility menu**, select **1** and press **Enter**.

The following prompt displays:

```
Select any of above (options or Q): 1
Loading image2 from /dev/mtd4
Extracting application from .stk file...done.
Loading Lenovo Campus NOS...done.
Uncompressing apps.lzma
Changing lighttpd file ownership to lighttpd:lighttpd
Expanding websrc.tar.gz into /mnt/www/htdocs...done
Product Name = Lenovo CE0128PB Switch, Product Id = 0x518
<185> Jan 1 00:02:00 0.0.0.0-0 General[fp_main_task]: unitmgr.c(6603) 1 %%% ALRT Reboot 1 (0x1)
DMA pool size: 16777216
AXI unit 0: Dev 0xb150, Rev 0x01, Chip BCM56150_A0, Driver BCM56150_A0
SOC unit 0 attached to PCI device BCM56150_A0
```

## *Load Code Update Package*

Use option 2 when a new software version must be downloaded to replace corrupted files, update, or upgrade the system software.

To download software from the Utility menu:

1. On the **Utility menu**, select **2** and press **Enter**.

The following prompt displays:

```
Select Mode of Transfer (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM)
```

2. Select the transfer mode (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM).
3. When using HyperTerminal for XMODEM/YMODEM/ZMODEM transfers, click **Transfer** on the **HyperTerminal** menu bar.
4. From the **Transfer** menu, click **Send File**.

The **HyperTerminal Send File** window displays.

5. Enter the file path for the file to be downloaded.
6. Make sure the protocol is defined per the transfer option selected in step 2 (XMODEM/YMODEM/ZMODEM).
7. Click **Send**.

The software is downloaded. Software downloading takes several minutes. The terminal emulation application, such as HyperTerminal, may display the loading process progress.

After software downloads, the switch reboots automatically.

## TFTP Transfer Option

When the TFTP transfer option is selected:

1. The switch prompts:  
Downloading code file...  
Select Mode of IP address configuration (Press D for DHCP or S for Static) []: S
2. If Static is selected, the switch will prompt for the Host IP address, Host Subnet, Gateway IP, TFTP Server IP address and the Filename as shown below:  
Enter Host IP []:  
Enter Host Subnet Mask [255.255.255.0]:  
Enter Gateway IP []:  
Enter Server IP []:  
Enter Filename []:  
Do you want to continue? Press(Y/N):
3. Enter the required information and press **Y** to start the file transfer. Pressing **N** returns.
4. If dynamic address assignment is selected, the switch prompts for the TFTP Server IP address and the Filename as shown below:  
Enter Server IP []:  
Enter Filename []:  
Do you want to continue? Press(Y/N):
5. Enter the required information and press **Y** to start the file transfer.

## Load Configuration

Use option 3 when a new configuration file must be downloaded to replace the saved system configuration file.

To download software from the Utility menu:

1. On the **Utility menu**, select **3** and press **Enter**.

The following prompt displays:

```
Select any of above (options or Q): 3
Creating tmpfs filesystem on tmpfs for download...done.
Select Configuration Type (Press T/B for Text/Binary) []: T
```

2. Select the transfer mode (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM).
3. When using HyperTerminal, click **Transfer** on the **HyperTerminal** menu bar.
4. From the **Transfer** menu, click **Send File**.

The **Send File** window displays.

5. Enter the file path for the file to be downloaded.
6. Make sure the protocol is defined per the transfer option selected in step 2 (XMODEM/YMODEM/ZMODEM).
7. Click **Send**.

The configuration file is downloaded. The terminal emulation application, such as HyperTerminal, may display the loading process progress.

## TFTP Transfer Option

When the TFTP transfer option is selected:

1. The switch prompts:

```
Creating tmpfs filesystem on tmpfs for download...done.
Select Configuration Type (Press T/B for Text/Binary) []: T
Select Mode of Transfer (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM) []:T
Select Mode of IP address configuration (Press D for DHCP or S for Static) []:S
```

2. If Static is selected, the switch will prompt for the Host IP address, Host Subnet, Gateway IP, TFTP Server IP address and the Filename as shown below:

```
Enter Host IP []:
Enter Host Subnet Mask [255.255.255.0]:
Enter Gateway IP []:
Enter Server IP []:
Enter Filename []:
Do you want to continue? Press(Y/N):
```

3. Enter the required information and press **Y** to start the file transfer. Pressing **N** returns.
4. If dynamic address assignment is selected, the switch prompts for the TFTP Server IP address and the Filename as shown below:

```
Enter Server IP []:
Enter Filename []:
Do you want to continue? Press(Y/N):
```

5. Enter the required information and press **Y** to start the file transfer.

## Select Serial Speed

Use option **4** to change the baud rate of the serial interface.

To change the baud rate from the Utility menu:

1. On the **Utility menu**, select **4** and press **Enter**.

The following prompt displays:

```
Select any of the above (options or Q): 4
```

```
1 - 1200
```

```
2 - 2400
```

```
3 - 4800
```

```
4 - 9600
```

```
5 - 19200
```

```
6 - 38400
```

```
7 - 57600
```

```
8 - 115200
```

```
9 - Exit without change
```

```
Select option (1-9):
```

**Note:** The selected baud rate takes effect immediately.

2. The Utility menu reappears.

## Retrieve Error Log

Use option **5** to retrieve the event log and download it to your ASCII terminal.

To retrieve the event log from the Utility menu:

1. On the **Utility menu**, select **5** and press **Enter**.

The following prompt displays:

```
Select Mode of Transfer (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM)
```

2. Select the transfer mode (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM).

The following prompt displays:

```
File asciilog.bin Ready to SEND in binary mode
```

```
Estimated File Size 169K, 1345 Sectors, 172032 Bytes
```

```
Estimated transmission time 3 minutes 20 seconds
```

```
Send several Control-X characters to cancel before transfer starts.
```

3. The Utility menu is displayed.

## TFTP Transfer Option

When the TFTP transfer option is selected:

1. The switch prompts:

```
Creating tmpfs filesystem on tmpfs for download...done.
```

```
Select Configuration Type (Press T/B for Text/Binary) []: T
```

```
Select Mode of Transfer (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM) []:T
```

```
Select Mode of IP address configuration (Press D for DHCP or S for Static) []:S
```

2. If Static is selected, the switch will prompt for the Host IP address, Host Subnet, Gateway IP, TFTP Server IP address and the Filename as shown below:

```
Enter Host IP []:
```

```
Enter Host Subnet Mask [255.255.255.0]:
```

```
Enter Gateway IP []:
```

Enter Server IP []:  
Enter Filename []:  
Do you want to continue? Press(Y/N):

3. Enter the required information and press **Y** to start the file transfer. Pressing **N** returns.
4. If dynamic address assignment is selected, the switch prompts for the TFTP Server IP address and the Filename as shown below:  
  
Enter Server IP []:  
Enter Filename []:  
Do you want to continue? Press(Y/N):
5. Enter the required information and press **Y** to start the file transfer.

## *Erase Current Configuration*

Use option 6 to erase the startup configuration. The Boot Sequence can then be started by selecting 1 from the Utility menu.

To erase the current configuration from the Utility menu:

1. On the **Utility menu**, select **6** and press **Enter**.
2. The switch requests confirmation of the selected action. Enter **Y** to confirm or **N** to continue without performing the action:  
  
Are you sure you want to Erase Current Configuration? (Y/N)
3. The Utility menu reappears.

## *Erase Permanent Storage*

Use option 7 to reformat the file system. All configuration information is removed from the switch. The active and backup images are not disturbed by this operation. User action is confirmed with a Y/N question before executing the command.

This operation will take several minutes. Do not remove power during this operation.

To reformat the file system from the Utility menu:

1. On the **Utility menu**, select **7** and press **Enter**.
2. The switch requests confirmation of the selected action. Enter **Y** to confirm or **N** to continue without performing the action:  
  
Do you want to erase the permanent storage? (Press Y/N):y  
Unmounting filesystem...done.  
Formatting filesystem...Mounting filesystem...done
3. The Utility menu reappears.

## *Select Boot Method*

Use option 8 to select the method used to boot the system (FLASH, Network, or Serial boot). The default selection is FLASH.

To select the boot method from the Utility menu:

1. On the **Utility menu**, select **8** and press **Enter**.

The following prompt displays:

```
Current boot method: FLASH
1 - Flash Boot
2 - Network Boot
3 - Serial Boot
4 - Exit without change
Select option (1-4):
```

2. The Utility menu reappears.

## *Activate Backup Image*

Use option 9 to activate the backup image. The active image becomes the backup when this option is selected.

To activate the backup image:

1. From the **Utility menu**, select **9** and press **Enter**.

The following message displays:

```
Backup image - image2 activated -- system reboot recommended!
Reboot? (Y/N):
```

2. Enter **Y** to reboot.

## *Start Diagnostic Application*

Use option 10 to enter the diagnostic shell.

1. On the **Utility menu**, select **10** and press **Enter**.

The following message displays:

```
Loading image2 from /dev/mtd4
Extracting application from .stk file...done.
Loading Lenovo Campus NOS...done.
Uncompressing apps.lzma
Changing lighttpd file ownership to lighttpd:lighttpd
Mounting websrc.sqfs onto /mnt/www/htdocs...done
Product Name = Lenovo CE0128TB Switch, Product Id = 0x517
Enter diag password:
```

2. The diagnostic application is protected by the password **LeNoVoCe**. After the user enters the password, the system enters the bcm shell. Use the **exit** command to exit the diagnostic shell and continue the boot process.

```
Broadcom Command Monitor: Copyright (c) 1998-no d Broadcom
Release: unknown built no datestamp (no date)
From unknown@unknown:unknown
Platform: IPROC_CMICD
OS: Unix (Posix)
DMA pool size: 16777216
AXI unit 0: Dev 0xb150, Rev 0x01, Chip BCM56150_A0, Driver BCM56150_A0
SOC unit 0 attached to PCI device BCM56150_A0
ERROR loading rc script on unit 0
BCM.0>
```

3. The bootup process restarts.

## Reboot

Use option 11 to reboot the system.

To reboot the system:

1. From the **Utility menu**, select **11** and press **Enter**.
2. The switch is rebooted.

## Erase All Configuration Files

Use option 12 to remove the startup-config, factory-defaults, and \*.cfg configuration files from the flash.

Selecting 12 from the Utility menu restores system defaults. Boot Sequence can then be started by selecting 1 from the Utility menu.

To erase the configuration files from the Utility menu:

1. On the **Utility menu**, select **12** and press **Enter**.
2. The switch requests confirmation of the selected action. Enter **Y** to confirm or **N** to continue without performing the action:  
Are you sure you want to erase all configuration files? (Y/N):
3. The Utility menu reappears.

## Q - Quit from Lenovo Campus NOS Startup

To exit the Utility menu and enter the Linux shell, press **Q** (Quit) at the Utility menu prompt as shown below:

Lenovo Campus NOS Startup Rev: 8.4.3

Lenovo Campus NOS Startup -- Utility Menu

- 1 - Start Lenovo Campus NOS Application
- 2 - Load Code Update Package
- 3 - Load Configuration
- 4 - Select Serial Speed
- 5 - Retrieve Error Log
- 6 - Erase Current Configuration
- 7 - Erase Permanent Storage
- 8 - Select Boot Method
- 9 - Activate Backup Image
- 10 - Start Diagnostic Application
- 11 - Reboot
- 12 - Erase All Configuration Files

Q - Quit from Lenovo Campus NOS Startup

Select any of above (options or Q): **Q**  
Quitting...done.

(none) login: root  
Password:

The system enters the Linux shell after the user uses the correct user root and password LeNoVoCe.



Enter a **Ctrl-D** at the login prompt to return to the boot menu.

---

## Understanding the User Interfaces

CE0128XB/CE0152XB software includes a set of comprehensive management functions for configuring and monitoring the system by using one of the following methods:

- Web User Interface
- Command-Line Interface (CLI)
- Simple Network Management Protocol (SNMP)

Each of the standards-based management methods allows you to configure and monitor the components of the CE0128XB/CE0152XB software. The method you use to manage the system depends on your network size and requirements, and on your preference.

**Note:** Not all components can be managed by each interface.

This guide describes how to use the Web-based interface to manage and monitor the system. For information about how to manage and monitor the system by using the CLI, see the *CE0128TB/CE0128PB and CE0152TB/CE0152PB CLI Command Reference* and the *CE0128TB/CE0128PB and CE0152TB/CE0152PB Configuration Guide*.

**Note:** The Web configuration and monitoring pages and CLI commands available for each platform depend on the CE0128XB/CE0152XB software version and modules installed.

## Using the Web Interface

To access the switch by using a Web browser, the browser must meet the following software requirements:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript version 1.5, or later

Use the following procedures to log on to the Web Interface:

1. Open a Web browser and enter the IP address of the switch in the Web browser address field. The user has to use a secure connection because, by default, only https is enabled and not http too.
2. Type the user name and password into the fields on the login screen, and then click **Login**.

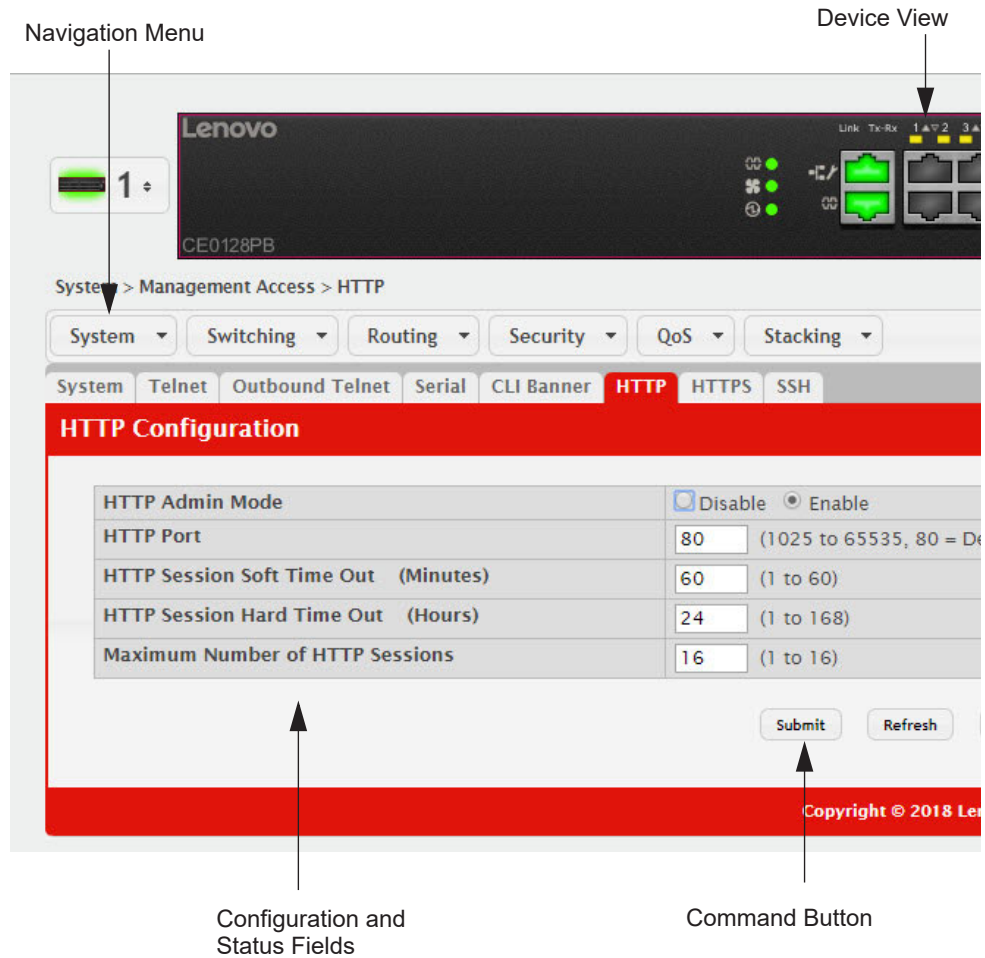
The user name and password are the same as those you use to log on to the command-line interface. By default, the user name is **admin**, and the default password is **admin**. Passwords are case sensitive.



3. After the system authenticates you, the System Description page displays.

Figure 1, “Web Interface Layout,” on page 27 shows the layout of the CE0128XB/CE0152XB software Web interface. Each Web page contains three main areas: device view, the navigation menu, and the configuration status and options.

**Figure 1.** Web Interface Layout

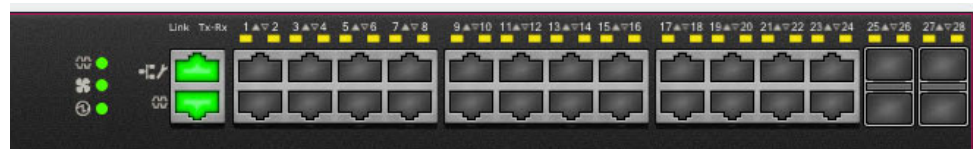


## Device View

The Device View is an interactive graphic that displays the ports on the switch. This graphic appears at the top of each page to provide an alternate way to navigate to port related configuration and monitoring options. The graphic also provides information about device ports, current configuration and status, table information, and feature components.

The port coloring indicates if a port is currently active. Green indicates that the port is enabled, red indicates that an error has occurred on the port, and blue indicates that the link is disabled.

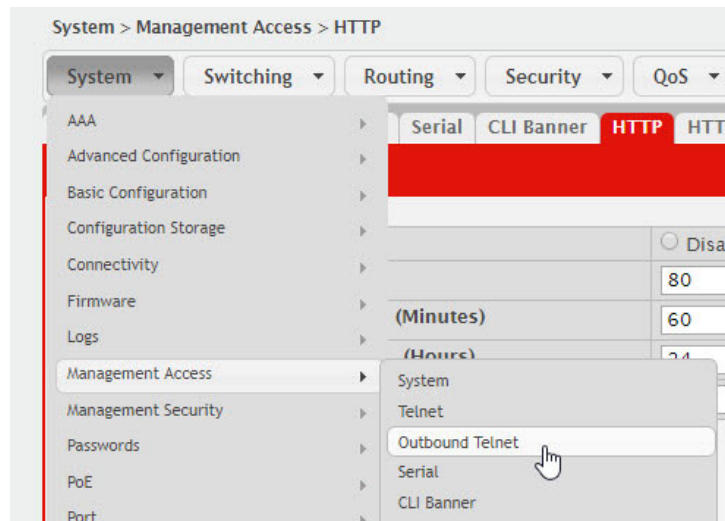
**Figure 2.** Device View



Click the port you want to view or configure to see a menu that displays statistics and configuration options. Click the menu option to access the page that contains the configuration or monitoring options.

If you click the graphic but do not click a specific port, the main menu appears, as [Figure 3](#) shows. This menu contains the same option as the navigation menu on the left side of the page.

**Figure 3.** Management Access Menu

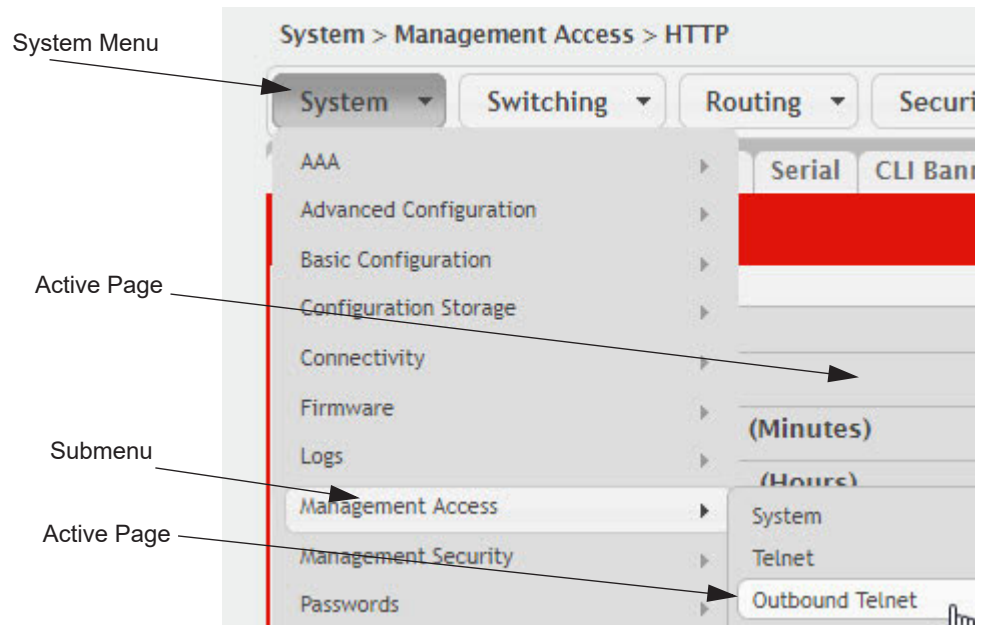


## Navigation Menu

The navigation menu is on the top of the Web interface. The navigation menu contains a list of various device features. The main items in the navigation menu can be expanded to view all the components under a specific feature, or retracted to hide the feature's components.

The navigation menu consists of a combination of main feature menus, submenus, and configuration and status pages. Click the feature menu, such as System or Switching, to view the options in that menu. Each menu contains submenus, HTML pages, or a combination of both. [Figure 4, "Navigation Menu View," on page 29](#) shows an example of a feature menu (Switching), submenu (VLAN), and the active page in the navigation menu (Port Configuration).

**Figure 4.** Navigation Menu View



When you click a menu or submenu, the color turns from gray to red, the menu expands to show its contents, and the arrow on the right side of the menu rotates. If you click a page under a menu or submenu, a new page displays in the main frame.

## Configuration and Status Fields

The main area of the screen displays the fields you use to configure or monitor the switch. On pages that contain configuration options, you can input information into fields or select options from drop-down menus.

Each page contains access to the HTML-based help that explains the fields to configure or view on the page. Many pages also contain command buttons.

Table 2 shows the command buttons that are used throughout the pages in the Web interface.

**Table 2.** Common Command Buttons

Button	Function
Submit	Sends the updated configuration to the switch. Configuration changes take effect immediately, but changes are not retained across a power cycle unless you save them to the system configuration file. To save the configuration to non-volatile memory, navigate to the <b>System &gt; System Utilities &gt; Save All Applied Changes</b> page and click <b>Save</b> .
Refresh	Refreshes the page with the most current information.
Delete	Removes the selected entry from the running configuration.
Clear	Removes all entries from a table or resets statistical counters to the default value.
Edit	Changes an existing entry.

**Table 2.** *Common Command Buttons*

Button	Function
Remove	Deletes the selected entries.
Clear Counter	Clear all the statistics counters, resetting all switch summary and detailed statistics to default values.
Logout	Ends the session.



**CAUTION:**

**Submitting changes makes them effective during the current boot session only. You must save any changes if you want them to be retained across a power cycle (reboot).**

## Table Sorting

Tables shown in the web pages now have the ability to be sorted in each column. To sort a column, click at the top of the column to sort by that field. For example, in the Event Log page, clicking on the Event Time will sort the entries by that field.

## Help Page Access

The **Help** button is always available in the upper right corner of the active page. Click **Help** to open a new page that contains information about the configuration fields, status fields, and command buttons available on the active page. The online help pages are context sensitive. For example, if the IP Addressing page is open, the help topic for that page displays if you click Help. [Figure 5](#) shows the **Help** icon.

**Figure 5.** Help Icon



[Figure 1, “Web Interface Layout,” on page 27](#) shows the location of the Help link on the Web interface.

## User-Defined Fields

User-defined fields can contain 1-159 characters, unless otherwise noted on the configuration Web page.

All characters may be used except for the following (unless specifically noted in for that feature):

\                    <  
/                    >|  
\*                    |  
?

## Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

The CLI groups commands into modes according to the command function. Each of the command modes supports specific software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

To display the commands available in the current mode, enter a question mark (?) at the command prompt. To display the available command keywords or parameters, enter a question mark (?) after each word you type at the command prompt. If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>          Press Enter to execute the command
```

For more information about the CLI, see the *CE0128TB/CE0128PB and CE0152TB/CE0152PB CLI Command Reference*.

The *CE0128TB/CE0128PB and CE0152TB/CE0152PB CLI Command Reference* lists each command available from the CLI by the command name and provides a brief description of the command. Each command reference also contains the following information:

- The command keywords and the required and optional parameters.
- The command mode you must be in to access the command.
- The default value, if any, of a configurable setting on the device.

The `show` commands in the document also include a description of the information that the command shows.

## Using SNMP

For CE0128XB/CE0152XB software that includes the SNMP module, you can configure SNMP groups and users that can manage traps that the SNMP agent generates.

CE0128XB/CE0152XB uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. Some interface configurations also involve objects in the public MIB, IF-MIB.

SNMP is enabled by default. The System Description Web page, which is the page the displays after a successful login and the `show sysinfo` command display the information you need to configure an SNMP manager to access the switch.

Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, you need to configure a new user profile. To configure a profile by using the CLI, see the SNMP section in the *CE0128TB/CE0128PB and CE0152TB/CE0152PB CLI Command Reference*.

To configure an SNMPv3 profile by using the Web interface, use the following steps:

1. Select **System > Configuration > User Accounts** from the navigation menu on the left side of the Web interface.
2. From the **User** menu, select **Create** to create a new user.
3. Enter a new user name in the **User Name** field.
4. Enter a new user password in the **Password** field and then retype it in the **Confirm Password** field.  

To use SNMPv3 Authentication for this user, set a password of eight or more alphanumeric characters.
5. To enable authentication, use the **Authentication Protocol** menu to select either MD5 or SHA for the authentication protocol.
6. To enable encryption, use the **Encryption Protocol** menu to select **DES** for the encryption scheme. Then, enter an encryption code of eight or more alphanumeric characters in the Encryption Key field.
7. Click **Submit**.

To access configuration information for SNMPv1 or SNMPv2, click the page that contains the information to configure.



---

## Chapter 3. Getting Started with Stacking

This section describes the concepts and recommended operating procedures to manage stacked Ethernet switches running CE0128XB/CE0152XB.

**Note:** For complete syntax and usage information for the commands used in this chapter, see the *CE0128TB/CE0128PB and CE0152TB/CE0152PB CLI Command Reference* for this release.

---

### Understanding Switch Stacks

A *switch stack* is a set of up to eight Ethernet switches connected through their stacking ports. One of the switches controls the operation of the stack and is called the *stack manager*. All other switches in the stack are *stack members*. The stack members use stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

CE0128XB and CE0152XB switches stack up to eight units in a ring topology. A mixture of CE0128XB and CE0152XB switches may be stacked together. Stacks are only resilient against stacking failures when configured in a ring topology. Stacks not configured in a ring topology are susceptible to stack splits where two independent stacks are formed when a stack link has errors or is disconnected.

To configure an SFP+ port pair to act as stacking ports, configure the ports as stacking using the **stack-port** command in Stack Configuration mode. The switch must be rebooted for the command to take effect.

The stack manager is the single point of stack-wide management. From the stack manager, you configure:

- System-level (global) features that apply to all stack members
- Interface-level features for all interfaces on any stack member

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack manager. The MAC address used by the switch is the MAC address of the manager. You can see this address by issuing the `show network` command. Every stack member is uniquely identified by its own *stack member number*.

All stack members are eligible stack managers. Exception: Setting a stack member's priority to 0 (zero) makes it ineligible for manager selection. When the stack is formed, one of the units is automatically selected as the Standby for the stack. The standby of the stack takes over as Manager if the current Manager fails. The standby of the stack can also be configured using the `standby <unit-number>` command.

The stack manager contains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes.

If the manager is removed from the stack, the standby of the stack will take over and will then run from that saved configuration.

You can use these methods to manage switch stacks:

- Web interface
- Command line interface (CLI) over a serial connection to the console port of the manager
- A network management application through the Simple Network Management Protocol (SNMP)

## Switch Stack Membership

A switch stack has up to eight stack members, including the manager, connected through their stacking ports. A switch stack always has one stack manager.

A standalone switch is a switch stack with one stack member that also operates as the stack manager. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them being the stack manager. You can connect standalone switches to an existing switch stack to increase the stack membership.

If you replace a stack member with an identical model, the new switch functions with exactly the same configuration as the replaced switch, assuming that the new switch is using the same member number as the replaced switch. By default, CE0128XB/CE0152XB configures the new member.

The operation of the switch stack continues uninterrupted during membership changes unless you remove the stack manager.

## Stack Manager Election and Re-Election

The stack manager is elected or re-elected based on one of these factors and in the order listed:

- The switch that is currently the stack manager
- The switch with the highest stack member priority value

**Note:** Assign the highest priority value to the switch that you prefer to be the stack manager. This ensures that the switch is re-elected as stack manager if a re-election occurs.

- The switch with the higher MAC address

A stack manager retains its role unless one of these events occurs:

- The stack manager is removed from the switch stack
- The stack manager is reset or powered off
- The stack manager has failed
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks

In the case of a manager re-election, the new stack manager becomes available after a few seconds.

If a new stack manager is elected and the previous stack manager becomes available, the previous stack manager does not resume its role as stack manager.

## Stack Member Numbers

A stack member number (1 to n) identifies each member in the switch stack. The member number also determines the interface-level configuration that a stack member uses. You can display the stack member number by using the `show switch` Privileged EXEC command.

A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a switch stack, its default stack member number changes to the lowest available member number in the stack.

Stack members in the same switch stack cannot have the same stack member number. Every stack member, including a standalone switch, retains its member number until you manually change the number or unless the number is already being used by another member in the stack. See [“Renumbering Stack Members”](#) on page 45 and [“Merging Two Operational Stacks”](#) on page 49.

## Stack Member Priority Values

You can set the stack member’s priority in the range 0 to 15.

---

## Switch Stack Software Compatibility Recommendations

All stack members must run the same CE0128XB/CE0152XB software version to ensure compatibility between stack members. The software versions on all stack members, including the stack manager, must be the same. This helps ensure full compatibility in the stack protocol version among the stack members.

If a stack member is running a software version that is not the same as the stack manager, then the stack member joins the stack but stays in *code incompatible* status (the stack unit is not allowed to join the stack as a fully functional member). Use the `show switch` command to list the stack members and the software versions. The new unit will be visible. The administrator can load the code to that new unit and reset the unit. The ports on the unit in *software mismatch* state do not come up.

---

## Incompatible Software and Stack Member Image Upgrades

You can upgrade a switch that has an incompatible software image by using the `copy {active | backup} unit://<unit-number>/{active | backup}` command from config stack mode. It copies the software image from an existing stack member to the one with incompatible software. Because that switch does not automatically reload, issue a `reload` command to that switch and it joins the stack as a fully functioning member.

---

## Switch Stack Configuration Files

The configuration files record settings for all global and interface specific settings that define the operation of the stack and individual members. Once a save to the configuration is issued, all stack members store a copy of the configuration settings. If a stack manager becomes unavailable, any stack member assuming the role of stack manager will operate from the saved configuration files.

When a new, out-of-box switch joins a switch stack, it uses the system-level settings of that switch stack. If the switch to store this system-level configuration, you must issue the following command (in Privileged EXEC mode):

```
copy system:running-config nvram:startup-config
```

This will save passwords and all other changes to the device.

If you do not save the configuration by doing this command, all configurations will be lost when a power cycle is performed on the networking device or when the networking device is reset.

**Note:** After downloading a configuration file to a stack, you must perform a configuration save operation from the CE0128XB/CE0152XB user interface (i.e. the `copy` command shown above) to distribute this configuration to non-management units in the stack. This is also true of SSH key files and SSL certificate files. From the command line interface, the following command can be used: `copy system:running-config nvram:startup-config` (in Privileged EXEC)

You back up and restore the stack configuration in the same way as you would for standalone switch configuration.

---

## Switch Stack Management Connectivity

You manage the switch stack and the stack member interfaces through the stack manager. You can use the web interface, CLI, and SNMP. You cannot manage stack members on an individual switch basis.

### Connectivity to the Switch Stack Through Console Ports

You can connect to the stack manager through the console port of the stack manager only.

### Connectivity to the Switch Stack Through Telnet

You can also telnet to the stack manager using the command `telnet <ipaddress>` then `login`.

---

## General Practices

The following practices are recommended:

- When issuing a command (such as `move management`, or `renumber`), allow the command to fully complete before issuing the next command. For example, if you issue a reset to a stack member, use the `show port` command to verify that the unit has remerged with the stack, and all ports are joined before issuing the next command.
- When physically removing or relocating a unit, always power down the unit before disconnecting stack cables.
- When reconnecting stack cables, connect them before powering up the unit, if possible. Tighten all connector screws, where applicable, to ensure a good connection.

The following sections provide switch stack configuration scenarios. Most of the scenarios assume at least two switches are connected through their stacking ports.



---

## Initial Installation and Power-up of a Stack

Use the following steps to install and power-up a stack of switches:

1. Install units in rack whenever possible to prevent the units and cables from being disturbed
2. Install all stacking cables. Fully connect all cables, including the redundant stack link. Install a redundant link because this provides stack resiliency.
3. Identify the unit to be the manager. Power this unit up first.
4. To set up a stack, complete the following steps:
  - a. Make sure there is a CE0128XB/CE0152XB image on each box.
  - b. If the image does not exist or needs to be updated, use TFTP or xmodem to perform the update operation.
5. Monitor the console port. Allow this unit to come up to the login prompt. If the unit has the default configuration, it should come up as unit #1, and will automatically become a manager unit. If not, renumber the unit as desired.
6. If desired, preconfigure other units to be added to the stack. See [“Preconfiguration” on page 50](#).
7. Power on a second unit, making sure it is adjacent (next physical unit in the stack) to the unit already powered up. This will ensure the second unit comes up as a member of the stack, and not a *Manager* of a separate stack.
8. Monitor the manager unit to see that the second unit joins the stack. Use the `show switch` command to determine when the unit joins the stack. It will be assigned a unit number (unit #2, if it has the default configuration.)
9. If desired, renumber this stack unit. See [“Renumbering Stack Members” on page 45](#) for recommendations for renumbering stack members.
10. Repeat steps 6 through 8 to add additional members to the stack. Always power on a unit adjacent to the units already in the stack.

---

## Removing a Unit from the Stack

Use the following steps to remove a switch from the stack:

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.
2. Power down the unit to be removed.
3. Disconnect the stacking cables
4. If the unit is not to be replaced, reconnect the stack cable from the stack member above to the stack member below the unit being removed.
5. Remove the unit from the rack.
6. If desired, remove the unit from the configuration by issuing the command: `no member <unit-id>` in Stack mode.

Using the Web Interface, you delete a member of the stack through the **Stacking - Unit Configuration** page. To delete a member, select the unit number on the **Switch ID** menu and click the **Delete** button.

---

## Adding a Unit to an Operating Stack

Use the following steps to add a switch to a stack of switches while the stack is running:

1. Make sure that the redundant stack link is in place and functional. All stack members should be connected in a logical ring.
2. Preconfigure the new unit, if desired.
3. Install the new unit in the rack. (Assumes installation below the bottom-most unit, or above the top-most unit).
4. Disconnect the redundant stack cable that connects the last unit in the stack back up to the first unit in the stack at the new position in the ring where the new unit is to be inserted.
5. Connect this cable to the new unit, following the established order of connections. In other words, use the redundant stack cable to connect from the first box in the stack to the last.
6. Power up the new unit. Verify, by monitoring the manager unit console port, that the new unit successfully joins the stack by using the `show switch` command in EXEC mode. The new unit should always join as a *member* (never as manager; the existing manager of the stack should not change).
7. If the CE0128XB/CE0152XB software version of the newly added member is not the same as the existing stack, update the software image.

Adding a powered-up standalone unit to an operational stack is similar to merging two operational stacks where the standalone unit is a stack of one unit. See [“Merging Two Operational Stacks” on page 49](#) for more details.

Using the Web Interface, you create a new member for the stack through the **Stacking - Unit Configuration** page. To create a new member, select the **create** option from the **Switch ID** pull-down menu.

---

## Replacing the Stack Member with a New Unit

There are two options here. If a stack member of a certain model number is replaced with another unit of the same model, follow these steps:

1. Follow the process in [“Removing a Unit from the Stack” on page 42](#) to remove the desired stack member.
2. Follow the process in [“Adding a Unit to an Operating Stack” on page 43](#) to add a new member to the stack with the following exceptions:
  - o Insert the new member in the same position in the stack as the one removed.
  - o The preconfiguration described in step 2 of [“Adding a Unit to an Operating Stack” on page 43](#) is not required.

If a stack member is replaced with a unit of a different model number, follow these steps:

1. Follow the process in [“Removing a Unit from the Stack” on page 42](#) to remove the desired stack member.
2. Remove the now-absent stack member from the configuration by issuing the `no member` command in Config Stack mode.
3. Add the new stack unit to the stack using the process described in [“Adding a Unit to an Operating Stack” on page 43](#). The unit can be inserted into the same position as the unit just removed, or the unit can be inserted at the bottom of the stack. In either case, make sure all stack cables are connected with the exception of the cable at the position where the new unit is to be inserted to ensure that the stack does not get divided into two separate stacks, causing the election of a new manager.

---

## Renumbering Stack Members

1. If particular numbering is required, assign specific numbers to stack members when they are first installed and configured in the stack, if possible.
2. If the desired stack unit number for a particular unit is unused, a unit can be renumbered simply by using the switch `<oldunit-id> renumber <newunit-id>` CLI command in Global Config mode.
3. Renumbering a non-manager unit requires a unit reset for the renumbering to take effect. Renumbering a manager unit requires a reset of all the switches in the stack for the renumbering to take effect.
4. If the newunit-id has been preconfigured, you may need to remove the newunit-id from the configuration before renumbering the unit.
5. If reassignment of multiple existing stack unit numbers is necessary, there are a number of implications in terms of mismatching of configuration. In this case, power down all units except the manager and add back one at a time using the procedure in [“Adding a Unit to an Operating Stack” on page 43](#).

Using the Web Interface, you renumber a switch through the **Stacking - Unit Configuration** page. To renumber a switch:

1. Select the switch you want to renumber from the **Switch ID** menu
2. Type the new number into the **Switch ID** input box and click a button to submit

---

## Moving a Manager to a Different Unit in the Stack

Use the following steps to change the stack manager from the current switch to a new switch in the stack:

1. Using the `movemanagement` command, move the manager to the desired unit number. The operation may take three minutes or longer depending on the stack size and configuration. The command is `movemanagement <fromunit-id><tounit-id>` in Config Stack mode.
2. Make sure that you can log in on the console attached to the new manager. Use the `show switch` command to verify that all units rejoined the stack.
3. Reset the stack with the `reload` command in Privileged EXEC mode after moving the manager.

---

## Removing a Manager Unit from an Operating Stack

Use the following steps to remove the manager unit from the stack during operation:

1. Move the designated manager to a different unit in the stack using the [“Moving a Manager to a Different Unit in the Stack”](#) on page 46 procedure on this page.
2. Using the procedure [“Removing a Unit from the Stack”](#) on page 42, remove the unit from the stack.

---

## Initiating a Warm Failover of the Manager Unit

You can use the `initiate failover` command to initiate a *warm* restart. This command reloads the management unit, triggering the standby unit to take over. As the standby management unit takes over, the system continues to forward end-user traffic. The end-user data streams may lose a few packets during the failure, but they do not lose their IP sessions, such as VoIP calls.

If there no standby unit is available when the `initiate failover` command is issued, the command fails with an error message stating that no standby unit exists. If the standby unit is not ready for a warm restart, the command fails with a similar error message. The `move management` command triggers a cold restart, even if the target unit is the backup unit.



---

## Merging Two Operational Stacks

The recommended procedure for merging two operational stacks is as follows:

1. Always power off all units in one stack before connecting to another stack.
2. Add the units as a group by unplugging one stacking cable in the operational stack and physically connecting all unpowered units.
3. Completely cable the stacking connections, making sure the redundant link is also in place.

Two operational stacks can also be merged by reconnecting stack cables without powering down all units in one stack. Connecting a powered-up standalone unit to an existing stack leads to same behavior as when merging two operational stacks. In such cases, the Manager re-election is done based on the rules listed in [“Stack Manager Election and Re-Election” on page 34](#). One of the two managers wins the election and the losing stack manager resets itself and all its member units. After the reset, all the losing stack members join the winning stack to form a single stack. The winning stack remains functional through the merge process. If the stack merge is performed in this way, then it is strongly recommended that the user set the priority of the desired winner stack manager to a higher value than the stack manager that should lose the election.

---

## Preconfiguration

This section is intended to explain how to configure units. Units do not necessarily have to be preconfigured in order to be added to the stack.

1. General information: All configuration on the stack, except unit numbers, is stored on the management unit. This means that a stack unit may be replaced with another device of the same type without having to reconfigure the switch. Unit numbers are stored independently on each switch, so that after power cycling the stack, the units always come back with the same unit numbers. The unit type associated with each unit number may be learned by the management unit automatically as the units are connected or preconfigured by the administrator.
2. Issue the `member <unit-id> <switchindex>` command to preconfigure a unit from the config stack mode. Supported unit types are shown by the `show supported switchtype` command.
  - o To display supported switches:  
Use Privileged EXEC mode  
  
Enter the command `show supported switchtype <x>` where x is the SID.
  - o To add a new member (see [“Adding a Unit to an Operating Stack” on page 43](#)):  
Use Config stack mode  
  
Enter the `member <unit-id>` command
3. Next, configure the unit you just defined with configuration commands, just as if the unit were physically present.
4. Ports for the preconfigured unit come up in *detached* state and can be seen with the `show port all` command in Privileged EXEC mode. The detached ports may now be configured for VLAN membership and any other port-specific configuration.
5. After a unit type is preconfigured for a specific unit number, attaching a unit with a different unit type for this unit number causes the switch to report an error. The Privileged Exec mode `show switch` command indicates *config mismatch* for the new unit and the ports on that unit do not come up. To resolve this situation, you may change the unit number of the mismatched unit, using the procedure in [“Renumbering Stack Members” on page 45](#), or delete the preconfigured unit type using the `no member <unit-id>` command from the config stack mode.

## Chapter 4. Configuring System Information

Use the features in the System feature menu to define the switch's relationship to its environment.

### Viewing the Dashboard

After a successful login, the Dashboard page displays. This page provides a brief overview of the system.

To navigate to the Dashboard, click **System > Summary > Dashboard** in the navigation menu.

**Figure 6.** System Dashboard

The screenshot displays the System Dashboard interface. At the top, there are navigation tabs for System, Switching, Routing, Security, QoS, and Stacking. Below these are sub-tabs for Dashboard, Description, Inventory, and MAC Address Table. A red banner with the word "ENTERPRISE" is visible. The main content area is divided into several sections:

- System Information:** A table with the following data:

System Description	Lenovo CE0128PB Switch, 1.2.22.7, Linux 4.4.1
System Name	dhcp-10-27-7-158
System Location	
System Contact	
IP Address	0.0.0.0
Burned In MAC Address	80:96:21:F1:01:00
Service Port IP Address	10.27.7.158
Service Port MAC Address	80:96:21:F1:01:01
System Up Time	0 days, 4 hours, 2 mins, 15 secs
- Device Information:** A table with the following data:

Machine Type	Lenovo CE0128PB Switch
Machine Model	CE0128PB
Serial Number	
FRU Number	
Maintenance Level	
Software Version	1.2.22.7
Operating System	Linux 4.4.145
- System Resource Usage:** Two progress bars are shown: CPU Utilization (60 Second Average) and Memory Usage.
- Disk Space Utilization:** A table with the following data:

Total Disk Space (Kbytes)	27,584
Free Disk Space (Kbytes)	26,776
Used Disk Space (Kbytes)	808
Disk Usage	

**Table 3.** *Dashboard Fields*

Field	Description
System Information	
System Description	The product name of this device.
System Name	The configured name used to identify this device.
System Location	The configured location of this device.
System Contact	The configured contact person for this device.
IP Address	The IP address assigned to the network interface. The network interface is the logical interface that allows remote management of the device via any of the front-panel switch ports.
Burned In MAC Address	The device burned-in universally-administered media access control (MAC) address of the base system.
Service Port IP Address	The IP address assigned to the service port. The service port provides remote management access to the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.
Service Port MAC Address	The device burned-in universally-administered media access control (MAC) address of the service port.
System Up Time	The time in days, hours, minutes and seconds since the system was last reset.
Device Information	
Machine Type	The device hardware type or product family.
Machine Model	The model identifier, which is usually related to the Machine Type.
Serial Number	The unique device serial number.
FRU Number	The field replaceable unit number.
Maintenance Level	The device hardware change level identifier.
Software Version	The release.version.maintenance number of the software currently running on the device. For example, if the release is 1, the version is 2 and the maintenance number is 4, this version number is displayed as 1.2.4.
Operating System	The device operating system type and version identification information.
System Resource Usage	
CPU Utilization (60 Second Average)	The percentage of CPU utilization for the entire system averaged over the past 60 seconds.
Memory Usage	The percentage of total available system memory (RAM) that is currently in use.
Disk Space Utilization	
Disk Usage	The percentage of total available disk space that is currently in use.
Additional Fields	
Logged In Users	A brief summary indicating all other users currently logged into the device. The Idle Time field gives an indication of user activity, with a smaller time value denoting more recent access to the system.
Recent Log Entries	A brief list of the newest entries recorded in the system log.

Click **Refresh** to reload the page and refresh the Dashboard.

## Viewing ARP Cache

The ARP cache is a table maintained locally in each station on a network. ARP cache entries are learned by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), every recipient has the opportunity to store the sender's IP and MAC address in their respective ARP cache. The ARP response, being unicast, is normally seen only by the requester, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The ARP cache can support 512 entries, although this size is user-configurable to any value less than 512. A single ARP cache is used for all interfaces.

To display the system ARP cache, click **System > Status > ARP Cache** page in the navigation menu.

**Figure 7.** ARP Cache

MAC Address	IP Address
E0:2F:6D:44:17:C1	10.27.6.1
02:02:BC:80:00:02	250.251.252.254

**Table 4.** ARP Cache Fields

Field	Description
MAC Address	Displays the physical (MAC) address of the system in the ARP cache.
IP Address	Displays the IP address associated with the system's MAC address.
Interface	Displays the unit, slot, and port number being used for the connection. For non-stacking systems, only the slot and port number is displayed. For units that have a service port, the service port will be listed as <i>Management</i> in this field.

Click **Refresh** to reload the page and refresh the ARP cache view. Click **Clear Entries** to clear all entries from the table. The table will be repopulated as new addresses are learned.

## Viewing Inventory Information

Use the Inventory Information page to display the switch's Vital Product Data, which is stored in non-volatile memory at the factory.

To display the inventory information, click **System** > **Summary** > **Inventory** page in the menu.

**Figure 8.** Inventory Information

System Inventory Information	
Management Unit Number	1
System Description	Lenovo CE0128PB Switch, 1.2.22.7, Lin
Machine Type	Lenovo CE0128PB Switch
Machine Model	CE0128PB
Serial Number	
FRU Number	
Part Number	7Z34CTO2WW
Maintenance Level	
Manufacturer	
Burned In MAC Address	80:96:21:F1:01:00
Software Version	8.4.3
Operating System	Linux 4.4.145
Network Processing Device	BCM56150_A0
Additional Packages	QOS Multicast IPv6 IPv6 Management Stacking Routing

**Table 5.** Inventory Information Fields

Field	Description
Management Unit Number	Unit number that corresponds to the stack manager. This field is available only on switches that support stacking.
System Description	The product name of this switch.
Machine Type	The machine type of this switch.
Machine Model	The model within the machine type.
Serial Number	The unique serial number for this switch.
FRU Number	The field replaceable unit number.
Part Number	The manufacturing part number.
Maintenance Level	The identification of the hardware change level.
Manufacturer	The two-octet code that identifies the manufacturer.

**Table 5.** *Inventory Information Fields (continued)*

<b>Field</b>	<b>Description</b>
Burned In MAC Address	The burned-in universally administered MAC address of this switch.
Software Version	The release version.maintenance number of the code currently running on the switch. For example, if the release is 1, the version is 2 and the maintenance number is 4, the format is <b>1.2.4</b> .
Operating System	The operating system currently running on the switch.
Network Processing Device	Identifies the network processor hardware.
Additional Packages	A list of the optional software packages installed on the switch, if any. For example, Campus NOS IPv6, or Campus NOS Multicast.

## Viewing the System Firmware Status

The pages in the Firmware folder allow you to view and monitor the system firmware status. The Firmware folder has links to the following pages.

### Dual Image Status

The Dual Image feature allows the switch to have two CE0128XB/CE0152XB software images in the permanent storage. One image is the active image, and the second image is the backup. This feature reduces the system down-time during upgrades and downgrades. You can use the Dual Image Status page to view information about the system images on the device.

To display the Dual Image Status page, click **System > Firmware > Status** in the navigation menu.

**Figure 9.** Dual Image Status

Unit	Active	Backup	Current Active
1	8.4.3	8.4.2	8.4.3

Image Description	
Active	
Backup	

Refresh

**Table 6.** Dual Image Status Fields

Field	Description
Unit	Displays the unit ID of the switch.
Active	Displays the version of the active code file.
Backup	Displays the version of the backup code file.
Current Active	Displays the currently active image on this unit.
Next Active	Displays the image to be used on the next restart of this unit.
Active Description	Displays the description associated with the active code file.
Backup Description	Displays the description associated with the backup code file.

Click **Refresh** to display the latest information from the router.

For information about how to update or change the system images, see [“Using System Utilities”](#) on page 184.



## Dual Image Configuration and Upgrade

Use the Dual Image Configuration and Upgrade feature to transfer a new firmware (code) image to the device, select which image to load during the next boot cycle, and add a description to each image on the device. The device uses the HTTP protocol to transfer the image, and the image is saved per user choice - either as active image or backup image.

To display the Dual Image Configuration and Upgrade page, click **System > Firmware > Configuration and Upgrade** in the navigation menu.

**Figure 10.** Dual Image Configuration and Upgrade

**Table 7.** Dual Image Status Fields

Field	Description
Unit	Use this field to select the unit with the code image to activate, upgrade, delete, or describe.
Active	<p>The active code file version. Use the icons to the right of the field to perform the file transfer.</p> <ul style="list-style-type: none"> <li>To transfer a new code image to the device, click the <b>File Transfer</b> icon. The <b>Firmware Upgrade</b> window opens. Click <b>Choose File</b> to browse to the file to transfer. After you select the appropriate file, click <b>Begin Transfer</b> to launch the HTTP transfer process. The active image is overwritten by the file that you transfer.</li> </ul>
Backup	<p>The backup code file version. Use the icons to the right of the field to perform the following tasks:</p> <ul style="list-style-type: none"> <li>To transfer a new code image to the device, click the <b>File Transfer</b> icon. The <b>Firmware Upgrade</b> window opens. Click <b>Choose File</b> to browse to the file to transfer. After you select the appropriate file, click <b>Begin Transfer</b> to launch the HTTP transfer process. If a backup image already exists on the device, it is overwritten by the file that you transfer.</li> <li>To delete the backup image from permanent storage, click the – (minus) icon. You must confirm the action before the image is deleted. Deleting an image can take several minutes. Do not power cycle or reboot the switch during the operation.</li> </ul>

**Table 7.** *Dual Image Status Fields*

Field	Description
Next Active	Use this field to select the image version to load the next time this unit reboots.
Active Description	Use this field to specify a description to associate with the image that is currently the active code file.
Backup Description	Use this field to specify a description to associate with the image that is currently the backup code file.
Select File	Use this field to provide option to browse to the directory where the file is located and select the file to transfer to the device.
Status	Provides information about the status of the file transfer.

## AutoInstall

The AutoInstall feature enables the configuration of a switch automatically when the device is turned on and, during the boot process, no configuration file is found in device storage. By communicating with a DHCP server, AutoInstall obtains an IP address for the switch and an IP address for a TFTP server. AutoInstall attempts to download a configuration file from the TFTP server and install in on the switch.

The DHCP server that the switch communicates with must provide the following information:

- The IP address and subnet mask (option 1) to be assigned to the switch.
- The IP address of a default gateway (option 3), if needed for IP communication.
- The identification of the TFTP server from which to obtain the boot file. This is given by any of the following fields, in the priority shown (highest to lowest):
  - The sname field of the DHCP reply.
  - The hostname of the TFTP server (option 66). Either the TFTP address or name is specified (not both) in most network configurations. If a TFTP hostname is given, a DNS server is required to translate the name to an IP address.
  - The IP address of the TFTP server (option 150).
  - The address of the TFTP server supplied in the siaddr field.
  - The name of the configuration file (boot file or option 67) to be downloaded from the TFTP server. **The boot file name must have a file type of \*.cfg.**
- The IP addresses of DNS name servers (option 6). The IP addresses of DNS name servers should be returned from the DHCP server only if the DNS server is in the same LAN as the switch performing AutoInstall. A DNS server is needed to resolve the IP address of the TFTP server if only the **sname** or option 66 values are returned to the switch.

After obtaining IP addresses for both the switch and the TFTP server, the AutoInstall feature attempts to download a host-specific configuration file using the boot file name specified by the DHCP server. If the switch fails to obtain the file, it will retry indefinitely.

To display the AutoInstall page, click **System > Firmware> AutoInstall**.

**Figure 11.** AutoInstall

AutoInstall Configuration	
Admin Mode	<input type="radio"/> Start <input checked="" type="radio"/> Stop
Persistent Mode	<input type="checkbox"/>
AutoSave Mode	<input type="checkbox"/>
AutoReboot Mode	<input checked="" type="checkbox"/>
Retry Count	<input type="text" value="3"/> (1 to 3)
Status	AutoInstall is completed.

**Table 8.** *AutoInstall Fields*

Field	Definition
Admin Mode	The current administrative mode of the AutoInstall feature: <ul style="list-style-type: none"> <li>• <b>Start</b> — AutoInstall is enabled, and the feature will attempt to automatically configure the device during the next boot cycle.</li> <li>• <b>Stop</b> — AutoInstall is disabled. The automatic process will begin only if no configuration file is located during the next boot cycle.</li> </ul>
Persistent Mode	If this option is selected, the settings you configure on this page are automatically saved to persistent memory in the startup-config file when you apply the changes. If this option is not selected, the device treats these settings like any other applied changes (i.e. the changes are not retained across a reboot unless you save the configuration).
AutoSave Mode	If this option is selected, the downloaded configuration is automatically saved to persistent storage. If this option is not selected, you must explicitly save the downloaded configuration in non-volatile memory for the configuration to be available for the next reboot.
AutoReboot Mode	If this option is selected, the switch automatically reboots after a new image is successfully downloaded and makes the downloaded image the active image. If this option is not selected, the device continues to boot with the current image. The downloaded image will not become the active image until the device reboots.
Retry Count	When attempting to retrieve the DHCP-specified configuration file, this value represents the number of times the TFTP client on the device tries to use unicast requests before reverting to broadcast requests.
Status	The current status of the AutoInstall process.

Click **Refresh** to display the most recently configured AutoInstall state from the switch.

## Viewing System Resources

Use the System Resources page to display the following memory information for the switch:

- Free memory
- Allocated memory
- CPU utilization by task
- Total CPU utilization at the following intervals:
  - Five seconds
  - One minute
  - Five minutes

To display the Resource Status page, click **System > Status > Resource Status** in the navigation menu.

**Figure 12.** System Resource Status

System Resource Status			
Memory Usage			
Free Memory (Kbytes)	285424		
Alloc Memory (Kbytes)	731180		
CPU Utilization Report			
Display 10 rows		Showing 1 to 10 of 45 entries	
Task ID	Task Name	5 Seconds	60 Seconds
	(kworker/u2:0)	0.00%	0.01%
	(rcu_preempt)	0.00%	0.05%
	(procmgr)	0.41%	0.28%
	(syncdb)	0.00%	0.01%
	osapiTimer	0.20%	0.15%
	bcmINTR	0.00%	0.01%
	socdmadesc.0	0.20%	0.19%
	bcmMEM_SCAN.0	0.62%	0.31%
	bcmL2X.0	3.73%	3.59%
	bcmCNTR.0	1.45%	1.15%

**Table 9.** System Resource Status Fields

Field	Description
Free Memory	Displays the available Free Memory on the switch.
Alloc Memory	Displays the allocated Memory for the switch.
Task Id	Displays the Id of running tasks.
Task Name	Displays the name of the running tasks.

**Table 9.** System Resource Status Fields (continued)

Field	Description
CPU Utilization Report	Displays the Total CPU Utilization in terms of percentage. <b>Total CPU Utilization is shown in the following intervals:</b> <ul style="list-style-type: none"> <li>• 5 seconds</li> <li>• 60 seconds</li> <li>• 300 seconds</li> </ul>

To display the Resource Configuration page, click **System > Status > Resource Configuration** in the navigation menu.

**Figure 13.** System Resources Configuration

**Table 10.** System Resource Configuration Fields

Field	Description
Rising Threshold	The CPU Rising utilization threshold in percentage. A zero percent threshold indicates CPU Utilization Notification feature is disabled.
Rising Threshold Interval	The CPU Rising threshold interval in seconds. The time interval is configured in multiples of 5. A time interval of zero seconds indicates CPU Utilization Notification feature is disabled.
Falling Threshold	The CPU Falling utilization threshold in percentage. Configuration of this field is optional. If configured, the Falling threshold value must be equal to or less than the Rising threshold value. If not configured, it takes the same value as the Rising threshold.
Falling Threshold Interval	The CPU Falling threshold interval in seconds. Configuration of this field is optional. If configured, the Falling interval value must be equal to or less than the Rising interval value. If not configured, it takes the same value as the Rising interval. The time interval is configured in multiples of 5.
Free Memory Threshold	The CPU Free Memory threshold in kilobytes. A zero threshold value indicates CPU Free Memory Notification feature is disabled.

Click **Submit** to send the updated configuration to the switch. Click **Refresh** to update the page with the most current information. Click **Cancel** exit the page.

## Defining General Device Information

The **Configuration** submenu in the **System** menu contains links to pages that allow you to configure device parameters.

### System Description

After a successful login, the System Description page displays. Use this page to configure and view general device information.

To display the System Description page, click **System > Summary > Description** in the navigation menu.

**Figure 14.** System Description

Field	Description
System Description	Lenovo CE0128PB Switch, 1.2.22.7, Linux 4.4.145, U-Boot 20
System Name	hhcp-10-27-7-158 (0 to 255 alphanumeric charact)
System Location	(0 to 255 alphanumeric charact)
System Contact	(0 to 255 alphanumeric charact)
IP Address	0.0.0.0
Service Port IP Address	10.27.7.158
System Up Time	0 days, 4 hours, 40 mins, 47 secs
Current SNTP Synchronized Time	Not Synchronized

**Table 11.** System Description Fields

Field	Description
System Description	The product name of this switch.
System Name	Enter the name you want to use to identify this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
System Location	Enter the location of this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
System Contact	Enter the contact person for this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
IP Address	The IP Address assigned to the network interface. To change the IP address, see <a href="#">“IPv4 Network Connectivity Configuration”</a> on page 65.
Service Port IP Address	The IP address assigned to the service port. The service port provides remote management access to the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.
System Object ID	The base object ID for the switch's enterprise MIB.
System Up Time	Displays the number of days, hours, and minutes since the last system restart.
Current SNTP Synchronized Time	Displays currently synchronized SNTP time in UTC. If no SNTP server has been configured and the time is not synchronized, this field displays <b>Not Synchronized</b> . To specify an SNTP server, see <a href="#">“Configuring SNTP Settings”</a> on page 217.

**Table 11.** *System Description Fields (continued)*

Field	Description
MIBs Supported	Displays the list of MIBs supported by the management agent running on this switch.

## Defining System Information

1. Open the **System Description** page.
2. Define the following fields: **System Name**, **System Contact**, and **System Location**.
3. Scroll to the bottom of the page and click **Submit**.

The system parameters are applied, and the device is updated.

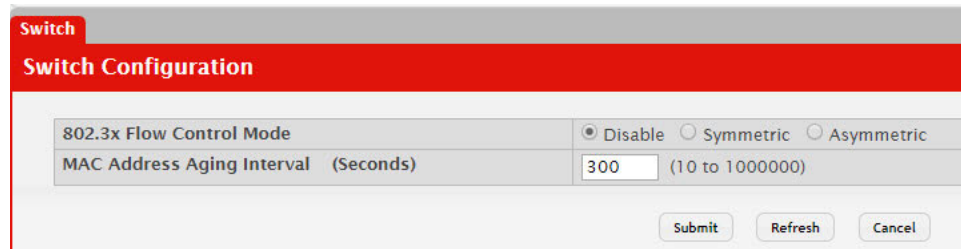
**Note:** If you want the switch to retain the new values across a power cycle, you must perform a save.

## Switch Configuration

The Switch Configuration page allows administrators with the appropriate privilege level to configure the 802.3X flow control mode and the MAC address aging timeout for the forwarding database.

To display the Switch Configuration page, click **System > Basic Configuration > Switch** in the navigation menu.

**Figure 15.** Switch 802.3x Flow Control



The screenshot shows the 'Switch Configuration' page. At the top, there is a red header with 'Switch' and 'Switch Configuration'. Below the header, there are two configuration fields:

- 802.3x Flow Control Mode:** This field has three radio button options: 'Disable' (which is selected), 'Symmetric', and 'Asymmetric'.
- MAC Address Aging Interval (Seconds):** This field is a text input box containing the value '300'. To the right of the input box, the range '(10 to 1000000)' is displayed.

At the bottom right of the configuration area, there are three buttons: 'Submit', 'Refresh', and 'Cancel'.

**Table 12.** *Switch Configuration Fields*

Field	Description
IEEE 802.3x Flow Control Mode	The 802.3x flow control mode on the switch. IEEE 802.3x flow control works by pausing a port when the port becomes oversubscribed. This allows lower-speed switches to communicate with higher-speed switches. A lower-speed or congested switch can send a PAUSE frame requesting that the peer device refrain from sending packets. Transmissions are temporarily halted to prevent buffer overflows. The options are as follows: <ul style="list-style-type: none"><li>• <b>Disable</b> – The switch does not send PAUSE frames if the port buffers become full.</li><li>• <b>Symmetric</b> – The switch can send as well as honor the PAUSE frames. The switch generates PAUSE frames towards the peer device in response to congestion at ingress and is also capable of throttling the transmit rate in response to PAUSE frames received from a peer device.</li><li>• <b>Asymmetric</b> – The switch can honor PAUSE frames it receives, but it will not generate PAUSE frames towards the peer device in response to congestion at ingress. The switch can throttle the transmit rate in response to the pause frames received from the peer.</li></ul>
MAC Address Aging Interval	The MAC address table (forwarding database) contains static entries, which never age out, and dynamically-learned entries, which are removed if they are not updated within a given time. Specify the number of seconds a dynamic address should remain in the MAC address table after it has been learned.

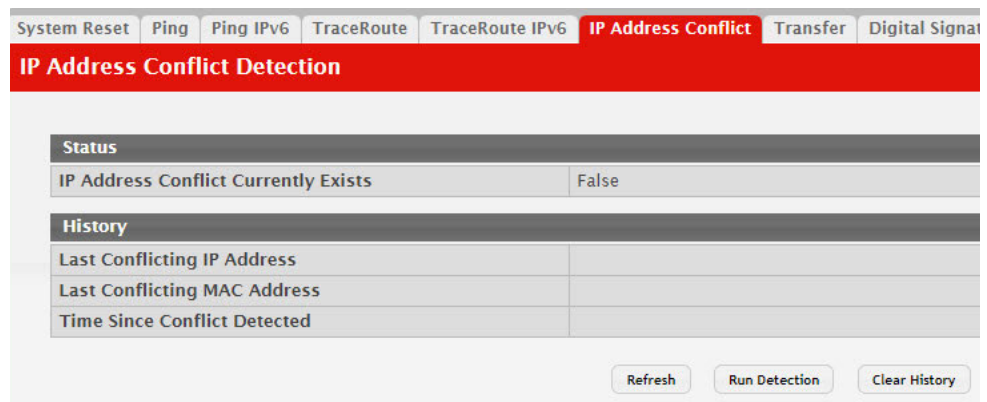
If you change the mode, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## IP Address Conflict Detection

Use the IP Address Conflict Detection page to run the IP Address Conflict Detection tool, which detects IP address conflicts for IPv4 addresses. When a conflict is detected, the switch updates the status on the page, generates an SNMP trap, and a logs a message noting the conflict.

To display the IP Address Conflict Detection page, click **System > Utilities > IP Address Conflict** in the navigation menu.

**Figure 16.** IP Address Conflict Detection





**Table 13.** IP Address Conflict Detection Fields

Field	Description
IP Address Conflict Currently Exists	Shows whether an address conflict has been detected since status was last reset.
Last Conflicting IP Address	The IP address of the interface that was last found to be conflicting. This field displays only if a conflict has been detected since the switch was last reset.
Last Conflicting MAC Address	The MAC address of the remote host associated with the IP address that was last found to be conflicting. This field displays only if a conflict has been detected since the switch was last reset.
Time Since Conflict Detected	The time elapsed (displayed in days, hours, minutes, seconds) since the last conflict was detected (provided a reset did not occur in the meantime). This field displays only if a conflict has been detected since the switch was last reset.

To run the tool and check for possible address conflicts, click **Run Conflict Detection**. If the conflict detection status is true, click **Reset Conflict Detection Status** to clear the information and run the tool again.

## IPv4 Network Connectivity Configuration

The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

The IPv4 Network Connectivity page allows you to change the IPv4 information using the Web interface. To access the page, click **System > Connectivity > IPv4** in the navigation menu.

**Figure 17.** Network Connectivity Configuration for IPv4

**Table 14.** Network Connectivity Configuration for IPv4 Fields

Field	Description
Network Configuration Protocol	Specify what the switch should do following power-up. The factory default is None. The options are as follows: <ul style="list-style-type: none"> <li>• <b>None:</b> Do not send any requests following power-up.</li> <li>• <b>Bootp:</b> Transmit a Bootp request.</li> <li>• <b>DHCP:</b> Transmit a DHCP request.</li> </ul>
DHCP Client Identifier	The DHCP Client Identifier (Option 61) is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain. The Client Identifier string will be displayed beside the check box once DHCP is enabled on the port on which the Client Identifier option is selected. This web page will need to be refreshed once this change is made.
IP Address	The IP address of the network interface. The factory default value is 0.0.0.0  <b>Note:</b> Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.
Subnet Mask	The IP subnet mask for the interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for the IP interface. The factory default value is 0.0.0.0.
MAC Address Type	Specify whether the burned-in or the locally administered MAC address should be used for in-band connectivity. The factory default is to use the burned-in MAC address
Burned-in MAC Address	This read-only field displays the MAC address that is burned-in to the network card at the factory. This MAC address is used for in-band connectivity if you choose not to configure a locally administered address.
Locally Administered MAC Address	Specifies a locally administered MAC address for in-band connectivity instead of using the burned-in universally administered MAC address. In addition to entering an address in this field, you must also set the MAC address type to locally administered. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 must have a value between x'40' and x'7F'.
Management VLAN ID	Specify the management VLAN ID of the switch. It may be configured to any value in the range of (1 to 4093). The management VLAN is used for management of the switch. This field is configurable for administrative users and read-only for other users.

If you change any of the network connectivity parameters, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Click **Renew DHCP IPv4 Address** to force the interface to release the current DHCP-assigned information and submit a request for new information.

## IPv6 Network Connectivity

IPv6 is the next generation of the Internet Protocol. With 128-bit addresses, versus 32-bit addresses for IPv4, IPv6 solves the address depletion issues seen with IPv4 and removes the requirement for Network Address Translation (NAT), which is used in IPv4 networks to reduce the number of globally unique IP addresses required for a given network. Its aggregate addresses can dramatically reduce the size of the global routing table through well known address combinations. Security is more integrated and network configuration is simplified yet more flexible.

IPv6 can coexist with IPv4. As with IPv4, IPv6 routing can be enabled on physical and VLAN interfaces. Each L3 routing interface can be used for IPv4, IPv6, or both. IP protocols running over L3 (for example, UDP and TCP) do not change with IPv6. For this reason, a single CPU stack is used for transport of both IPv4 and IPv6, and a single sockets interface provides access to both. Routing protocols are capable of computing routes for one or both IP versions.

**Note:** CLI commands are not available for all the IPv6 pages.

Use the IPv6 Network Connectivity page to configure and view IPv6 information on the network interface. The network interface is the logical interface that allows remote management of the device via any of the front-panel switch ports. To enable management of the device over an IPv6 network by using a Web browser, SNMP, Telnet, or SSH, you must first configure the device with the appropriate IPv6 information. The configuration parameters associated with the network interface do not affect the configuration of the front-panel ports through which traffic is switched or routed.

To display the page, click **System > Connectivity > IPv6** in the navigation menu.

**Figure 18.** IPv6 Network Connectivity Configuration

**Table 15.** IPv6 Network Connectivity Configuration Fields

Field	Description
IPv6 Mode	Enables or disables the IPv6 administrative mode on the network interface.
Network Configuration Protocol	Specify whether the device should attempt to acquire network information from a DHCPv6 server. Selecting <b>None</b> disables the DHCPv6 client on the network interface.

**Table 15.** IPv6 Network Connectivity Configuration Fields (continued)

Field	Description
IPv6 Stateless Address AutoConfig Mode	<p>Sets the IPv6 stateless address autoconfiguration mode on the network interface.</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b> – The network interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages.</li> <li>• <b>Disabled</b> – The network interface will not use the native IPv6 address autoconfiguration features to acquire an IPv6 address.</li> </ul>
DHCPv6 Client DUID	The client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.
IPv6 Gateway	The default gateway for the IPv6 network interface. To configure this field, click the <b>Edit</b> icon in the row. To reset the field to the default value, click the <b>Reset</b> icon in the row.
Static IPv6 Addresses	<p>Lists the manually configured static IPv6 addresses on the network interface. Use the buttons available in this table to perform the following tasks:</p> <p>To add an entry to the list, click the + (plus) button to open the Add IPv6 Address dialog and provide the following:</p> <ul style="list-style-type: none"> <li>• <b>New IPv6 Address</b> – Specify the IPv6 address to add to the interface.</li> <li>• <b>EUI Flag</b> – Select this option to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or clear the option to omit the flag.</li> </ul> <p>To delete an entry from the list, click the – (minus) button associated with the entry to remove.</p> <p>To delete all entries from the list, click the – (minus) button in the heading row.</p>
Dynamic IPv6 Addresses	Lists the IPv6 addresses on the network interface that have been dynamically configured through IPv6 autoconfiguration or DHCPv6.
Default IPv6 Routers	Lists the IPv6 address of each default router that has been automatically configured through IPv6 router discovery.

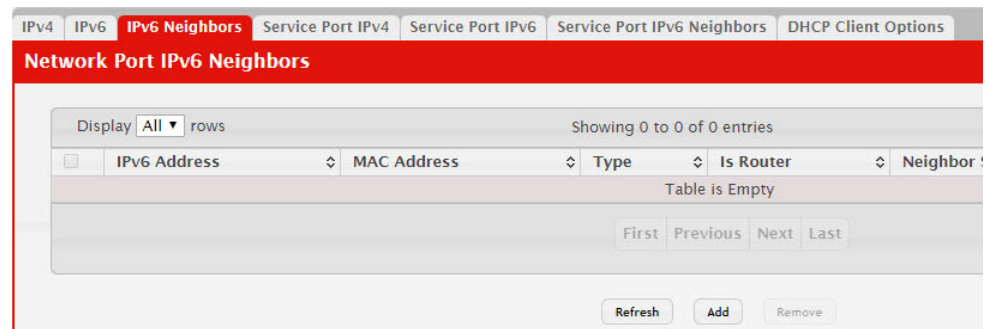
Click **Refresh** to update the information on the screen.

## Network Port IPv6 Neighbors

This page provides information about IPv6 neighbors the device has discovered through the network interface by using the Neighbor Discovery Protocol (NDP) and the manually configured static network port IPv6 neighbors.

To access this page, click **System > Connectivity > IPv6 Neighbors**.

**Figure 19.** Network Port IPv6 Neighbors



**Table 16.** Network Port IPv6 Neighbors Fields

Field	Description
IPv6 Address	Displays the IP address of the neighbor.
MAC Address	Displays the MAC address of the neighbor.
Type	The type of the neighbor entry, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Static</b>—The neighbor entry is manually configured.</li> <li>• <b>Dynamic</b>—The neighbor entry is dynamically resolved.</li> <li>• <b>Local</b>—The neighbor entry is a local entry.</li> <li>• <b>Other</b>—The neighbor entry is an unknown entry.</li> </ul>
IS Router	Indicates whether the neighbor is a router. If the neighbor is a router, the value is TRUE. If the neighbor is not a router, the value is FALSE.

**Table 16.** Network Port IPv6 Neighbors Fields (continued)

Field	Description
Neighbor State	<p>Specifies the state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> <li>• <b>Reachable</b>—Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.</li> <li>• <b>Stale</b>—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.</li> <li>• <b>Delay</b>—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.</li> <li>• <b>Probe</b>—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.</li> <li>• <b>Unknown</b>—The reachability status cannot be determined.</li> </ul>
Last Updated	Displays the time since the address was confirmed to be reachable.

Use the buttons to perform the following tasks:

- To add network port static IPv6 neighbor entry, click **Add** and configure the desired settings.
- To remove network port static IPv6 neighbor entries, select each static neighbor entry to remove and click **Remove**.

After you click Add or Edit, a window opens and allows you to configure Network Port IPv6 Neighbor settings.

You can configure the **IPv6 Address** and the **MAC Address**.

**Figure 20.** Add Network Port IPv6 Neighbor

The screenshot shows a web-based configuration window titled "Add Network Port IPv6 Neighbor". The window contains two input fields: "IPv6 Address" with a placeholder "(x:x:x:x:x:x:x)" and "MAC Address" with a placeholder "(xx:xx:xx:xx:xx:xx)". At the bottom right of the window, there are two buttons: "Submit" and "Cancel".

**Table 17.** Add Network Port IPv6 Neighbor Fields

Field	Description
IPv6 Address	Use this field to enter the IP address of the neighbor.
MAC Address	Use this field to enter the MAC address of the neighbor.

## Service Port IPv4

Some platforms have a built-in service port that can serve as a dedicated network management interface. For systems that have the service port, the Service Port IPv4 Configuration page allows you to configure network information for the switch.

To access the Service Port Configuration page, click **System > Connectivity > Service Port IPv4** in the navigation menu.

**Figure 21.** Service Port IPv4 Configuration

**Table 18.** Service Port IPv4 Configuration Fields

Field	Description
IPv4 Fields:	These display IPv4 configuration information.
Service Port Configuration Protocol	Specify what the switch should do following power-up. The factory default is None. The options are as follows: <ul style="list-style-type: none"> <li>• <b>None:</b> Do not send any requests following power-up.</li> <li>• <b>BootP:</b> Transmit a BootP request.</li> <li>• <b>DHCP:</b> Transmit a DHCP request.</li> </ul>
IP Address	The IP address of the network interface. The factory default value is 0.0.0.0 <b>Note:</b> Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.
Subnet Mask	The IP subnet mask for the interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for the IP interface. The factory default value is 0.0.0.0.

**Table 18.** *Service Port IPv4 Configuration Fields (continued)*

Field	Description
Burned-in MAC Address	This read-only field displays the MAC address that is burned-in to the network card at the factory. This MAC address is used for in-band connectivity if you choose not to configure a locally administered address.

To renew the IPv4 address learned from a DHCP server on the service port, click **Renew DHCP IPv4 Address**.

If you change any of the parameters on this page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Service Port IPv6

Use this page to configure IPv6 network information on the service port. The service port is a dedicated Ethernet port for out-of-band management of the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.

To access the Service Port Configuration page, click **System > Connectivity > Service Port IPv6** in the navigation menu.

**Figure 22.** Service Port IPv6 Configuration

**Table 19.** *Service Port IPv6 Configuration Fields*

Field	Description
IPv6 Mode	Enables or disables IPv6 mode on the interface.



**Table 19.** *Service Port IPv6 Configuration Fields (continued)*

Field	Description
Service Port Configuration Protocol	Specify whether the device should attempt to acquire network information from a DHCPv6 server. Selecting None disables the DHCPv6 client on the service port.
IPv6 Stateless Address AutoConfig Mode	Sets the IPv6 stateless address autoconfiguration mode on the service port. <ul style="list-style-type: none"> <li>• <b>Enabled</b> – The service port can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages.</li> <li>• <b>Disabled</b> – The service port will not use the native IPv6 address autoconfiguration features to acquire an IPv6 address.</li> </ul>
DHCPv6 Client DUID	The client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.
Static IPv6 Addresses	Lists the manually configured static IPv6 addresses on the service port interface. Use the buttons available in this table to perform the following tasks: <ul style="list-style-type: none"> <li>• To add an entry to the list, click the + (plus) button to open the Add IPv6 Address dialog and provide the following: <ul style="list-style-type: none"> <li>– New IPv6 Address – Specify the IPv6 address to add to the service port interface.</li> <li>– EUI Flag – Select this option to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or clear the option to omit the flag.</li> </ul> </li> <li>• To delete an entry from the list, click the – (minus) button associated with the entry to remove.</li> <li>• To delete all entries from the list, click the – (minus) button in the heading row.</li> </ul>
Dynamic IPv6 Addresses	Lists the IPv6 addresses on the service port interface that have been dynamically configured through IPv6 autoconfiguration or DHCPv6.
Default IPv6 Routers	Lists the IPv6 address of each default router that has been automatically configured through IPv6 router discovery.

To renew the IPv6 address learned from a DHCP server on the service port, click **Renew DHCP IPv6 Address**.

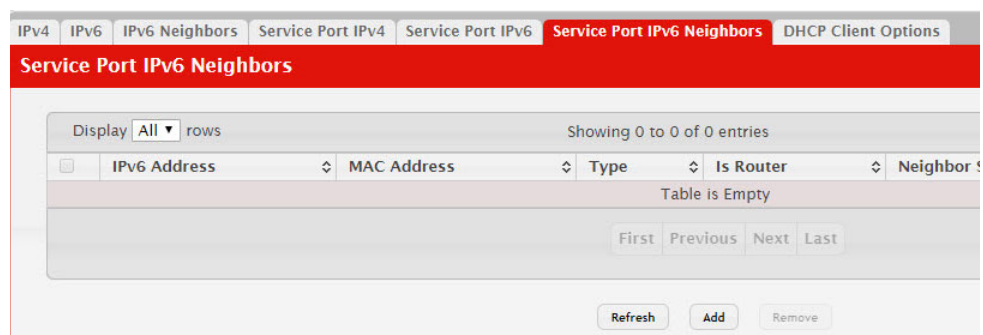
If you change any of the parameters on this page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Service Port IPv6 Neighbors

This page provides information about IPv6 neighbors the device has discovered through the service port by using the Neighbor Discovery Protocol (NDP). The manually configured static service port IPv6 neighbors are also displayed.

To display the page, click **System > Connectivity > Service Port IPv6 Neighbors**

**Figure 23.** Service Port IPv6 Neighbors



**Table 20.** Service Port IPv6 Neighbors Fields

Field	Description
IPv6 Addresses	Displays the IP address of the neighbor.
MAC Address	Displays the MAC address of the neighbor.
Type	The type of the neighbor entry, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Static</b>—The neighbor entry is manually configured.</li> <li>• <b>Dynamic</b>—The neighbor entry is dynamically resolved.</li> <li>• <b>Local</b>—The neighbor entry is a local entry.</li> <li>• <b>Other</b>—The neighbor entry is an unknown entry.</li> </ul>
Is Router	Indicates whether the neighbor is a router. If the neighbor is a router, the value is TRUE. If the neighbor is not a router, the value is FALSE.
Neighbor State	Specifies the state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache: <ul style="list-style-type: none"> <li>• <b>Reachable</b>—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.</li> <li>• <b>Stale</b>—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.</li> <li>• <b>Delay</b>—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.</li> <li>• <b>Probe</b>—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.</li> <li>• <b>Unknown</b>—The reachability status cannot be determined.</li> </ul>
Last Updated	Displays the time since the address was confirmed to be reachable.

Use the buttons to perform the following tasks:

- To add service port static IPv6 neighbor entry, click **Add** and configure the desired settings.
- To remove service port static IPv6 neighbor entries, select each static neighbor entry to remove and click **Remove**.

After you click Add or Edit, a window opens and allows you to configure Service Port IPv6 Neighbor settings.

You can configure the **IPv6 Address** and the **MAC Address**.

**Figure 24.** Add Service Port IPv6 Neighbor

**Table 21.** Add Service Port IPv6 Neighbor Fields

Field	Description
IPv6 Address	Use this field to enter the IP address of the neighbor.
MAC Address	Use this field to enter the MAC address of the neighbor.

## DHCP Client Options

Use the DHCP Client Options page to configure DHCP client settings on the system.

To access the DHCP Client Options page, click **System > Connectivity > DHCP Client Options** in the navigation menu.

**Figure 25.** DHCP Client Options

**Table 22.** DHCP Client Options Fields

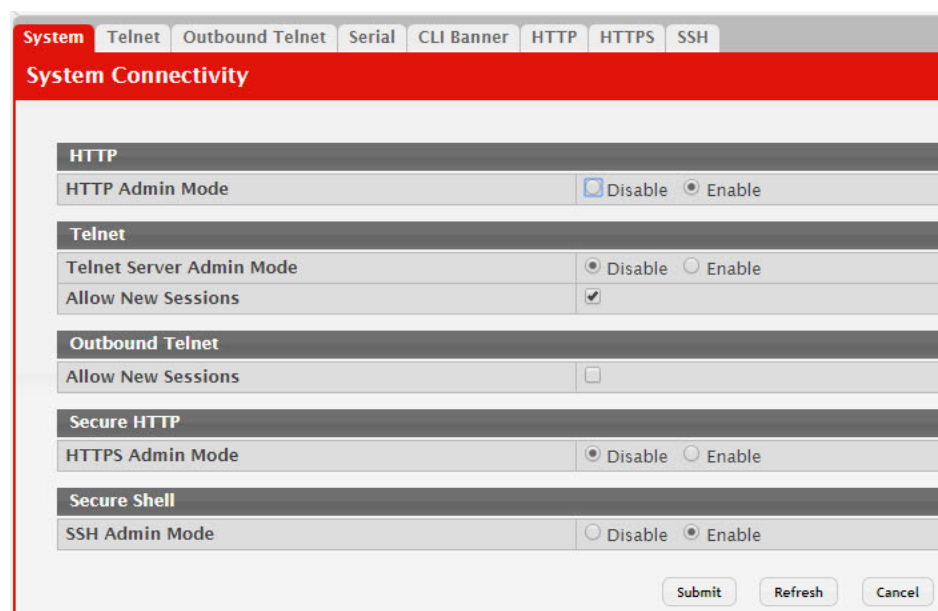
Field	Description
DHCP Vendor Class ID Mode	Enables/Disables the vendor class identifier mode.
DHCP Vendor Class ID String	The string added to DHCP requests as Option-60. i.e., Vendor Class Identifier option.

## System Connectivity

Use the System Connectivity page to control access to the management interface by administratively enabling or disabling various access methods.

To display the System Connectivity page, click **System > Management Access > System** in the navigation menu.

**Figure 26.** System Connectivity Configuration



**Table 23.** System Connectivity Configuration Fields

Field	Description
HTTP Admin Mode	Enables or disables the HTTP administrative mode. When this mode is enabled, the device management interface can be accessed through a web browser using the HTTP protocol.
Telnet Server Admin Mode	Enables or disables the telnet administrative mode. When this mode is enabled, the device command-line interface (CLI) can be accessed through the telnet port. Disabling this mode disconnects all existing telnet connections and shuts down the telnet port in the device.
Telnet — Allow New Sessions	Enables or disables new telnet sessions. When this option is disabled, the system does not accept any new telnet sessions, but existing telnet sessions are unaffected.

**Table 23.** *System Connectivity Configuration Fields (continued)*

Field	Description
Outbound Telnet – Allow New Sessions	Enables or disables new outbound telnet sessions. When this option is disabled, initiating telnet sessions from the system is not allowed.
HTTPS Admin Mode	Enables or disables the administrative mode of secure HTTP. When this mode is enabled, the device management interface can be accessed through a web browser using the HTTPS protocol.
SSH Admin Mode	Enables or disables the administrative mode of SSH. When this mode is disabled, all existing SSH connections remain connected until timed-out or logged out, but new SSH connections cannot be established.

If you change any of the parameters, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Telnet Session

Telnet is a terminal emulation TCP/IP protocol. ASCII terminals can be virtually connected to the local device through a TCP/IP protocol network. Telnet is an alternative to a local login terminal where a remote login is required.

The switch supports up to five simultaneous telnet sessions. All CLI commands can be used over a telnet session.

The Telnet Session Configuration page allows you to control inbound telnet settings on the switch. Inbound telnet sessions originate on a remote system and allow a user on that system to connect to the switch CLI.

To display the Telnet Session Configuration page, click **System > Management Access > Telnet** in the navigation menu.

**Figure 27.** Telnet Session Configuration

**Table 24.** *Telnet Session Configuration Fields*

Field	Description
Admin Mode	Enables or disables the telnet administrative mode. When enabled, the device may be accessed through the telnet port (23). Disabling this mode value disconnects all existing telnet connections and shuts down the telnet port in the device.

**Table 24.** *Telnet Session Configuration Fields (continued)*

Field	Description
Telnet Port	The TCP port number on which the telnet server listens for requests. Existing telnet login sessions are not affected by a change in this value, although establishment of any new telnet sessions must use the new port number. <b>Note:</b> Before changing this value, check your system, e.g., using netstat, to make sure the desired port number is not currently being used by any other service.
Session Timeout (Minutes)	Specify how many minutes of inactivity should occur on a telnet session before the session is logged off. You may enter any number from 1 to 160. The factory default is 5. <b>Note:</b> When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.
Maximum Number of Sessions	From the drop-down menu, select how many simultaneous telnet sessions to allow. The maximum is 4, which is also the factory default. A value of 0 indicates that no outbound Telnet session can be established.
Allow New Sessions	Controls whether to allow new telnet sessions: <ul style="list-style-type: none"><li>• <b>Yes:</b> Permits new telnet sessions until the maximum number allowed is reached.</li><li>• <b>No:</b> New telnet sessions will not be allowed, but existing sessions are not disconnected.</li></ul>

If you change any of the telnet parameters, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Outbound Telnet Configuration

This page displays the current value of the outbound Telnet settings on the device. An outbound Telnet session is a Telnet session initiated from the CLI of the device to the Telnet client on a remote device.

To display the Outbound Telnet Configuration page, click **System > Management Access > Outbound Telnet** in the navigation menu.

**Figure 28.** Outbound Telnet Configuration

Field	Value
Allow New Sessions	<input type="checkbox"/>
Maximum Number of Sessions	5 (0 to 5)
Session Timeout (Minutes)	5 (1 to 160)

**Table 25.** *Outbound Telnet Configuration Fields*

Field	Description
Allow New Sessions	Controls whether new outbound Telnet sessions are allowed. Setting this value to Disable disallows any new outbound Telnet sessions from starting (although existing Telnet sessions are unaffected).
Maximum Number of Sessions	The maximum number of allowed outbound Telnet sessions from the device simultaneously.
Session Timeout	Outbound telnet session inactivity timeout value, in minutes. An outbound Telnet session is closed automatically if there is no activity within the configured amount of time.

If you change any of the outbound telnet parameters, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Serial Port

The Serial Port Configuration page allows you to change the switch’s serial port settings. In order for a terminal or terminal emulator to communicate with the switch, the serial port settings on both devices must be the same. Some settings on the switch cannot be changed.

To view or configure the serial port settings on the switch, click **System > Management Access > Serial** in the navigation menu.

**Figure 29.** Serial Port

**Table 26.** *Serial Port Fields*

Field	Description
Serial Port Time Out (Minutes)	Indicates how many minutes of inactivity should occur on a serial port connection before the switch closes the connection. Enter a number between 0 and 160. The factory default is 5. Entering 0 disables the timeout.
Baud Rate (bps)	Select the default baud rate for the serial port connection from the menu. The factory default is 115200 baud
Character Size (Bits)	The number of bits in a character. This is always 8.

**Table 26.** *Serial Port Fields (continued)*

Field	Description
Parity	The parity method used on the serial port. It is always None.
Stop Bits	The number of stop bits per character. Its is always 1.
Flow Control	Whether hardware flow control is enabled or disabled. It is always disabled.

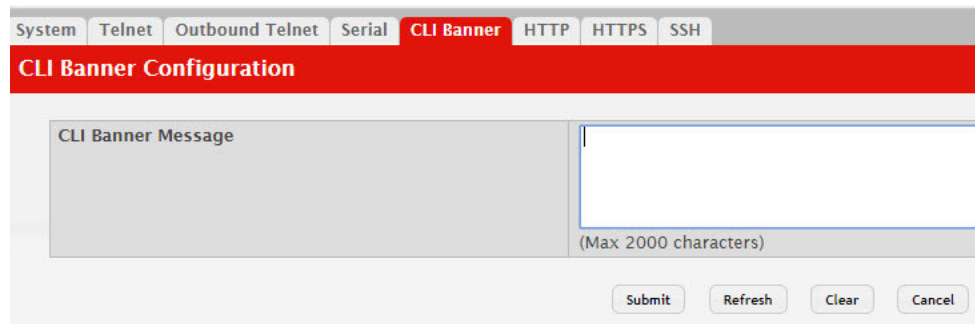
If you change any data, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## CLI Banner Configuration

Use the CLI Banner Configuration page to configure a message that appears before the user prompt as a Pre-login banner. The message configured shows up on Telnet, SSH and Console connections.

To access the CLI Banner Configuration page, click **System > Management Access > CLI Banner** in the navigation menu.

**Figure 30.** CLI Banner Configuration



**Table 27.** *CLI Banner Configuration Fields*

Field	Description
CLI Banner Message	Text area for creating, viewing, or updating the CLI banner message. To to create the CLI banner message, type the desired message in the text area. If you reach the end of the line, the text wraps to the next line. The line might not wrap at the same location in the CLI. To create a line break (carriage return) in the message, press the Enter key on the keyboard. The line break in the text area will be at the same location in the banner message when viewed through the CLI.
Clear (Button)	Clears the CLI banner message from the device. After you click Clear, you must confirm the action. You can also clear the CLI banner by deleting the text in the CLI Banner Message field and clicking <b>Submit</b> .

Click **Submit** to apply the changes to the system. You must perform a save to make the changes persist across a reboot.



## HTTP Configuration

Use the HTTP Configuration page to configure the HTTP server settings on the system.

To access the HTTP Configuration page, click **System > Management Access > HTTP** in the navigation menu.

**Figure 31.** HTTP Configuration

**Table 28.** HTTP Configuration Fields

Field	Description
HTTP Admin Mode	This select field is used to Enable or Disable the Administrative Mode of HTTP. The currently configured value is shown when the web page is displayed. The default value is Disable. If you disable the HTTP admin mode, access to the web interface is limited to secure HTTP, which is enabled by default.
HTTP Port	The TCP port number on which the HTTP server listens for requests. Existing HTTP login sessions are closed whenever this value is changed. All new HTTP sessions must use the new port number. <b>Note:</b> Before changing this value, check your system to make sure the desired port number is not currently being used by any other service.
HTTP Session Soft Timeout	This field is used to set the inactivity timeout for HTTP sessions. The value must be in the range of (1 to 60) minutes. A value of zero corresponds to an infinite timeout. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.
HTTP Session Hard Timeout	This field is used to set the hard timeout for HTTP sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (1 to 168) hours. A value of zero corresponds to an infinite timeout. The default value is 24 hours. The currently configured value is shown when the web page is displayed.
Maximum Number of HTTP Sessions	This field is used to set the maximum allowable number of HTTP sessions. The value must be in the range of (0 to 16). The default value is 16. The currently configured value is shown when the web page is displayed.

If you make changes to the page, click **Submit** to apply the changes to the system.

## HTTPS Configuration

Use this page to view and modify the Secure HTTP (HTTPS) settings on the device. HTTPS increases the security of web-based management by encrypting communication between the administrative system and the device.




To access the HTTPS Configuration page, click **System > Management Access > HTTPS** in the navigation menu.

**Figure 32.** HTTPS Configuration

**Table 29.** HTTPS Configuration Fields

Field	Description
HTTPS Admin Mode	Enables or disables the HTTPS administrative mode. When this mode is enabled, the device can be accessed through a web browser using the HTTPS protocol.
TLS Version 1	Enables or disables Transport Layer Security Version 1.0. When this option is enabled, communication between the web browser on the administrative system and the web server on the device is sent through TLS 1.0.
SSL Version 3	Enables or disables Secure Sockets Layer Version 3.0. When this option is enabled, communication between the web browser on the administrative system and the web server on the device is sent through SSL 3.0. SSL must be administratively disabled while downloading an SSL certificate file from a remote server to the device.
HTTPS Port	The TCP port number that HTTPS uses.
HTTPS Session Soft Time Out (Minutes)	HTTPS session inactivity timeout value. A logged-in user that does not exhibit any HTTPS activity for this amount of time is automatically logged out of the HTTPS session.
HTTPS Session Hard Time Out (Hours)	HTTPS session hard timeout value. A user connected to the device via an HTTPS session is automatically logged out after this amount of time regardless of the amount of HTTPS activity that occurs.
Maximum Number of HTTPS Sessions	The maximum number of HTTPS sessions that can be connected to the device simultaneously.

**Table 29.** *HTTPS Configuration Fields (continued)*

Field	Description
Certificate Status	The status of the SSL certificate generation process. <ul style="list-style-type: none"> <li>• <b>Present</b> – The certificate has been generated and is present on the device</li> <li>• <b>Absent</b> – Certificate is not available on the device</li> <li>• <b>Generation In Progress</b> – An SSL certificate is currently being generated.</li> </ul>
Download Certificates (Button) 	Allows you to download an SSL certificate file from a remote system to the device. <b>Note:</b> To download SSL certificate files, SSL must be administratively disabled.
Generate Certificate (Button) 	Generates an SSL certificate to use for secure communication between the web browser and the embedded web server on the device.
Delete Certificates (Button) 	Deletes the SSL certificate. This button is available only if an SSL certificate is present on the device.

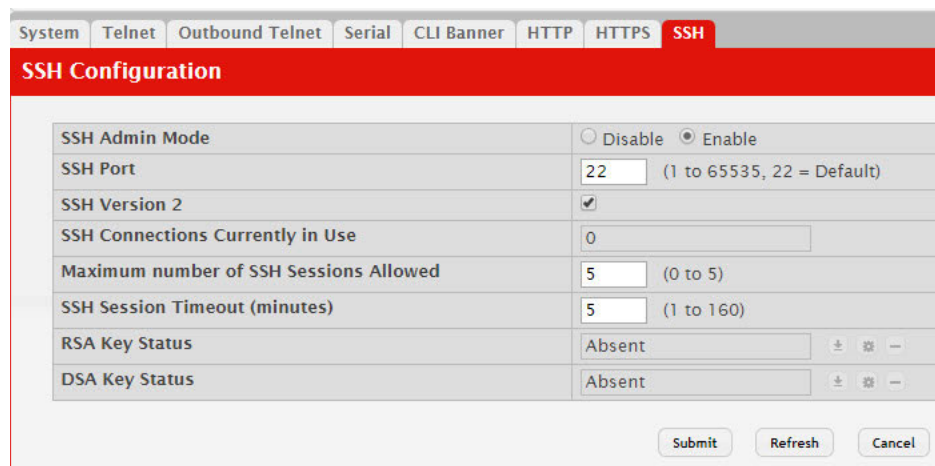
If you make changes to the page, click **Submit** to apply the changes to the system.

## SSH Configuration




Use this page to view and modify the Secure Shell (SSH) server settings on the device. SSH is a network protocol that enables access to the CLI management interface by using an SSH client on a remote administrative system. SSH is a more secure access method than Telnet because it encrypts communication between the administrative system and the device. This page also allows you to download or generate SSH host keys for secure CLI-based management.

To access the SSH Configuration page, click **System > Management Access > SSH** in the navigation menu.

**Figure 33.** SSH Configuration



**Table 30.** *SSH Configuration Fields*

Field	Description
SSH Admin Mode	Enables or disables the SSH server administrative mode. When this mode is enabled, the device can be accessed by using an SSH client on a remote system.
SSH Port	The TCP port number on which the SSH server listens for requests. Existing SSH login sessions are not affected by a change in this value, although establishment of any new SSH sessions must use the new port number. <b>Note:</b> Before changing this value, check your system, e.g., using netstat, to make sure the desired port number is not currently being used by any other service.
SSH Version 2	When this option is selected, the SSH server on the device can accept connections from an SSH client using SSH-2 protocol. If the option is clear, the device does not allow connections from clients using the SSH-2 protocol. <b>Note:</b> This is the only supported SSH version and is enabled by default. Clearing this option is not permitted.
SSH Connections Currently in Use	The number of active SSH sessions between remote SSH clients and the SSH server on the device.
Maximum number of SSH Sessions Allowed	The maximum number of SSH sessions that may be connected to the device simultaneously.
SSH Session Timeout (minutes)	The SSH session inactivity timeout value. A connected user that does not exhibit any SSH activity for this amount of time is automatically disconnected from the device.
RSA Key Status	The status of the SSH-1 Rivest-Shamir-Adleman (RSA) key file or SSH-2 RSA key file (PEM Encoded) on the device, which might be Present, Absent, or Generation in Progress. <b>Note:</b> CE0128XB/CE0152XB supports only SSHv2. SSH1-RSA keys can be downloaded, but they cannot be used.
DSA Key Status	The status of the SSH-2 Digital Signature Algorithm (DSA) key file (PEM Encoded) on the device, which might be Present, Absent, or Generation in Progress.
Download Certificates (Button) 	Use this button to download an SSH-1 RSA, SSH-2 RSA, or SSH-2 DSA key file from a remote system to the device. After you click the button, a Download Certificate window opens. Select the file type to download, browse to the location on the remote system, and select the file to upload. Then, click Begin Transfer. The Status field provides information about the file transfer. <b>Note:</b> CE0128XB/CE0152XB supports only SSHv2. SSH1-RSA keys can be downloaded, but they cannot be used.
Generate Certificate (Button) 	Use this button to manually generate an RSA key or DSA key on the device.
Delete Certificates (Button) 	Use this button to delete an RSA key or DSA key that has been downloaded to the device or manually generated on the device.

If you make changes to the page, click **Submit** to apply the changes to the system.

## Management Access Control and Administration List

Use this page to create and configure a management access list to help secure access to the switch management features. The Management Access Control and Administration List (MACAL) feature is used to ensure that only known and trusted devices are allowed to remotely manage the switch via TCP/IP.

MACALs can be applied only to in-band ports and cannot be applied to the service port.

To access the Management Access List Configuration page, click **System > Management Security > Access Profile** in the navigation menu.

**Figure 34.** Management Access List Configuration

This Management Access List Configuration page provides the capability to add, edit, and remove MACALs.

**Note:** Profile rules cannot be added or modified when a profile is active. To add or edit a profile, the Active Profile field must be set to None.

- To add a new MACAL, click **Add**. The Add Profile Rule dialog box opens. Specify the rule criteria in the available fields.
- To edit an existing rule, select the appropriate check box or click the row to select the account and click **Edit**. The Edit Profile Rule box opens. Modify the rule criteria as needed.
- To remove a Profile Rule, select one or more table entries and click **Remove** to delete the selected entries.

**Table 31.** User Accounts Fields

Field	Description
Access Profile	Profile name for the Management Access Control list. One user defined Access Profile can be created.
Active Profile	Currently enabled profile name.
Packets Filtered	The number of packets filtered due to matching a rule in the MACAL.

**Table 31.** *User Accounts Fields (continued)*

Field	Description
Interface	The port/interface or trunk ID.
Management Method	The types of action will be taken on access control list. <ul style="list-style-type: none"><li>• Permit: To allow conditions for the management access list.</li><li>• Deny: To deny conditions for the management access list.</li></ul> In the Add or Edit Profile Rule dialog, this is specified by using the Action field.
Source IP Address	IP Address of device which needs to permit or deny in the management access list.
Subnet Mask	Specifies the network mask of the source IP address.
VLAN	The VLAN ID.
Port Channel	Port channels, also known as Link Aggregation Groups (LAGs), allow one or more full-duplex Ethernet links of the same speed to be aggregated together.
Service	The type of service to permit or deny: <ul style="list-style-type: none"><li>• ANY</li><li>• TELNET</li><li>• HTTP</li><li>• HTTPS</li><li>• SNMP</li><li>• SSH</li><li>• TFTP</li><li>• SNTP</li></ul>
Priority	Priority for the rule. Duplicates are not allowed.

## User Accounts

By default, the switch contains two user accounts:

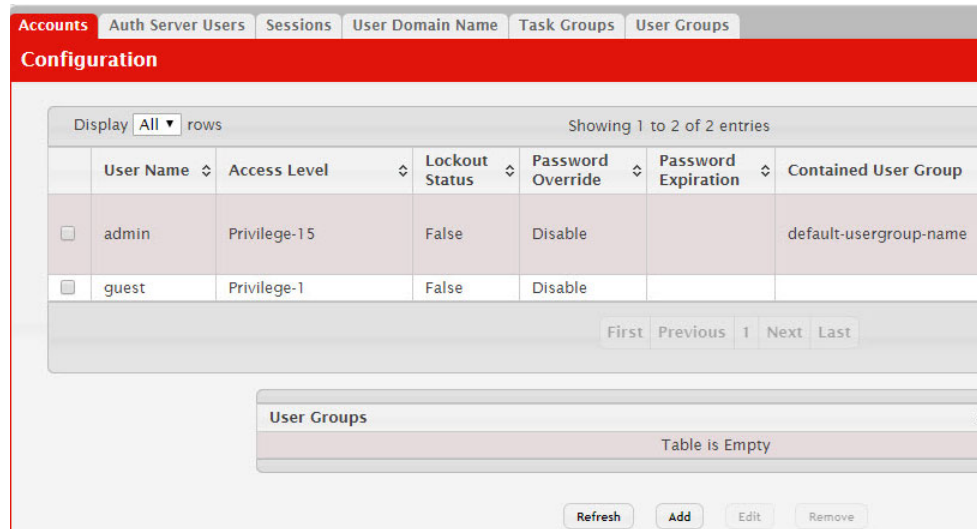
- admin, with 'Read/Write' privileges. The user can view and modify the configuration.
- guest, with 'Read' privileges. The user can view the configuration but cannot modify any fields.

Both of these accounts use the admin password by default. The names are not case sensitive.

If you log on to the switch with the user account that Read/Write privileges (i.e., as admin), you can use the **User Accounts** page to assign passwords and set security parameters for the default accounts. You can also add up to five accounts. You can delete all accounts except for the admin account.

To access the User Accounts page, click **System > Users > Accounts** in the navigation menu.

**Figure 35.** User Accounts



This User Accounts page provides the capability to add, edit, and remove user accounts.

- To add a user, click **Add**. The Add new user dialog box opens. Specify the new account information in the available fields.
- To edit an existing user, select the appropriate check box or click the row to select the account and click **Edit**. The Edit existing user dialog box opens. Modify the account information as needed.
- To remove a user, select one or more table entries and click **Remove** to delete the selected entries.

**Table 32.** User Accounts Fields

Field	Description
User Name	Enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) User names are up to 32 alphanumeric characters in length and are not case sensitive. Valid characters include all the alphanumeric characters and the dash ('-') and underscore ('_') characters. User name <i>default</i> is not valid.
Password	Enter the optional new or changed password for the account. It will not display as it is typed, only asterisks (*) or dots(.) will show based on the browser used. Passwords must be greater than eight characters and can be up to 64 characters in length, and are case sensitive.
Confirm	Enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (*)
Access Level	Indicates the access or privilege level for this user. The options are: <ul style="list-style-type: none"> <li>• <b>Privilege-15</b> - The user can view and modify the configuration.</li> <li>• <b>Privilege-1</b> - The user can view the configuration but cannot modify any fields.</li> <li>• <b>Privilege-0</b> - The user exists but is not permitted to log on to the device.</li> </ul>

**Table 32.** *User Accounts Fields (continued)*

Field	Description
Lockout Status	Provides the current lockout status for this user. If the lockout status is True, the user cannot access the management interface even if the correct username and password are provided. The user has been locked out of the system due to a failure to supply the correct password within the configured number of login attempts.
Password Override	Identifies the password override complexity status for this user. <ul style="list-style-type: none"><li>• <b>Enable</b> - The system does not check the strength of the password.</li><li>• <b>Disable</b> - When configuring a password, it is checked against the Strength Check rules configured for passwords.</li></ul>
Password Expiration	Indicates the date when this user's current password will expire. This is determined by the date the password was created and the number of days specified in the aging Password Aging setting on the Passwords > Password Rules page.
Contained User Group	The associated user groups for the user.
Operational Permissions	The operational task permissions for the user. In addition to the fields described above, the User Groups table will be populated when you click on each row. To configure this user group, click the Add icon in the header row. To remove the user group, click the Reset icon in the row.

## Adding a User Account

Use the following procedures to add a user account.

1. From the **User** menu, select **Add**.  
The screen refreshes.
2. Enter a username and password for the new user, then re-enter the password in the **Confirm Password** field.
3. The **Password Strength** field shows the status of the password strength check.
4. Select the **Encrypt Password** option to encrypt the password before it is stored on the device.
5. Click **Submit** to update the switch with the values on this screen.  
If you want the switch to retain the new values across a power cycle, you must perform a save.

## Changing User Account Information

You cannot add or delete the default "admin" Read/Write user, but you can change the password. To change the password for an existing account or to overwrite the username on an existing account, use the following procedures.

1. From the **User** menu, select the user to change.  
The screen refreshes.
2. Click **Edit** to change the user settings.  
This button is only visible when you have selected a user account with 'Read Only' access. You cannot delete the default admin 'Read/Write' user.



3. To change the password, delete any asterisks (\*) in the **Password** and **Confirm Password** fields, and then enter and confirm the new password.
4. Click **Submit** to update the switch with the values on this screen.

If you want the switch to retain the new values across a power cycle, you must perform a save.

## Removing a User Account

Use the following procedures to remove any of the Read Only user accounts.

1. From the **User** menu, select the user to remove.

The screen refreshes.

2. Click **Remove** to delete the user.

This button is only visible when you have selected a user account with 'Read/Write' access. You cannot remove the default admin 'Read/Write' user.

If you want the switch to retain the new values across a power cycle, you must perform a save.

## Authentication Server Users

To access the Authentication Server Users page, click **System > Users > Auth Server Users** in the navigation menu.

Use the Auth Server Users page to add and remove users from the local authentication server user database. For some security features, such as IEEE 802.1X port-based authentication, you can configure the device to use the locally stored list of usernames and passwords to provide authentication to users instead of using an external authentication server.

**Note:** The preconfigured users, admin and guest, are assigned to a pre-configured list named defaultList, which you cannot delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list.

You can create a text file that contains a list of IAS users to add to the database and then download the file to the switch. The following script is an example of an IAS user text file that contains three users:

```
configure
aaa ias-user username client-1
password my-password1
exit
aaa ias-user username client-2
password aa5c6c251fe374d5e306c62496c3bcf6 encrypted
exit
aaa ias-user username client-3
password 1f3ccb1157
exit
```

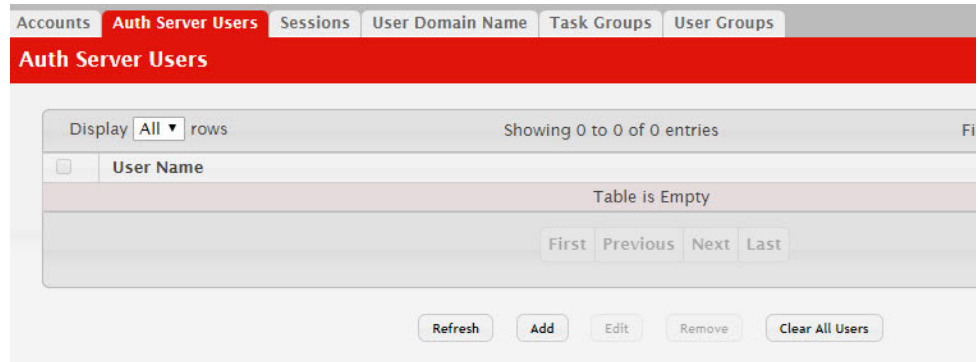
After the download completes, client-1, client-2, and client-3 are added to the IAS database. The password for client-2 is encrypted.

When Dot1x authentication is enabled on the ports and the authentication method is LOCAL, port access is allowed only to users in this database that provide the correct name and password.

Use the buttons to perform the following tasks:

- To add a new authentication server user, click **Add**.
- To add a user to the local authentication server database, click **Add** and complete the required information.
- To change the password information for an existing user, select the user to update and click **Edit**.
- To delete a user from the database, select each user to delete and click **Remove**.
- To remove all users from the database, click **Clear All Users**.

**Figure 36.** Auth Server Users



When **Add** is selected from **Auth Server Users** list, the **Add New User** page displays.

**Figure 37.** Add New User

**Table 33.** Add New Authentication User Fields

Field	Description
User Name	A unique name used to identify this user account. You configure the User Name when you add a new user.

**Table 33.** Add New Authentication User Fields (continued)

Field	Description
Password Required	Select this option to indicate that the user must enter a password to be authenticated. If this option is clear, the user is required only to enter a valid user name.
Password	Specify the password to associate with the user name (if required).
Confirm	Re-enter the password to confirm the entry.
Encrypted	Select this option to encrypt the password before it is stored on the device.

Click **Submit** to apply the changes to the system. You must perform a save to make the changes persist across a reboot.

Click **Clear All Users** to remove all users from the database.

## Logged in Sessions

The Sessions page identifies the users that are logged in to the management interface of the device. The page also provides information about their connections.

To access the **Login Session** page, click **System > Users > Sessions** in the navigation menu.

**Figure 38.** Logged in Sessions

ID	User Name	Connection From	Idle Time	Session Time
14	admin	10.27.64.153	00:00:00	00:51:59

**Table 34.** Logged in Sessions Fields

Field	Description
ID	The unique ID of the session.
User Name	The name that identifies the user account.
Connection From	Identifies the administrative system that is the source of the connection. For remote connections, this field shows the IP address of the administrative system. For local connections through the console port, this field shows the communication standard for the serial connection.
Idle Time	Shows the amount of time in hours, minutes, and seconds that the logged-on user has been inactive.
Session Time	Shows the amount of time in hours, minutes, and seconds since the user logged onto the system.

**Table 34.** *Logged in Sessions Fields (continued)*

Field	Description
Session Type	Shows the type of session, which can be Telnet, Serial, SSH, HTTP, or HTTPS.

Click **Refresh** to update the information on the screen.

## User Domain Name

Use this page to configure the domain name to send to the authentication server, along with the user name and password, to authenticate a user attempting to access the device management interface. Domain name authentication is supported when user authentication is performed by a RADIUS server or TACACS+ server.

To access the User Domain Name page, click **System > Users > User Domain Name** in the navigation menu.

**Figure 39.** User Domain Name

**Table 35.** *User Domain Name Fields*

Field	Description
User Domain Name Mode	The administrative mode of domain name authentication on the device. When enabled, the domain name is included when the user name and password are sent to the authentication server. The domain name can be input by the user in the User Name field on the login screen in a domain-name\username format, or the domain name can be specified in the Domain Name field.
Domain Name	The domain name to send to the authentication server when the user does not provide one in the User Name field during logon. When only the username is provided, the device sends the username as domain-name\username, where domain-name is the string configured in this field. To configure the domain name, click the Edit icon and specify the desired string. To reset the field to its default value, click the Reset icon and confirm the action.

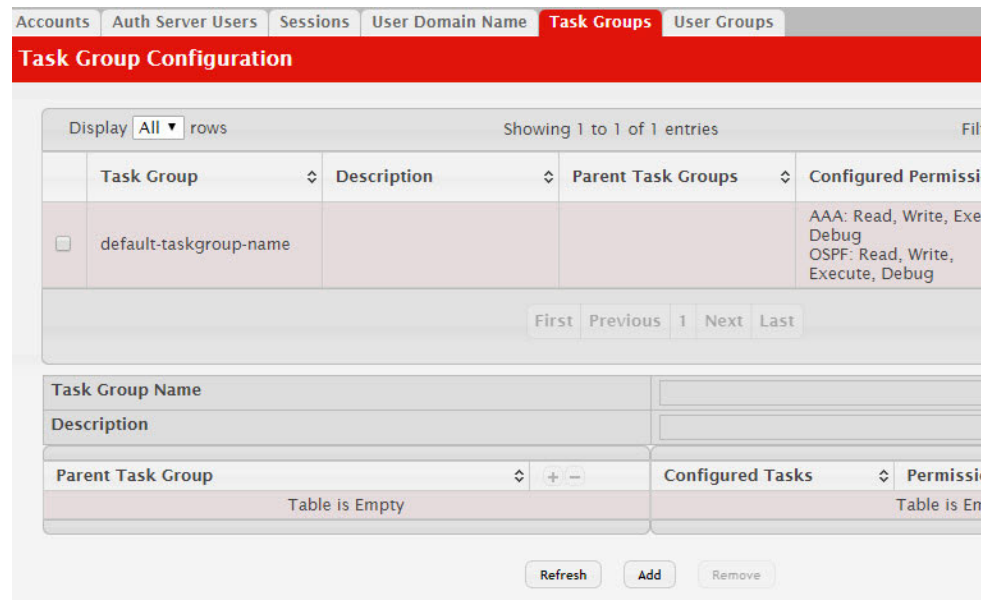
## Task Group

The **Task Group Configuration** page allows you to add, edit, and remove task groups. Task groups allow users to have different permission levels (read, write, execute, debug) at a per-component level. Task-based authorization uses the concept of components/tasks to define permission for commands for a given user.

Users are assigned to User Groups that are, in turn, associated with Task Groups. Each Task Group is then associated with one or more tasks/components. This feature is supported only for users who are authenticated locally via the Web interface.

To access the **Task Group** page, click **System > Users > Task Groups** in the navigation menu.

**Figure 40.** Task Group Configuration



**Table 36.** Task Group Configuration Fields

Field	Description
Task Group	The task group name.
Description	The associated description for task group name.
Parent Task Groups	The associated parent task groups for task group name. To configure this parent task group, click the Add icon in the header row. To remove the parent task group, click the Reset icon in the row.
Configured Permission	The configured task permissions for task group.
Operational Permission	The operational task permissions for the task group.
Configured Tasks	The list of task names. To configure this task, click the Add icon in the header row. To remove the task, click the Reset icon in the row. The tasks available are platform and package dependent.
Permissions	The task permissions. <ul style="list-style-type: none"> <li>• Read</li> <li>• Write</li> <li>• Debug</li> <li>• Execute</li> </ul>

Use the buttons to perform the following:

- To add a task group, click **Add** and specify a name for the group.
- To remove a task group, select the check box associate to the group to remove and click **Remove**.
- Click **Refresh** to update the information on the screen.

## User Group

The **User Group Configuration** page allows you to add, edit, and remove user groups.

To access the **User Group** page, click **System > Users > User Group** in the navigation menu.

**Figure 41.** User Group Configuration

**Table 37.** User Group Configuration Fields

Field	Description
User Group	The user group name.
Description	The associated description for User group name.
Parent User Groups	The associated parent user groups for user group. To configure this parent user group, click the Add icon in the header row. To remove the parent user group, click the Reset icon in the row.
Contained Task Group	The associated task groups for user group. To configure this task group, click the Add icon in the header row. To remove the task group, click the Reset icon in the row.
Operational Permission	The operational task permissions for the user group. <ul style="list-style-type: none"> <li>• Read</li> <li>• Write</li> <li>• Debug</li> <li>• Execute</li> </ul>

Use the buttons to perform the following:

- To add a user group, click **Add** and specify a name for the group.
- To remove a user group, select the check box associate to the group to remove and click **Remove**.
- Click **Refresh** to update the information on the screen.

## Accounting List Configuration

Use the Accounting List Configuration page to view and configure the accounting lists for users who access the command-line interface (CLI) to manage and monitor the device. Accounting lists are used to record user activity on the device. The device is preconfigured with accounting lists. These are default lists, and they cannot be deleted. Additionally, the List Name and Accounting Type settings for the default lists cannot be changed.

To access the Accounting List Configuration page, click **System > AAA > Accounting List** in the navigation menu.

**Figure 42.** Accounting List Configuration



The table below describes the fields on the Accounting List Configuration page.

**Table 38.** Accounting List Configuration Fields

Field	Description
Accounting Type	The type of accounting list, which is one of the following: <b>Command</b> – Each CLI command executed by the user, along with the time the command was executed, is recorded and sent to an external AAA server. <b>EXEC</b> – User login and logout times are recorded and sent to an external AAA server. <b>dot1x</b> – Provides accounting for dot1x user commands, sent to an external RADIUS server.
List Name	The name of the accounting list. This field can be configured only when adding a new accounting list.

**Table 38.** Accounting List Configuration Fields (continued)

Field	Description
Record Type	Indicates when to record and send information about the user activity: <ul style="list-style-type: none"> <li>• <b>StartStop</b> – Accounting notifications are sent at the beginning and at the end of an exec session or a user-executed command. User activity does not wait for the accounting notification to be recorded at the AAA server.</li> <li>• <b>StopOnly</b> – Accounting notifications are sent at the end of an exec session or a user-executed command.</li> <li>• <b>None</b> – Accounting will not be notified.</li> </ul>
Method Options	The method(s) used to record user activity. The possible methods are as follows: <ul style="list-style-type: none"> <li>• <b>TACACS+</b> – Accounting notifications are sent to the configured TACACS+ server.</li> <li>• <b>RADIUS</b> – Accounting notifications are sent to the configured RADIUS server.</li> </ul>
List Type	The type of accounting list, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Default</b> – The list is preconfigured on the system. This type of list cannot be deleted, and only the Method Options and Record Type settings are configurable.</li> <li>• <b>Configured</b> – The list has been added by a user.</li> </ul>
Access Line	The access method(s) that use the list for accounting user activity. The settings for this field are configured on the <b>Accounting Selection</b> page.

Use the buttons to perform the following tasks:

- To configure a new accounting list, click **Add**.
- To edit a list, select the entry to modify and click **Edit**. The settings that can be edited depend on the list type.
- To remove a non-default accounting list, click the – (minus) button associated with the entry. You must confirm the action before the entry is deleted.
- To reset the Method Options for a default accounting list to the factory default values, click the **Reset** icon associated with the entry. You must confirm the action before the entry is reset.

**Figure 43.** Add New Accounting List



Figure 43 shows the fields on the Add New Accounting List page.

After you click **Add** or **Edit**, a window opens and allows you to configure accounting list settings. When adding an accounting list, you can configure the List Name, Accounting Type, and Record Type fields as well as the Accounting Methods. When editing an existing authentication list, only the Record Type and Accounting Methods can be configured. The following information describes how to set the Accounting Methods.

**Table 39.** *Add New Accounting List Fields*

Field	Description
Accounting Methods	This area includes the Available Methods and Selected Methods fields. If a list uses multiple accounting methods, the order in which you move the method from the Available Methods field to the Selected Methods field determines the order in which the device attempts to send accounting notifications. If the device successfully sends the accounting notifications by using the first method, the next method is not attempted.
Available Methods	The accounting methods that can be used for the accounting list. To set the accounting method, select the method in the Available Methods field and click the right arrow to move it into the Selected Methods field.
Selected Methods	The accounting methods currently configured for the list. When multiple methods are in this field, the order in which the methods are listed is the order in which the methods will be used. If the device is unable to send accounting notifications by using the first method, the device attempts to send notifications by using the second method. To remove a method from this field, select it and click the left arrow to return it to the Available Methods area.

If you change any of the parameters, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Accounting List Selection

Use this page to associate an accounting list with each access method. For each access method, the following two accounting lists are associated:

- Exec – The accounting list to record user login and logout times.
- Commands – The accounting list to record which actions a user takes on the system, such as page views or configuration changes. This list also records the time when the action occurred. For Terminal access methods, this list records the CLI commands a user executes and when each command is issued.

To access the Accounting List Configuration page, click **System > AAA > Accounting Selection** in the navigation menu.

**Figure 44.** Accounting List Configuration

**Table 40.** Accounting List Configuration Fields

Field	Description
Terminal	<p>The access methods in this section are CLI-based.</p> <ul style="list-style-type: none"> <li>• <b>Console</b>—The Exec accounting list and the Commands accounting list to apply to users who access the CLI by using a connection to the console port.</li> <li>• <b>Telnet</b> — The Exec accounting list and the Commands accounting list to apply to users who access the CLI by using a Telnet session.</li> <li>• <b>SSH</b> — The Exec accounting list and the Commands accounting list to apply to users who access the CLI by using a secure shell (SSH) session.</li> </ul>
Hypertext Transfer Protocol	<p>The access methods in this section are through a web browser.</p> <ul style="list-style-type: none"> <li>• <b>HTTP</b> — The Exec accounting list and the Commands accounting list to apply to users who access the web-based management interface by using HTTP.</li> <li>• <b>HTTPS</b> — The Exec accounting list to apply to users who access the web-based management interface by using secure HTTP (HTTPS).</li> </ul>

If you change any of the parameters, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Authentication List Configuration

Use the Authentication List Configuration page to view and configure the authentication lists used for management access and port-based (IEEE 802.1X) access to the system. An authentication list specifies which authentication method(s) to use to validate the credentials of a user who attempts to access the device. Several authentication lists are preconfigured on the system. These are default lists, and they cannot be deleted. Additionally, the List Name and Access Type settings for the default lists cannot be changed.

To access the Authentication List Configuration page, click **System > AAA > Authentication List** in the navigation menu.

**Figure 45.** Authentication List Configuration

The screenshot shows the 'Authentication List Configuration' page. At the top, there are navigation tabs: 'Authentication List' (selected), 'Authentication Selection', 'Authorization List', 'Authorization Selection', 'Accounting List', and 'Accounting Selection'. Below the tabs is a red header with the text 'Authentication List Configuration'. Underneath, there is a control bar with 'Display All rows' and 'Showing 1 to 7 of 7 entries'. The main content is a table with the following columns: List Name, Access Type, Method Options, List Type, and Access I. The table contains seven rows of data:

List Name	Access Type	Method Options	List Type	Access I
defaultList	Login	Local	Default	Console
networkList	Login	Local	Default	Telnet,SSH
enableList	Enable	Enable,None	Default	Console
enableNetList	Enable	Enable,Deny	Default	
httpList	HTTP	Local	Default	HTTP
httpsList	HTTPS	Local	Default	HTTPS
dot1xList	Dot1x		Default	Dot1x

At the bottom of the table, there are navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'.

Table 41 describes the fields for the Authentication List Configuration page.

**Table 41.** Authentication List Configuration Fields

Field	Description
List Name	The name of the authentication list. This field can be configured only when adding a new authentication list.
Access Type	The way the user accesses the system. This field can be configured only when adding a new authentication list, and only the Login and Enable access types can be selected. The access types are as follows: <ul style="list-style-type: none"> <li>• <b>Login</b> – User EXEC-level management access to the command-line interface (CLI) by using a console connection or a telnet or SSH session. Access at this level has a limited number of CLI commands available to view or configure the system.</li> <li>• <b>Enable</b> – Privileged EXEC-level management access to the CLI by using a console connection or a telnet or SSH session. In Privileged EXEC mode, read-write users have access to all CLI commands.</li> <li>• <b>HTTP</b> – Management-level access to the web-based user interface by using HTTP.</li> <li>• <b>HTTPS</b> – Management-level access to the web-based user interface by using secure HTTP.</li> <li>• <b>Dot1x</b> – Port-based access to the network through a switch port that is controlled by IEEE 802.1X.</li> </ul>

**Table 41.** *Authentication List Configuration Fields (continued)*

Field	Description
Method Options	<p>The method(s) used to authenticate a user who attempts to access the management interface or network. The possible methods are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b> – Uses the locally configured Enable password to verify the user's credentials.</li> <li>• <b>IAS</b> – Uses the local Internal Authentication Server (IAS) database for 802.1X port-based authentication.</li> <li>• <b>Line</b> – Uses the locally configured Line password to verify the user's credentials.</li> <li>• <b>Local</b> – Uses the ID and password in the Local User database to verify the user's credentials.</li> <li>• <b>None</b> – No authentication is used.</li> <li>• <b>Radius</b> – Sends the user's ID and password to the configured Radius server to verify the user's credentials.</li> <li>• <b>TACACS</b> – Sends the user's ID and password to the configured TACACS server to verify the user's credentials.</li> <li>• <b>Deny</b> – Denies authentication.</li> </ul>
List Type	<p>The type of list, which is one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Default</b> – The list is preconfigured on the system. This type of list cannot be deleted, and only the Method Options are configurable.</li> <li>• <b>Configured</b> – The list has been added by a user.</li> </ul>
Access Line	<p>The access method(s) that use the list for authentication. The settings for this field are configured on the Authentication Selection page.</p>

- Click **Refresh** to update the information on the screen.

After you click **Add** or **Edit**, a window opens and allows you to configure authentication list settings. When adding an authentication list, you can configure the List Name and Access Type fields as well as the Authentication Methods. When editing an existing authentication list, only the Authentication Methods can be configured. The following information describes how to set the Authentication Methods.

**Table 42.** *Add New Authentication List*

Field	Description
Authentication Methods	<p>This area includes the Available Methods and Selected Methods fields. For lists that allow multiple authentication methods, the order in which you move the method from the Available Methods field to the Selected Methods field determines the order in which the device attempts to authenticate the user. For example, if the selected methods are Enable, followed by None, a user who fails to authenticate with the enable password is granted access anyway because the final method indicates that no authentication is required.</p>

Field	Description
Available Methods	The authentication methods that can be used for the authentication list. Not all authentication methods are available for all lists. To set the authentication method, select the method in the Available Methods field and click the right arrow to move it into the Selected Methods field.
Selected Methods	The authentication methods currently configured for the list. When multiple methods are in this field, the order in which the methods are listed is the order in which the methods will be used to authenticate a user. If the user fails to be authenticated using the first method, the device attempts to verify the user's credentials by using the next method in the list. No authentication methods can be added after None. To remove a method from this field, select it and click the left arrow to return it to the Available Methods area.

## Authentication List Selection

Use the Authentication List Selection page to associate an authentication list with each CLI-based access method (Console, Telnet, and SSH). Each access method has the following two authentication lists associated with it:

- **Login** – The authentication list to use for User EXEC-level management access to the CLI. Access at this level has a limited number of CLI commands available to view or configure the system. The options available in this menu include the default Login authentication lists as well as any user-configured Login lists.
- **Enable** – The authentication list to use for Privileged EXEC-level management access to the CLI. In Privileged EXEC mode, read-write users have access to all CLI commands. The options available in this menu include the default Enable authentication lists as well as any user-configured Enable lists.

To access the Authentication List Selection page, click **System > AAA > Authentication Selection** in the navigation menu.

**Figure 46.** Authentication List Selection

Terminal	Login	Enable
Console	defaultList	enable
Telnet	networkList	enable
SSH	networkList	enable

Submit Refresh Cancel

Table 43 describes the fields for the Authentication List Selection page.

**Table 43.** *Select Authentication List Fields*

Field	Description
Console	The Login authentication list and the Enable authentication list to apply to users who attempt to access the CLI by using a connection to the console port.
Telnet	The Login authentication list and the Enable authentication list to apply to users who attempt to access the CLI by using a Telnet session.
Secure Telnet (SSH)	The Login authentication list and the Enable authentication list to apply to users who attempt to access the CLI by using a secure shell (SSH) session.

### Command Button

The page has the following command button:

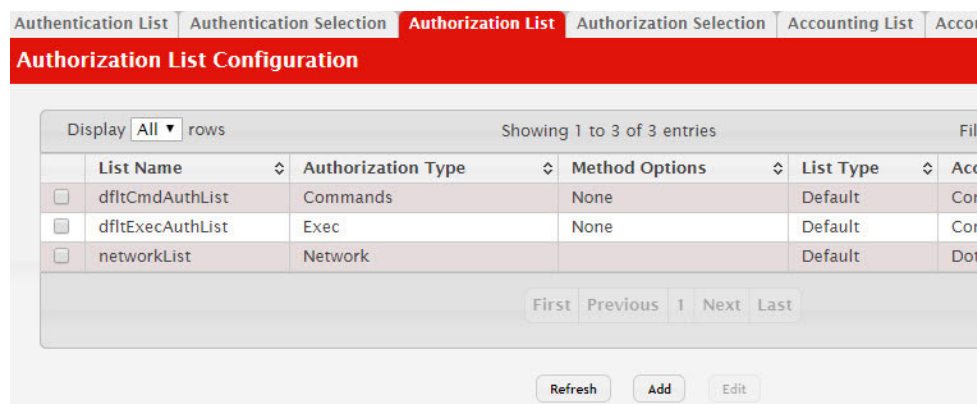
- **Submit**—Update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

## Authorization List Configuration

Use this page to view and configure the authorization lists for users who access the command-line interface (CLI) and for users who access the network through IEEE 802.1X-enabled ports. Authorization lists are used to determine whether a user is permitted to perform a given activity on the system or network. Several authorization lists are preconfigured on the system. These are default lists, and they cannot be deleted. Additionally, the List Name and Authorization Type settings for the default lists cannot be changed.

To access the Authorization List Configuration page, click **System > AAA > Authorization List** in the navigation menu.

**Figure 47.** Authorization List Configuration



**Table 44.** *Authorization List Configuration Fields*

Field	Description
List Name	The name of the authorization list. This field can be configured only when adding a new authorization list.

**Table 44.** *Authorization List Configuration Fields (continued)*

Field	Description
Authorization Type	The type of authorization list, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Command</b> – Determines which CLI commands a user is permitted to issue. When command authorization is enabled, each command a user enters must be validated before the command is executed.</li> <li>• <b>EXEC</b> – Determines whether a user can bypass User EXEC mode and enter Privileged EXEC mode directly after a successful Login authentication.</li> <li>• <b>Network</b> – Determines whether the user is permitted to access various network services. This authorization type applies to port-based access (IEEE 802.1X) rather than access to the CLI.</li> </ul>
Method Options	The method(s) used to authorize a user's access to the device or network services. The possible methods are as follows: <ul style="list-style-type: none"> <li>• <b>TACACS+</b> – When a user issues a CLI command, the device contacts the configured TACACS+ server to verify whether the user is allowed to issue the command. If approved, the command is executed. Otherwise, the command fails.</li> <li>• <b>RADIUS</b> – When a user is authenticated by the RADIUS server, the device downloads a list of permitted/denied commands from the RADIUS server. The list of authorized commands that are associated with the authenticated user is cached during the user's session. If this method is selected, the authentication method for the access type must also be RADIUS.</li> <li>• <b>Local</b> – Uses a list stored locally on the system to determine whether the user is authorized to access the given services.</li> <li>• <b>None</b> – No authorization is used. If the method is None, the authorization type is effectively disabled.</li> </ul>
List Type	The type of authorization list, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Default</b> – The list is preconfigured on the system. This type of list cannot be deleted, and only the Method Options are configurable.</li> <li>• <b>Configured</b> – The list has been added by a user.</li> </ul>
Access Line	The access method(s) that use the list for authorization. The settings for this field are configured on the <b>Authorization Selection</b> page.

- To configure a new authorization list, click **Add**.
- To edit a list, select the entry to modify and click **Edit**. The settings that can be edited depend on the list type.
- To remove a non-default authorization list, click the – (minus) button associated with the entry. You must confirm the action before the entry is deleted.

To reset the Method Options for a default authorization list to the factory default values, click the **Reset** icon associated with the entry. You must confirm the action before the entry is reset.

After you click **Add** or **Edit**, a window opens and allows you to configure authorization list settings.

**Figure 48.** Add New Authorization List

When adding an authorization list, you can configure the List Name and Authorization Type fields as well as the Authorization Methods. When editing an existing authentication list, only the Authorization Methods can be configured. The following information describes how to set the Authorization Methods.

**Table 45.** Add New Authorization List Fields

Field	Description
Authorization Methods	This area includes the <b>Available Methods</b> and <b>Selected Methods</b> fields. For lists that allow multiple authorization methods, the order in which you move the method from the <b>Available Methods</b> field to the <b>Selected Methods</b> field determines the order in which the device attempts to authorize the user.
Available Methods	The authorization methods that can be used for the authorization list. Not all methods are available for all lists. To set the authorization method, select the method in the <b>Available Methods</b> field and click the right arrow to move it into the <b>Selected Methods</b> field.
Selected Methods	The authorization methods currently configured for the list. When multiple methods are in this field, the order in which the methods are listed is the order in which the methods will be used to authorize a user. If the user fails to be authorized using the first method, the device attempts to authorize the user by using the next method in the list. No authorization methods can be added after <b>None</b> . To remove a method from this field, select it and click the left arrow to return it to the <b>Available Methods</b> area.

## Authorization List Selection

Use this page to associate an authorization lists with each CLI-based access method (Console, Telnet, and SSH). Each access method has the following two authorization lists associated with it:



- **Exec** – The authorization list that determines whether the user is permitted to enter Privileged EXEC mode immediately after a successful Login authentication.
- **Commands** – The authorization list that determines which CLI commands the user is permitted to issue.

To access the Authorization List Selection page, click **System > AAA > Authorization Selection** in the navigation menu.

**Figure 49.** Authorization List Selection

Terminal	Exec	Commands
Console	dfltExecAuthList	dfltC
Telnet	dfltExecAuthList	dfltC
SSH	dfltExecAuthList	dfltC

**Table 46.** Authorization List Selection Fields

Field	Description
Console	The Exec authorization list and the Commands authorization list to apply to users who access the CLI by using a connection to the console port.
Telnet	The Exec authorization list and the Commands authorization list to apply to users who access the CLI by using a Telnet session.
SSH	The Exec authorization list and the Commands authorization list to apply to users who access the CLI by using a secure shell (SSH) session.

- Click **Refresh** to refresh the page with the most current data from the switch.
- If you make any changes to the page, click **Submit** to apply the changes to the system and update the running configuration. If you want the device to retain these changes across a reset, you must first save the configuration.

## Line Password

Use the Line Password page to configure line mode passwords.

To display the page, click **System > Passwords > Line Password** in the navigation menu.

**Figure 50.** Line Password

Line Mode	Password / Confirm Password
<input type="checkbox"/> Console	<input type="password"/> / <input type="password"/>
<input type="checkbox"/> Telnet	<input type="password"/> / <input type="password"/>
<input type="checkbox"/> SSH	<input type="password"/> / <input type="password"/>

**Table 47.** Line Password Fields

Field	Description
Line Mode	Any or all of the following passwords may be changed on this page by checking the box that precedes it: <ul style="list-style-type: none"><li>• Console</li><li>• Telnet</li><li>• SSH</li></ul>
Password (8–64 characters)	Enter the new password for the corresponding Line Mode in this field. Be sure the password conforms to the allowed number of characters. The password characters are not displayed on the page, but are disguised in a browser-specific manner.
Confirm Password (8–64 characters)	Re-enter the new password for the corresponding Line Mode in this field. This must be the same value entered in the Password field. Be sure the password conforms to the allowed number of characters. The password characters are not displayed on the page, but are disguised in a browser-specific manner.

If you change any data, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Enable Password

Use the Enable Password page to configure the enable password.

To display the page, click **System > Passwords > Enable Password** in the navigation menu.

**Figure 51.** Enable Password Configuration

The screenshot shows a web interface for configuring the enable password. It features a navigation bar with tabs for 'Line Password', 'Enable Password', 'Password Rules', 'Last Password', and 'Reset Passwords'. The 'Enable Password' tab is active. Below the navigation bar is a red header with the text 'Enable Password Configuration'. The main content area contains two input fields: 'Enable Password' and 'Confirm Enable Password', both with a character count '(8 to 64 characters)'. At the bottom of the form are four buttons: 'Submit', 'Refresh', 'Cancel', and 'Remove'.

**Table 48.** Enable Password Fields

Field	Description
Enable Password	Specify the password all users must enter after executing the enable command at the CLI prompt.
Confirm Enable Password	Confirms the new enable password. The password appears in the ***** format.

If you change any data, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Password Rules

Use this page to configure settings that apply to all user passwords.

To display the page, click **System > Passwords > Password Rules** in the navigation menu.

**Figure 52.** Password Rules Configuration

**Table 49.** Password Rules Configuration Fields

Field	Description
Minimum Length	Passwords must have at least this many characters (8 to 64).
Aging (days)	The number of days that a user password is valid from the time the password is set. Once a password expires, the user is required to enter a new password at the next login.
History	The number of previous passwords that are retained to prevent password reuse. This helps to ensure that a user does not attempt to reuse the same password too often.
Lockout Attempts	After a user fails to log in this number of times, the user is locked out until the password is reset by the administrator.
Strength Check	Enable or disable the password strength check feature. Enabling this feature forces the user to configure passwords that comply with the strong password configuration specified in the following fields.
Minimum Number of Uppercase Letters	Specify the minimum number of uppercase letters a password must include.
Minimum Number of Lowercase Letters	Specify the minimum number of lowercase letters a password must include.
Minimum Number of Numeric Characters	Specify the minimum number of numbers a password must include.
Minimum Number of Special Characters	Specify the minimum number of special characters (non-alphanumeric, such as # or &) a password must include.
Maximum Number of Repeated Characters	Specify the maximum number of repeated characters a password is allowed to include. An example of four repeated characters is <i>aaaa</i> .

**Table 49.** Password Rules Configuration Fields (continued)

Field	Description
Maximum Number of Consecutive Characters	Specify the maximum number of consecutive characters a password is allowed to include. An example of four consecutive characters is <i>abcd</i>
Minimum Character Classes	Specify the minimum number of character classes a password must contain. There are four character classes: <ul style="list-style-type: none"> <li>• Uppercase</li> <li>• Lowercase</li> <li>• Numbers</li> <li>• Special Characters</li> </ul>
Exclude Keyword Name	The list of keywords that a valid password must not contain. Excluded keyword checking is case-insensitive. Additionally, a password cannot contain the backwards version of an excluded keyword. For example, if <i>pass</i> is an excluded keyword, passwords such as <i>23passA2c</i> , <i>ssapword</i> , and <i>PASwoRD</i> are prohibited. Use the plus and minus buttons to perform the following tasks: <ul style="list-style-type: none"> <li>• To add a keyword to the list, click the + (plus) button, type the word to exclude in the Exclude Keyword Name field, and click <b>Submit</b>.</li> <li>• To remove a keyword from the list, click the – (minus) button associated with the keyword to remove and confirm the action.</li> <li>• To remove all keywords from the list, click the – (minus) button in the header row and confirm the action.</li> </ul>

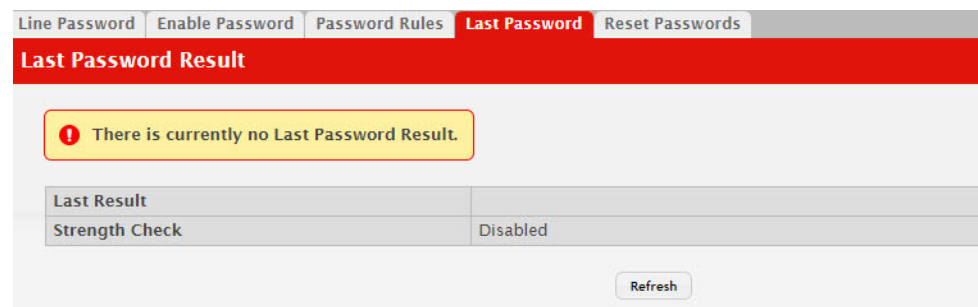
If you change any data, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

## Last Password Result

Use the Last Password Result page view information about the last attempt to set a user password. If the password set was unsuccessful, a reason for the failure is given.

To display the page, click **System > Password > Last Password** in the navigation menu.

**Figure 53.** Last Password Result



**Table 50.** *Last Password Result*

Field	Description
Last Password Set Result	Displays information about the last (User/Line/Enable) password configuration result. If the field is blank, no passwords have been configured on the device. Otherwise, the field shows that the password was successfully set or provides information about the type of password configuration that failed and why it could not be set.
Strength Check	Displays Enabled if Strength Check is applied in last password change, otherwise it displays Disabled.

## Denial of Service

Use the Denial of Service (DoS) page to configure DoS control. CE0128XB/CE0152XB software provides support for classifying and blocking specific types of DoS attacks. You can configure your system to monitor and block these types of attacks:

- **SIP=DIP:** Source IP address = Destination IP address.
- **First Fragment:** TCP Header size smaller than configured value.
- **TCP Fragment:** IP Fragment Offset = 1.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.

**Note:** Monitoring and blocking of the types of attacks listed below are supported only on the following platforms:

- | BCM56514
- | BCM56624
- | BCM56820
- | BCM56224
- | BCM56634
- | BCM56636

- **SMAC=DMAC:** Source MAC address=Destination MAC address.
- **TCP Port:** Source TCP Port = Destination TCP Port.
- **UDP Port:** Source UDP Port = Destination UDP Port.
- **TCP Flag & Sequence:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **TCP Offset:** TCP Header Offset = 1.
- **TCP SYN:** TCP Flag SYN set.
- **TCP SYN & FIN:** TCP Flags SYN and FIN set.

- **TCP FIN & URG & PSH:** TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- **ICMP V6:** Limiting the size of ICMPv6 Ping packets.
- **ICMP Fragment:** Checks for fragmented ICMP packets.
- **Smurf Attack:** A flood of spoofed broadcast ping messages are sent to the system.
- **PingFlood Attack:** Similar to a Smurf Attack, a flood of ping packets are sent to the system.
- **SYN ACK Flood Attack:** A series of SYN requests are sent to force the switch to reply with SYN-ACK messages.

To access the **Denial of Service** page, click **System > Advanced Configuration > Protection > Denial of Service** in the navigation menu.

**Figure 54.** Denial of Service

**Table 51.** Denial of Service Configuration Fields

Field	Description
TCP Settings	
First Fragment	Enable this option to allow the device to drop packets that have a TCP header smaller than the value configured in the Min TCP Hdr Size field.
TCP Port	Enable this option to allow the device to drop packets that have the TCP source port equal to the TCP destination port.

**Table 51.** Denial of Service Configuration Fields (continued)

Field	Description
UDP Port	Enable this option to allow the device to drop packets that have the UDP source port equal to the UDP destination port.
SIP=DIP	Enable this option to allow the device to drop packets that have a source IP address equal to the destination IP address.
SMAC=DMAC	Enable this option to allow the device to drop packets that have a source MAC address equal to the destination MAC address.
TCP FIN and URG and PSH	Enable this option to allow the device to drop packets that have TCP Flags FIN, URG, and PSH set and a TCP Sequence Number equal to 0.
TCP Flag and Sequence	Enable this option to allow the device to drop packets that have TCP control flags set to 0 and the TCP sequence number set to 0.
TCP SYN	Enable this option to allow the device to drop packets that have TCP Flags SYN set.
TCP SYN and FIN	Enable this option to allow the device to drop packets that have TCP Flags SYN and FIN set.
TCP Fragment	Enable this option to allow the device to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
TCP Offset	Enable this option to allow the device to drop packets that have a TCP header Offset set to 1.
Port D-Disable	Enable this option to allow the system to diagnostically disable an interface if a potential DoS attack has been detected on that interface. If an interface is diagnostically disabled, it remains in the disabled state until an administrator manually enables the interface.
Min TCP Hdr Size	The minimum TCP header size allowed. If First Fragment DoS prevention is enabled, the device will drop packets that have a TCP header smaller than this configured value.
ICMP Settings: These options help prevent the device and the network from attacks that involve issues with the ICMP echo request packets (pings) that the device receives.	
ICMP	Enable this option to allow the device to drop ICMP packets that have a type set to ECHO_REQ (ping) and a payload size greater than the ICMP payload size configured in the Max ICMPv4 Size or Max ICMPv6 Size fields.
ICMP Fragment	Enable this option to allow the device to drop fragmented ICMP packets.
Max ICMPv4 Size	The maximum allowed ICMPv4 packet size. If ICMP DoS prevention is enabled, the device will drop ICMPv4 ping packets that have a size greater than this configured maximum ICMPv4 packet size.
Max ICMPv6 Size	The maximum allowed IPv6 ICMP packet size. If ICMP DoS prevention is enabled, the switch will drop IPv6 ICMP ping packets that have a size greater than this configured maximum ICMPv6 packet size.

If you change any of the DoS settings, click **Submit** to apply the changes to the switch. To preserve the changes across a switch reboot, you must perform a save.



## Managing Logs

The switch may generate messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored both locally on the platform and forwarded to one or more centralized points of collection for monitoring purposes as well as long term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

The *in-memory* log stores messages in memory based upon the settings for message component and severity. On stackable systems, this log exists only on the management unit. Other platforms in the stack forward their messages to the management unit log. Access to in-memory logs on other than the management unit is not supported.

## Log Configuration

The Log Configuration page allows administrators with the appropriate privilege level to configure the administrative mode and various settings for logging features on the switch.

To access the Log Configuration page, click **System > Logs > Configuration** in the navigation menu.

**Figure 55.** Log Configuration

Buffered Log	Event Log	Persistent Log	Hosts	Configuration	Source Interface Configuration	Statistics
<b>Log Configuration</b>						
<b>Buffered Log Configuration</b>						
Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable					
Behavior	<input checked="" type="radio"/> Wrap <input type="radio"/> Stop on Full					
<b>Command Logger Configuration</b>						
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable					
<b>Console Log Configuration</b>						
Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable					
Severity Filter	Error					
<b>Persistent Log Configuration</b>						
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable					
Severity Filter	Alert					
<b>Syslog Configuration</b>						
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable					
Protocol Version	<input checked="" type="radio"/> RFC 3164 <input type="radio"/> RFC 5424					
Local UDP Port	514 (1 to 65535)					
Submit Refresh Cancel						

**Table 52.** *Log Configuration Fields*

Field	Description
Buffered Log Configuration	
Admin Mode	Enable or disable logging to the buffered (RAM) log file.
Behavior	Specify what the device should do when the buffered log is full. It can either overwrite the oldest messages (Wrap) or stop writing new messages to the buffer (Stop on Full).
Command Logger Configuration	
Admin Mode	Enable or disable logging of the command-line interface (CLI) commands issued on the device.
Console Log Configuration	
Admin Mode	Enable or disable logging to any serial device attached to the host.
Severity Filter	Select the severity of the messages to be logged. All messages at and above the selected threshold are logged to the console. The severity can be one of the following: <ul style="list-style-type: none"> <li>• <b>Emergency (0):</b> The device is unusable.</li> <li>• <b>Alert (1):</b> Action must be taken immediately.</li> <li>• <b>Critical (2):</b> The device is experiencing primary system failures.</li> <li>• <b>Error (3):</b> The device is experiencing non-urgent failures.</li> <li>• <b>Warning (4):</b> The device is experiencing conditions that could lead to system errors if no action is taken.</li> <li>• <b>Notice (5):</b> The device is experiencing normal but significant conditions.</li> <li>• <b>Info (6):</b> The device is providing non-critical information.</li> <li>• <b>Debug (7):</b> The device is providing debug-level information.</li> </ul>
Persistent Log Configuration	
Admin Mode	Enable or disable logging to the persistent log. These messages are not deleted when the device reboots.
Severity Filter	Select the severity of the messages to be logged. All messages at and above the selected threshold are logged to the console. See the previous severity filter description for more information about each severity level.
Syslog Configuration	
Admin Mode	Enable or disable logging to configured syslog hosts. When the syslog admin mode is disabled the device does not relay logs to syslog hosts, and no messages will be sent to any collector/relay. When the syslog admin mode is enabled, messages will be sent to configured collectors/relays using the values configured for each collector/relay.
Protocol Version	The RFC version of the syslog protocol.
Local UDP Port	The UDP port on the local host from which syslog messages are sent.

If you change the buffered log settings, click **Submit** to apply the changes to the system. To preserve the changes after a system reboot, you must perform a save.

# Buffered Log

The log messages the device generates in response to events, faults, errors, and configuration changes are stored locally on the device in the RAM (cache). This collection of log files is called the RAM log or buffered log. When the buffered log file reaches the configured maximum size, the oldest message is deleted from the RAM when a new message is added. If the system restarts, all messages are cleared.

To access the Buffered Log page, click **System > Logs > Buffered Log** in the navigation menu.

**Figure 56.** Buffered Log

Log Index	Log Time	Severity	Component	Description
1	Feb 7 21:12:09	Info	USER_MGR	INFO HTTP Session 14 started for user admin connected from 10.10.10.10
2	Feb 7 20:52:58	Info	USER_MGR	INFO HTTP Session 13 ended for user admin connected from 10.10.10.10
3	Feb 7 16:44:39	Info	BONJOUR	INFO Change notifications received from CLI/WEB component services.
4	Feb 7 16:44:15	Info	USER_MGR	INFO HTTP Session 13 started for user admin connected from 10.10.10.10
5	Feb 7 16:40:53	Info	USER_MGR	INFO HTTP Session 12 ended for user admin connected from 10.10.10.10
6	Feb 7 16:22:25	Info	USER_MGR	INFO HTTP Session 12 started for user admin connected from 10.10.10.10
7	Feb 7 15:48:49	Info	USER_MGR	INFO HTTP Session 11 ended for user admin connected from 10.10.10.10
8	Feb 7 15:44:46	Notice	TRAPMGR	NOTE Session 0 of type 1 ended for user admin connected from 10.10.10.10
9	Feb 7 15:44:46	Info	CLI_WEB	INFO Serial Session 0 ended for user admin connected from 10.10.10.10
10	Feb 7 15:40:15	Info	USER_MGR	INFO HTTP Session 11 started for user admin connected from 10.10.10.10

**Table 53.** *Buffered Log Fields*

Field	Description
Log Index	The position of the entry within the buffered log file. The most recent log message always has a Log Index value of 1.
Log Time	The time the entry was added to the log.
Severity	The severity level associated with the log entry. The severity can be one of the following: <ul style="list-style-type: none"><li>• <b>Emergency (0):</b> The device is unusable.</li><li>• <b>Alert (1):</b> Action must be taken immediately.</li><li>• <b>Critical (2):</b> The device is experiencing primary system failures.</li><li>• <b>Error (3):</b> The device is experiencing non-urgent failures.</li><li>• <b>Warning (4):</b> The device is experiencing conditions that could lead to system errors if no action is taken.</li><li>• <b>Notice (5):</b> The device is experiencing normal but significant conditions.</li><li>• <b>Info (6):</b> The device is providing non-critical information.</li><li>• <b>Debug (7):</b> The device is providing debug-level information.</li></ul>
Component	The component that issued the log entry.
Description	The text description for the log entry.

Click **Refresh** to update the screen and associated messages.

## Event Log

Use the Event Log page to display the event log, which is used to hold error messages for catastrophic events. After the event is logged and the updated log is saved in flash memory, the switch will be reset. The log can hold at least 2,000 entries (the actual number depends on the platform and OS), and is erased when an attempt is made to add an entry after it is full. The event log is preserved across system resets.

To access the Event Log page, click **System > Logs > Event Log** in the navigation menu.

**Figure 57.** Event Log

Log Index	Type	Filename	Line	Task ID	Code
1	EVENT	bootos.c	194	051AB6EC	AAAAAA
2	EVENT	unitmgr.c	6602	B67F2164	0000000
3	EVENT	bootos.c	194	04D346EC	AAAAAA
4	EVENT	unitmgr.c	6602	0468059C	0000000
5	EVENT	bootos.c	194	046816EC	AAAAAA
6	EVENT	unitmgr.c	6602	B68FCCFC	0000000
7	EVENT	bootos.c	194	044C26EC	AAAAAA

**Table 54.** Event Log Fields

Field	Description
Log Index	A display row index number used to identify the event log entry, with the most recent entry listed first (lowest number).
Type	The incident category that indicates the cause of the log entry: EVENT, ERROR, etc.
Filename	The source code filename of the event origin.
Line	The line number within the source file of the code that detected the event.
Task ID	The OS-assigned ID of the task reporting the event. This value is assigned by, and is specific to, the operating system.
Code	The event code passed to the event log handler by the code reporting the event.
Event Time	A time stamp (days, hours, minutes, and seconds) indicating when the event occurred, measured from the time the device was last reset. The only correlation between any two entries in the event log is the relative amount of time after a system reset that the event occurred.

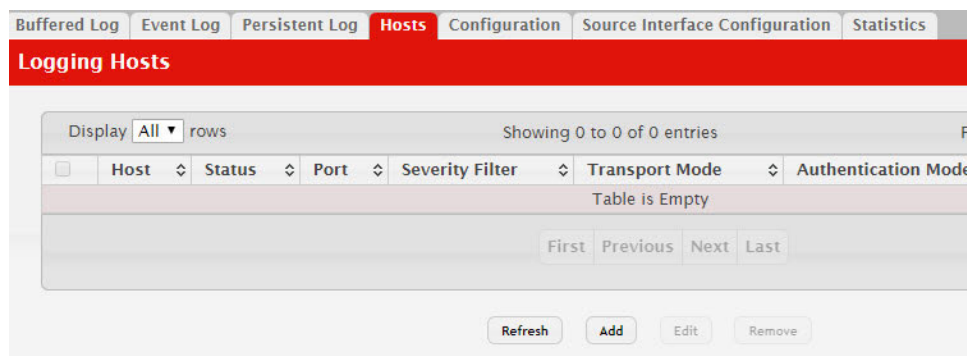
Click **Refresh** to update the screen and associated messages.

## Hosts Log Configuration

Use the Host Log Configuration page to configure remote logging hosts where the switch can send logs.

To access the Host Log Configuration page, click **System > Logs > Hosts** in the navigation menu.

**Figure 58.** Logging Hosts



**Table 55.** Logging Hosts Fields

Field	Description
Host (IP Address/Host Name)	The IP address or DNS-resolvable host name of the remote host to receive log messages.
Status	Indicates whether the host has been configured to be actively logging or not.
Port	The UDP port on the logging host to which syslog messages are sent.
Severity Filter	Severity level threshold for log messages. All log messages with a severity level at and above the configured level are forwarded to the logging host.
Transport Mode	Transport mode used while sending messages to syslog servers. Supported modes are UDP and TLS. If TLS is not configured, default transport mode is UDP.
Authentication Mode	Using TLS security user can configure anonymous authentication mode, in which no client authentication is done by the syslog server. For x509/name authentication mode, two-way authentication is done both by syslog client and client authentication by syslog server side.
Certificate Index	The index used for identifying corresponding certificate files.

Use the buttons to perform the following tasks:

- To add a logging host, click **Add** and configure the desired settings.
- To change information for an existing logging host, select the check box associated with the entry and click **Edit**. You cannot edit the host name or address of a host that has been added.
- To delete a configured logging host from the list, select the check box associated with each entry to delete and click **Remove**.

**Figure 59.** Add Host

The screenshot shows a web form titled "Add Host". It contains three input fields: "IP Address/Host Name" (with a note: "(Max 255 characters or x.x.x.x or x:x:x:x:x:x:x)"), "Port" (with the value "514" and a note: "(1 to 65535)"), and "Severity Filter" (with a dropdown menu set to "Critical"). A "Submit" button is located at the bottom right of the form.

After you add a logging host, the screen displays additional fields.

**Table 56.** Host Log Configuration Fields

Field	Description
IP Address/Host Name	The IP address or DNS-resolvable host name of the remote host to receive log messages.
Port	The UDP port on the logging host to which syslog messages are sent.
Severity Filter	Severity level threshold for log messages. All log messages with a severity level at and above the configured level are forwarded to the logging host.

## Adding a Remote Logging Host

Use the following procedures to add, configure, or delete a remote logging host.

1. From the **Host** field, select **Add** to add a new host, or select the IP address of an existing host to configure the host.  
If you are adding a new host, enter the IP address of the host in the **IP Address** field and click **Submit**. The screen refreshes, and additional fields appear.
2. In the **Port** field, type the port number on the remote host to which logs should be sent.
3. Select the severity level of the logs to send to the remote host.
4. Click **Submit** to apply the changes to the system.

## Deleting a Remote Logging Host

To delete a remote logging host from the configured list, select the IP address of the host from the Host field, and then click **Delete**.

## Syslog Source Interface Configuration

Use this page to specify the physical or logical interface to use as the logging (Syslog) client source interface. When an IP address is configured on the source interface, this address is used for all Syslog communications between the local logging client and the remote Syslog server. The IP address of the designated source interface is used in the IP header of Syslog management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device.

To access the Syslog Source Interface Configuration page, click **System > Logs > Source Interface Configuration** in the navigation menu.

**Figure 60.** Syslog Source Interface Configuration

**Table 57.** Syslog Source Interface Configuration Fields

Field	Description
Type	The type of interface to use as the source interface: <ul style="list-style-type: none"> <li>• <b>None</b> – The primary IP address of the originating (outbound) interface is used as the source address.</li> <li>• <b>Interface</b> – The primary IP address of a physical port is used as the source address.</li> <li>• <b>VLAN</b> – The primary IP address of a VLAN routing interface is used as the source address.</li> <li>• <b>Loopback</b> – The primary IP address of the loopback interface is used as the source address. A loopback is always reachable, as long as any routing interface is up.</li> <li>• <b>Network</b> – The network source IP is used as the source address.</li> <li>• <b>Service Port</b> – The management port source IP is used as the source address.</li> </ul>
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
Loopback Interface	When the selected Type is Loopback, select the loopback interface to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.

If you change any of the settings on the page, click **Submit** to apply the changes to system.



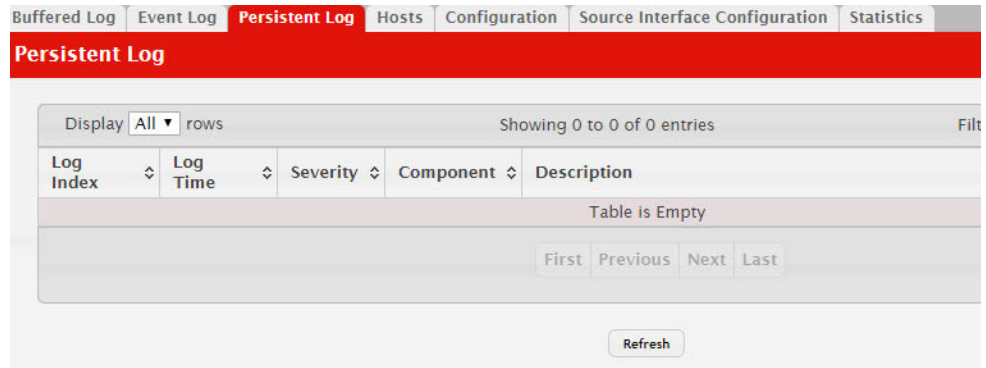
**Note:** Applied changes update the device running configuration. If you want the device to retain these changes across a reset, you must first save the configuration.

## Persistent Log

Use the Persistent Log page to view the persistent log messages.

To access the Persistent Log page, click **System > Log > Persistent Log** in the navigation menu.

**Figure 61.** Persistent Log



**Table 58.** Persistent Log Fields

Field	Description
Log Index	The position of the entry within the buffered log file. The most recent log message always has a Log Index value of 1.
Log Time	The time the entry was added to the log.
Severity	The severity level associated with the log entry. The severity can be one of the following: <ul style="list-style-type: none"> <li>• <b>Emergency (0):</b> The device is unusable.</li> <li>• <b>Alert (1):</b> Action must be taken immediately.</li> <li>• <b>Critical (2):</b> The device is experiencing primary system failures.</li> <li>• <b>Error (3):</b> The device is experiencing non-urgent failures.</li> <li>• <b>Warning (4):</b> The device is experiencing conditions that could lead to system errors if no action is taken.</li> <li>• <b>Notice (5):</b> The device is experiencing normal but significant conditions.</li> <li>• <b>Info (6):</b> The device is providing non-critical information.</li> <li>• <b>Debug (7):</b> The device is providing debug-level information.</li> </ul>
Component	The component that has issued the log entry.
Description	The text description for the log entry.

## Configuring Email Alerts

With the email alerting feature, log messages can be sent to one or more email addresses. You must configure information about the network Simple Mail Transport Protocol (SMTP) server for email to be successfully sent from the switch.

The pages available from the Email Alerting folder allow you to configure information about what type of log message are sent via email and to what address(es) the messages are emailed.

### Email Alert Global Configuration

Use the Email Alert Global Configuration page to configure the common settings for log messages emailed by the switch.

To access the Email Alert Global Configuration page, click **System > Advanced Configuration > Email Alerts > Global** in the navigation menu.

**Figure 62.** Email Alert Global Configuration

Field	Description
Admin Mode	Sets the administrative mode of the feature. <ul style="list-style-type: none"><li>• <b>Enable</b> – The device can send email alerts to the configured SMTP server.</li><li>• <b>Disable</b> – The device will not send email alerts.</li></ul>
From Address	Specifies the email address of the sender (the switch).
Log Duration	This duration in minutes determines how frequently the non critical messages are sent to the SMTP Server.

**Table 59.** Email Alert Global Configuration Fields

Field	Description
Admin Mode	Sets the administrative mode of the feature. <ul style="list-style-type: none"><li>• <b>Enable</b> – The device can send email alerts to the configured SMTP server.</li><li>• <b>Disable</b> – The device will not send email alerts.</li></ul>
From Address	Specifies the email address of the sender (the switch).
Log Duration	This duration in minutes determines how frequently the non critical messages are sent to the SMTP Server.

**Table 59.** Email Alert Global Configuration Fields (continued)

Field	Description
Urgent Messages Severity	Configures the severity level for log messages that are considered to be urgent. Messages in this category are sent immediately. The security level you select and all higher levels are urgent: <ul style="list-style-type: none"> <li>• Emergency indicates system is unusable. It is the highest level of severity.</li> <li>• Alert indicates action must be taken immediately</li> <li>• Critical indicates critical conditions</li> <li>• Error indicates error conditions</li> <li>• Warning indicates warning conditions</li> <li>• Notice indicates normal but significant conditions</li> <li>• Informational indicates informational messages</li> <li>• Debug indicates debug-level messages</li> </ul>
Non Urgent Messages Severity	Configures the severity level for log messages that are considered to be nonurgent. Messages in this category are collected and sent in a digest form at the time interval specified by the Log Duration field. The security level you select and all levels up to, but not including the lowest Urgent level are considered nonurgent. Messages below the security level you specify are not sent via email.  See the Urgent Message field description for information about the security levels.
Traps Severity	Configures the severity level for trap log messages. See the Urgent Message field description for information about the security levels.

If you make any changes to the page, click **Submit** to apply the change to the system.

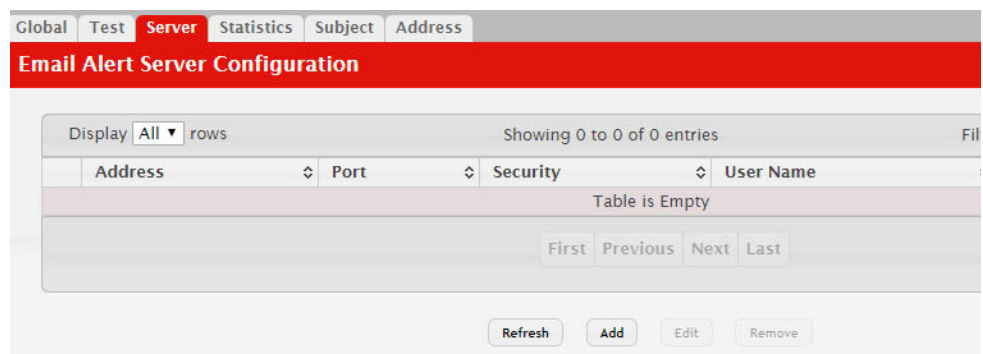
After configuring all email alert settings, click **Test** to send a test message to the configured address(es).

## Email Alert Server Configuration

Use the Email Alert Server Configuration page to configure information about up to three SMTP (mail) servers on the network that can handle email alerts sent from the switch.

To access the Email Alert Server Configuration page, click **System > Advanced Configuration > Email Alerts > Server** in the navigation menu.

**Figure 63.** Email Alert Server



Use the buttons to perform the following tasks:

- To add an SMTP server, click **Add** and configure the desired settings.
- To change information for an existing SMTP server, select the check box associated with the entry and click **Edit**. You cannot edit the host name or address of a server that has been added.
- To delete a configured SMTP server from the list, select the check box associated with the entry to delete and click **Remove**.

**Figure 64.** Email Alert Server Configuration

The screenshot shows a web form titled "Add new Email Server". It contains the following fields:

- Host Name or IP Address:** A text input field with a placeholder and a note "(Max 64 characters or x.x.x.x or x:x:...)".
- Security:** Two radio buttons, "None" (selected) and "TLSv1".
- Port:** A text input field with a note "(1 to 65535) - Recommend 465 for TLS Security, 25 for None".
- User Name:** A text input field with a note "(1 to 49 alphanumeric characters)".
- Password:** A text input field with a note "(1 to 49 characters)".

**Table 60.** Email Alert Server Configuration Fields

Field	Description
Host Name or IP Address	Shows the address or host name of the SMTP server that handles email alerts that the device sends.
Security	Specifies the type of authentication to use with the mail server, which can be TLSv1 (SMTP over SSL) or None (no authentication is required).
Port	Specifies the TCP port that email alerts are sent to on the SMTP server.
User Name	If the Security is TLSv1, this field specifies the user name required to access the mail server.
Password	If the Security is TLSv1, this field specifies the password associated with the configured user name for mail server access. When adding or editing the server, you must retype the password to confirm that it is entered correctly.

If you make any changes to the page, click **Submit** to apply the change to the system. To remove a configured SMTP server, select the Remove check box and click **Delete**.

## Email Alert Statistics

Use the Email Alert Statistics page to view information about email alerts sent from the switch.

To access the Email Alert Statistics page, click **System > Advanced Configuration > Email Alerts > Statistics** in the navigation menu.

**Figure 65.** Email Alert Statistics

**Table 61.** Email Alert Statistics Fields

Field	Description
Number of Emails Sent	Displays the number of email alert messages sent since last reset.
Number of Emails Failed	Displays the number of email alert messages that were unable to be sent since last reset.
Time Since Last Email Sent	Time that has passed since the last email alert message was sent successfully.

To update the page with the most current information, click **Refresh**. To reset the values on the page to zero, click **Clear Counters**.

## Email Alert Subject Configuration

Use the Email Alert Subject Configuration page to configure the subject line of the email alert messages sent from the switch.

To access the Email Alert Subject Configuration page, click **System > Advanced Configuration > Email Alerts > Subject** in the navigation menu.

**Figure 66.** Email Alert Subject Configuration

**Table 62.** Email Alert Subject Configuration Fields

Field	Description
Message Type	Select the appropriate option to configure the subject line of Urgent messages or Nonurgent messages.

**Table 62.** *Email Alert Subject Configuration Fields (continued)*

Field	Description
Email Subject	Specify the text to be displayed in the subject of the email alert message.
Remove	To reset the email alert subject to the default value, select the Remove option associated with the message type to reset, and click <b>Delete</b> .

If you make any changes to the page, click **Submit** to apply the change to the system. To remove a configured Email Subject, select the Remove check box associated with the entry and click **Delete**.

## Email Alert To Address Configuration

Use the Email Alert To Address Configuration page to configure the email addresses to which alert messages sent.

To access the Email Alert To Address Configuration page, click **System > Advanced Configuration > Email Alerts > Address** in the navigation menu.

**Figure 67.** Email Alert To Address Configuration



Use the buttons to perform the following tasks:

- To add an email address to the list of email alert message recipients, click **Add** and configure the desired settings.
- To delete an entry from the list, select the check box associated with each entry to delete and click **Remove**.

**Table 63.** *Email Alert To Address Configuration Fields*

Field	Description
Message Type	Select the appropriate option to configure email address where Urgent messages or Nonurgent messages are sent.
To Address	Specify the email address to which the selected type of messages are sent.

If you make any changes to the page, click **Submit** to apply the change to the system. To remove a configured email address, select the Remove check box associated with the entry and click **Delete**.

## Configuring and Viewing Device Slot Information

The pages in the Slot folder provide information about the cards installed in the slots on the switch. The physical location of the slots depends on the hardware on which CE0128XB/CE0152XB software is running. From the Configuration page, you can also manually configure information about cards on some platforms.

### Slot Card Configuration

Use the Card Configuration page to view information about the cards installed in a switch. On some platforms, you can manually configure information about slots.

To access the Card Configuration page, click **System > Slot > Configuration** in the navigation menu.

**Figure 68.** Slot Configuration



**Table 64.** Slot Configuration Fields

Field	Description
Slot	Identifies the slot number.
Status	Indicates whether the slot is empty or full.
Administrative State	Indicates whether the slot is administratively enabled or disabled. For some devices, you can change the Administrative State when you add or edit slot information.
Power State	Indicates whether the device is providing power to the slot. For some devices, you can change the Power State when you add or edit slot information.
Card Model	The model ID of the card configured for the slot.
Card Description	The description of the card configured for the slot.

Figure 69 shows the fields that display when the slot contains a card.

**Figure 69.** Card Configuration

Edit Existing Card	
Unit	1
Slot	0
Card Index	2
Card Description	Lenovo CE0128P
Status	Full
Administrative State	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Power State	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Inserted Card Model	Lenovo CE0128P
Inserted Card Description	Lenovo CE0128P 24 GE + 4 SFP+ PoE+ Ethernet Line Card
Configured Card Model	Lenovo CE0128P
Configured Card Description	Lenovo CE0128P 24 GE + 4 SFP+ PoE+ Ethernet Line Card
Pluggable	False
Power Down	False

Use the buttons to perform the following tasks:

- To preconfigure a card before adding it to a slot, click **Add** and configure the desired settings.
- To change slot or card settings, select the check box associated with the entry and click **Edit**.
- To delete a slot configuration entry from the list, select the check box associated with each entry to delete and click **Remove**.

**Table 65.** Card Configuration Fields

Field	Description
Unit	Indicates the unit in the stack for which data is to be displayed or configured.
Slot	Indicates the slot in the selected unit for which data is to be displayed or configured.
Card Index	Identifies the index number assigned to the card. This value is helpful when configuring the system by using SNMP.
Card Description	The description of the card configured for the slot.
Status	Indicates whether the slot is empty or full.
Administrative State	Indicates whether the slot is administratively enabled or disabled. For some devices, you can change the Administrative State when you add or edit slot information.
Power State	Indicates whether the device is providing power to the slot. For some devices, you can change the Power State when you add or edit slot information.
Inserted Card Model	The model ID of the card plugged into the slot.
Inserted Card Description	The description of the card plugged into the slot.
Configured Card Model	The model ID of the card configured for the slot.



**Table 65.** *Card Configuration Fields (continued)*

Field	Description
Configured Card Description	The description of the card configured for the slot.
Pluggable	If the value is True, the card can be administratively enabled or disabled. If the value is False, the Administrative State cannot be configured.
Power Down	If the value is True, the Power State can be administratively enabled or disabled. If the value is False, the Power State cannot be configured.

- If you make any changes to the page, click **Submit** to apply the changes to the system.
- If you want the device to retain these changes across a reset, you must first save the configuration by clicking **Save Configuration**.
- Click **Refresh** to redisplay the page with the current data from the switch.

## Supported Cards

The Supported Cards page provides information about the cards that your platform supports.

To access the Supported Cards page, click **System > Slot > Supported Cards** in the navigation menu.

**Figure 70.** Supported Cards

Card Index	Supported Cards	Card Type	Card Model	Card Type
1	Lenovo CE0128T	0x56150103	Lenovo CE0128T	Lenovo CE0128T
2	Lenovo CE0128P	0x56150104	Lenovo CE0128P	Lenovo CE0128P
3	Lenovo CE0152T	0x56150105	Lenovo CE0152T	Lenovo CE0152T
4	Lenovo CE0152P	0x56150106	Lenovo CE0152P	Lenovo CE0152P

**Table 66.** *Supported Card Fields*

Field	Description
Card Index	Displays the index assigned to the selected card type.

**Table 66.** *Supported Card Fields (continued)*

<b>Field</b>	<b>Description</b>
Supported Cards	The menu contains the list of all cards that the system can support. To view information about a card, select it from the drop-down list. The screen refreshes, and the information about that card appears in the other fields on the page.
Card Type	Displays the hardware type of this supported card. This is a 32-bit data field.
Card Model ID	Displays the string to identify the model of the supported card.
Card Descriptor	Displays a data field used to identify the supported card.

Click **Refresh** to redisplay the most current information from the router.

## Configuring Power Over Ethernet (PoE) and PoE Statistics

Use these pages to view Power over Ethernet (PoE) status information, configure global PoE settings, configure PoE settings on interfaces and view PoE interface statistical information.

### PoE Configuration

Use this page to view Power over Ethernet (PoE) status information and configure global PoE settings.

To access the PoE Configuration page, click **System > PoE > Configuration** in the navigation menu.

**Figure 71.** PoE Configuration

PoE Configuration	
Unit	1 ▾
Firmware Version	1.5.0.2
Operational Status	Off
Total Power Available (mWatts)	185000
Threshold Power (mWatts)	166500
Consumed Power (mWatts)	0
System Usage Threshold (%)	90 (1 to 99)
Power Management Mode	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic
Port Auto Reset Mode	<input type="checkbox"/>
Traps	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

**Table 67.** PoE Configuration Fields

Field	Description
Firmware Version	The firmware version of the PoE software component.
Operational Status	The current status of the switch PoE functionality, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>On</b> – At least one port on the switch is delivering power to a connected device.</li> <li>• <b>Off</b> – The PoE functionality is operational but no ports are delivering power.</li> <li>• <b>Faulty</b> – The PoE functionality is not operational.</li> </ul>
Total Power Available	The total power in mWatts that can be provided by the switch.
Threshold Power	When the PoE power being used exceeds this threshold, a trap is generated to the system log to alert the system administrator of high power usage. This value is determined by the configurable <b>System Usage Threshold</b> percent.
Consumed Power	The amount of power in mWatts currently being consumed by connected PoE devices.

**Table 67.** PoE Configuration Fields (continued)

Field	Description
System Usage Threshold	A percentage of the total power available. This percentage determines the <b>Threshold Power</b> .
Power Management Mode	The method by which the PoE controller determines supplied power, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Static</b> – The power allocated to each port is reserved and is not available to any other port, even when less than the maximum allocation is being used.</li> <li>• <b>Dynamic</b> – The power allocated to each port is not reserved. Unused power may be allocated from one port to another as needed, up to the power limit defined for each port.</li> </ul>
Port Auto Reset Mode	When enabled, the switch automatically resets a PoE port if an error condition occurs. When disabled, the administrator must reset the port manually.
Traps	When enabled, SNMP traps will be generated when certain events occur. Trap events include a change in whether power is being delivered on a port and when the power usage threshold is exceeded.

- If you make any changes to the page, click **Submit** to apply the changes to the system.
- Click **Refresh** to redisplay the page with the current data from the switch.

## PoE Port Configuration

Use this page to configure PoE settings on interfaces.

To access the PoE Configuration page, click **System > PoE > Port Configuration** in the navigation menu.

**Figure 72.** PoE Port Configuration

Interface	Admin Mode	Priority	High Power Mode	Power Limit Type	Power Limit	Detection Type	Timer Schedule	Status	Fault Status
1/0/1	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error
1/0/2	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error
1/0/3	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error
1/0/4	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error
1/0/5	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error
1/0/6	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error
1/0/7	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error
1/0/8	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error
1/0/9	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error
1/0/10	Enabled	Low	Dot3at	Class	N/A	4Pt-Dot3af	None	Searching	No Error

**Table 68.** PoE Port Configuration Fields

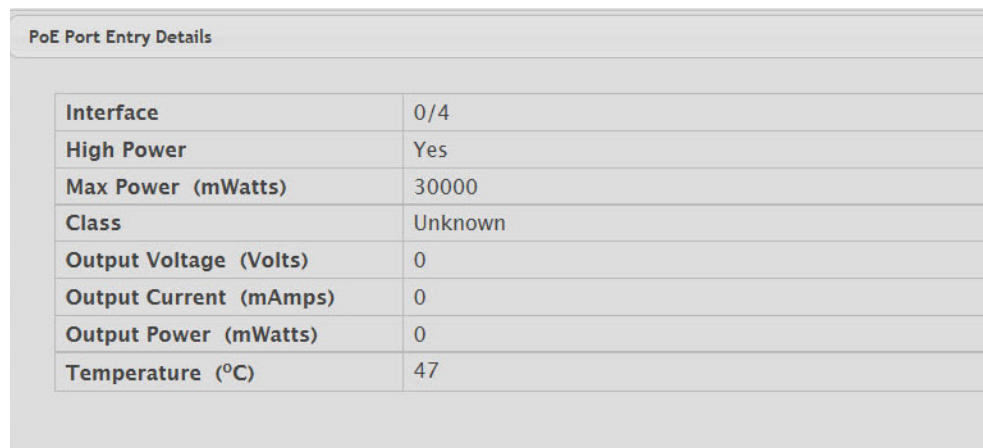
Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring PoE settings, this field identifies the interface(s) being configured.
Admin Mode	Indicates whether PoE is administratively enabled or disabled on the interface.
Priority	The priority of the port when allocating available power. Power is delivered to the higher priority ports when needed before providing it to the lower priority ports. Possible values are <b>Critical</b> , <b>High</b> , and <b>Low</b> .
High Power Mode	When enabled, the port supports the PoE+ power standard, which allows for providing up to 30W of power. When disabled, the port supports the original PoE standard only, which allows for providing up to 15.4W of power.
Power Limit Type	The type of power limiting used for the port, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Class</b> – The device class determines the power limit. The switch learns the class of the device through the receipt of Link Layer Discovery Protocol (LLDP) messages.</li> <li>• <b>User</b> – The power limit is user defined, overriding the LLDP information. When set to <b>User</b>, the Power Limit field is enabled.</li> </ul>
Power Limit	The power limit for the port, which can be specified. This field displays only when <b>Power Limit Type</b> is set to <b>User</b> .
Detection Type	The protocol(s) that can be used to detect the presence of a PD when connected to a PoE port. The IEEE specification 802.3af (Dot3af) specifies various detection algorithms. Some PDs use legacy detection algorithms that were in place prior to the 802.3af standard, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Legacy</b> – The switch uses a legacy detection scheme not defined in 802.3af.</li> <li>• <b>4Pt-Dot3af</b> – The switch uses the 802.3af 4-point detection scheme only.</li> <li>• <b>4Pt-Dot3af + Legacy</b> – The switch uses the 802.3af 4-point detection scheme, followed by the legacy detection scheme.</li> <li>• <b>2Pt-Dot3af</b> – The switch uses the 802.3af 2-point detection scheme.</li> <li>• <b>2Pt-Dot3af + Legacy</b> – The switch uses the 802.3af 2-point detection scheme, followed by the legacy detection scheme.</li> <li>• <b>None</b> – No detection is performed.</li> </ul>
Timer Schedule	The time range from the list of time ranges configured on the system.
Status	The status of the port as a provider of PoE. Such devices are referred to as PSE. The status can be one of the following: <ul style="list-style-type: none"> <li>• <b>Disabled</b> – The PSE is disabled.</li> <li>• <b>Delivering Power</b> – The PSE is delivering power.</li> <li>• <b>Fault</b> – The PSE has experienced a fault condition.</li> <li>• <b>Test</b> – The PSE is in test mode.</li> <li>• <b>Other Fault</b> – The PSE has experienced a variable error condition.</li> <li>• <b>Searching</b> – The PSE is transitioning between states.</li> <li>• <b>Requesting Power</b> – The PSE is currently not able to deliver power because power is unavailable to the port.</li> </ul>

**Table 68.** PoE Port Configuration Fields (continued)

Field	Description
Fault Status	<p>The error when PSE port is in fault status, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>None</b> – PSE port is not in any error state.</li> <li>• <b>MPS Absent</b> – PSE port has detected absence of main power supply.</li> <li>• <b>Short</b> – PSE port has detected a short circuit condition.</li> <li>• <b>Overload</b> – PD connected to PSE port tried to draw more power than permissible by the hardware.</li> <li>• <b>Power Denied</b> – PSE port has been denied power due to administrative action or shortage of power.</li> </ul>

To display additional PoE interface information, select an entry and click **Details**.

**Figure 73.** PoE Port Entry Details



PoE Port Entry Details	
Interface	0/4
High Power	Yes
Max Power (mWatts)	30000
Class	Unknown
Output Voltage (Volts)	0
Output Current (mAmps)	0
Output Power (mWatts)	0
Temperature (°C)	47

**Table 69.** PoE Port Entry Details

Field	Description
High Power	Indicates whether high power mode is enabled or disabled.
Max Power	If Power Limit Type for the port is set to User (user defined), this field displays the configured power limit. If Power Limit Type is set to Class, this field is blank.
Class	If Power Limit Type is set to Class, this field displays the class of the connected device, as learned in LLDP messages. Possible values are Unknown and Class 0 through Class 4. A higher class value indicates that the device requires higher power.
Output Voltage	The voltage being applied to the connected device.
Output Current	The current in milliamps being drawn by the powered device.
Output Power	The power in mWatts being drawn by the connected device.
Temperature	The temperature measured at the PoE port.

Use the buttons to perform the following tasks:

- To configure the settings for one or more interfaces, select each entry to modify and click **Edit**.

- To apply the same settings to all interfaces, click **Edit All**.

## PoE Port Statistics

Use this page to view PoE interface statistical information.

To access the PoE Port Statistics page, click **System > PoE > Statistics** in the navigation menu.

**Figure 74.** PoE Port Statistics

Interface	1/0/1 ▾
Overload Counter	0
Short Counter	0
Power Denied Counter	0
MPS Absent Counter	0
Invalid Signature Counter	0

[Refresh](#)

**Table 70.** PoE Port Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data on the page.
Overload Counter	Number of times there has been a power overload. Power overload occurs when a powered device connected to a port tries to draw more power than permissible by the hardware.
Short Counter	Number of times there has been a short circuit condition.
Power Denied Counter	Number of times the powered device has been denied power. Power is denied due to administrative action or shortage of power.
MPS Absent Counter	Number of times power has stopped because the powered device was not detected.
Invalid Signature Counter	Number of times an invalid signature was received. Signature detection is a stage in detecting the presence of a powered device, where a resistance value on the powered device is expected to be found within a particular range.

- Click **Refresh** to redisplay the page with the current data from the switch.

# Viewing Device Port Information

The pages in the Port folder allow you to view and monitor the physical port information for the ports available on the switch. The Port folder has links to the following pages:

## Port Summary

Use the Port Summary page to view the settings for all physical ports on the platform.

To access the Port Summary page, click **System > Port > Summary** in the navigation menu.

**Figure 75.** Port Summary

Summary	Description	Cable Test	Mirroring	Mirroring Summary						
<b>Port Summary</b>										
Display	10	rows	Showing 1 to 10 of 92 entries							
	Filter:									
<input type="checkbox"/>	Interface	Interface Index	Type	Admin Mode	Physical Mode	Physical Status	Auto Negotiate Capabilities	STP Mode	LACP Mode	Link Status
<input type="checkbox"/>	1/0/1	1	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
<input type="checkbox"/>	1/0/2	2	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
<input type="checkbox"/>	1/0/3	3	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
<input type="checkbox"/>	1/0/4	4	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
<input type="checkbox"/>	1/0/5	5	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
<input type="checkbox"/>	1/0/6	6	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
<input type="checkbox"/>	1/0/7	7	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
<input type="checkbox"/>	1/0/8	8	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
<input type="checkbox"/>	1/0/9	9	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
<input type="checkbox"/>	1/0/10	10	Normal	Enabled	Auto	Unknown	10h   10f   100h   100f   1000f	Enabled	Enabled	Link Down
First Previous 1 2 3 4 5 Next Last										

**Table 71.** Port Summary Fields

Field	Description
Interface	Identifies the port that the information in the rest of the row is associated with.
Interface Index	The interface index object value assigned by the IF-MIB. This value is used to identify the interface when managing the device by using SNMP.



**Table 71.** Port Summary Fields (continued)

Field	Description
Type	<p>For most ports this field is blank. Otherwise, the possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Normal</b> - The port is a normal port, which means it is not a LAG member or configured for port mirroring.</li> <li>• <b>Trunk Member</b> - The port is a member of a LAG.</li> <li>• <b>Mirrored</b> - Indicates that the port has been configured as a monitoring port and is the source port in a port mirroring session. For more information about port monitoring and probe ports, see <a href="#">“Mirroring” on page 142</a>.</li> <li>• <b>Probe</b> - Indicates that the port has been configured as a monitoring port and is the destination port in a port mirroring session. For more information about port monitoring and probe ports, see <a href="#">“Mirroring” on page 142</a>.</li> </ul>
Admin Mode	<p>Shows the port control administration state, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The port can participate in the network (default).</li> <li>• <b>Disabled:</b> The port is administratively down and does not participate in the network.</li> </ul>
Physical Mode	<p>Shows the speed and duplex mode at which the port is configured:</p> <ul style="list-style-type: none"> <li>• <b>Auto:</b> The duplex mode and speed will be set by the auto-negotiation process. The port's maximum capability will be advertised. The option to enable auto-negotiation</li> <li>• <b>&lt;Speed&gt; Half Duplex:</b> The port speeds available from the menu depend on the platform on which the CE0128XB/CE0152XB software is running and which port you select. In half-duplex mode, the transmissions are one-way. In other words, the port does not send and receive traffic at the same time.</li> <li>• <b>&lt;Speed&gt; Full Duplex:</b> The port speeds available from the menu depend on the platform on which the CE0128XB/CE0152XB software is running and which port you select. In half-duplex mode, the transmissions are two-way. In other words, the port can send and receive traffic at the same time.</li> </ul> <p>The physical mode for a LAG is reported as <i>LAG</i>.</p>
Physical Status	<p>Indicates the port speed and duplex mode at which the port is operating. The physical status for LAGs is not reported. When a port is down, the physical status is unknown.</p>
Auto Negotiate Capabilities	<p>Indicates the list of configured capabilities for a port when Auto Negotiate is on. The Capability status for LAGs is not reported.</p>
STP Mode	<p>The Spanning Tree Protocol (STP) Administrative Mode associated with the port or LAG. STP is a layer 2 protocol that provides a tree topology for switches on a bridged LAN. STP allows a network to have redundant paths without the risk of network loops, by providing a single path between end stations on a network. The possible values for STP mode are:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b> - Spanning tree is enabled for this port.</li> <li>• <b>Disable</b> - Spanning tree is disabled for this port.</li> </ul>

**Table 71.** Port Summary Fields (continued)

Field	Description
LACP Mode	Indicates the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation. This field can have the following values: <ul style="list-style-type: none"> <li>• <b>Enable:</b> Specifies that the port is allowed to participate in a port channel (LAG), which is the default mode.</li> <li>• <b>Disable:</b> Specifies that the port cannot participate in a port channel (LAG).</li> <li>• <b>N/A:</b> For LAG ports.</li> </ul>
Link Status	Indicates whether the Link is up or down.

The following fields can be accessed by selecting a port and clicking **Edit**.

**Figure 76.** Edit Port Configuration Fields

**Table 72.** Edit Port Configuration Fields

Field	Description
Auto Negotiate	Select this option to enable auto negotiation on the port.
Speed	Select this option to manually configure the physical mode for the port (speed and duplex mode).
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Specifies that the system sends a trap when the link status changes.</li> <li>• <b>Disable:</b> Specifies that the system does not send a trap when the link status changes.</li> </ul>
Maximum Frame Size	The maximum Ethernet frame size the interface supports or is configured to support. The maximum frame size includes the Ethernet header, CRC, and payload.

**Table 72.** *Edit Port Configuration Fields (continued)*

Broadcast Storm Recovery Mode	<p>Specifies the broadcast storm control threshold for the port. Broadcast storm control limits the amount of broadcast frames accepted and forwarded by the port. If the broadcast traffic on the Ethernet port exceeds the configured threshold, the system blocks (discards) the broadcast traffic.</p> <p>Specifies the broadcast storm recovery action to either Shutdown or Trap for specific interface. If configured to <b>Shutdown</b>, the interface which receives broadcast packets at a rate which is above threshold is diagnostically disabled. The <b>Trap</b> option sends trap messages at approximately every 30 seconds until broadcast storm control recovers.</p>
Multicast Storm Recovery Level	<p>Specifies the multicast storm control threshold for the port. Multicast storm control limits the amount of multicast frames accepted and forwarded by the port. If the multicast traffic on the Ethernet port exceeds the configured threshold, the system blocks (discards) the multicast traffic.</p> <p>Specifies the multicast storm recovery action to either Shutdown or Trap for specific interface. If configured to <b>Shutdown</b>, the interface which receives multicast packets at a rate which is above threshold is diagnostically disabled. The option <b>Trap</b> sends trap messages at approximately every 30 seconds until multicast storm control recovers.</p>
Unicast Storm Recovery Level	<p>Specifies the unicast storm control threshold for the port. Unicast storm control limits the amount of unicast frames accepted and forwarded by the switch. If the unicast traffic on the Ethernet port exceeds the configured threshold, the system blocks (discards) the unicast traffic.</p> <p>Specifies the unicast storm recovery action to either Shutdown or Trap for specific interface. If configured to <b>Shutdown</b>, the interface which receives unicast packets at a rate which is above threshold is diagnostically disabled. The <b>Trap</b> option sends trap messages at approximately every 30 seconds until unicast storm control recovers.</p>

Click **Refresh** to redisplay the most current information from the router.

## Port Description

Use the Port Description page to configure a human-readable description of the port.

To access the Port Description page, click **System > Port > Description** in the navigation menu.

**Figure 77.** Port Description

Interface	Physical Address	PortList Bit Offset	Interface Index	Port Description
1/0/1	80:96:21:F1:01:02	1	1	
1/0/2	80:96:21:F1:01:02	2	2	
1/0/3	80:96:21:F1:01:02	3	3	
1/0/4	80:96:21:F1:01:02	4	4	
1/0/5	80:96:21:F1:01:02	5	5	
1/0/6	80:96:21:F1:01:02	6	6	
1/0/7	80:96:21:F1:01:02	7	7	
1/0/8	80:96:21:F1:01:02	8	8	
1/0/9	80:96:21:F1:01:02	9	9	
1/0/10	80:96:21:F1:01:02	10	10	

**Table 73.** Port Description Fields

Field	Description
Interface	Select the interface for which data is to be displayed or configured.
Port Description (Input field)	A user-configurable description to help identify the port. To add a description to a port, select the port or LAG from the Interface drop-down menu, type a description in the Port Description field, and then click <b>Submit</b> .
Physical Address	Displays the physical address of the specified interface.
PortList Bit Offset	Displays the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.
Interface Index	The interface index object value assigned by the IF-MIB. This value is used to identify the interface when managing the device by using SNMP.
Port Description	Shows the configured port description. By default, the port does not have an associated description.

- If you change a port description, click **Submit** to apply the change to the system.
- Click **Refresh** to redisplay the page with the latest information from the router.

## Cable Test

The cable test feature enables you to determine the cable connection status on a selected port. You can also obtain an estimate of the length of the cable connected to the port, if the PHY on the ports supports this functionality.

**Note:** The cable test feature is supported only for copper cable. It is not supported for optical fiber cable.

To access the Cable Test feature, click **System > Port > Cable Test**.

The page displays with additional fields when you click **Test Cable**. The fields that display depend on the cable test results.

**Figure 78.** Cable Test

The screenshot shows a web interface with a navigation bar containing tabs: Summary, Description, Cable Test (highlighted), Mirroring, and Mirroring Summary. Below the navigation bar is a red header titled 'Port Cable Test'. Underneath, there is a form with the following fields:

- Interface:** A dropdown menu currently showing '1/0/1'.
- Failure Location Distance:** A text input field.
- Cable Length (Meters):** A text input field.
- Cable Status:** A text input field.

At the bottom right of the form is a button labeled 'Test Cable'.

**Table 74.** Cable Test Fields

Field	Description
Interface	If the test has not been performed, this is the only field that displays. Select the interface to test. After the test has been performed, this field shows the interface that was tested.
Cable Status	This displays the cable status as Normal, Open, or Short. <ul style="list-style-type: none"> <li>• <b>Normal:</b> The cable is working correctly.</li> <li>• <b>Open:</b> The cable is disconnected or there is a faulty connector.</li> <li>• <b>Open and Short:</b> There is an electrical short in the cable.</li> <li>• <b>Cable status Test Failed:</b> The cable status could not be determined. The cable may in fact be working. This field is displayed after you click Test Cable and results are available.</li> </ul>
Cable Length	The estimated length of the cable. If the cable length cannot be determined, Unknown is displayed. This field shows the range between the shortest estimated length and the longest estimated length. <b>Note:</b> This field displays a value only when the Cable Status is Normal; otherwise, this field is blank.
Failure Location	The estimated distance from the end of the cable to the failure location. <b>Note:</b> This field displays a value only when the Cable Status is Open or Short; otherwise, this field is blank.

Select a port and click **Test Cable** to display its status.

If the port has an active link while the cable test is run, the link can go down for the duration of the test. The test may take several seconds to run.

The command returns a cable length estimate if this feature is supported by the PHY for the current link speed.

**Note:** If the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded.

# Mirroring

Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port. You have the ability to configure how traffic is mirrored on a source port. Packets that are received on the source port, that are transmitted on a port, or are both received and transmitted, can be mirrored to the destination port.

The packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN tagged or untagged as it is being transmitted on the source port.

Use the Multiple Port Mirroring page to define port mirroring sessions.

To access the Multiple Port Mirroring page, click **System > Port > Mirroring** in the navigation menu.

**Figure 79.** Multiple Port Mirroring

Session ID	1
Mode	Disabled
Destination	None
IP ACL	None
MAC ACL	None

Display All rows      Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Source	Direction
Table is Empty		

First Previous Next Last

Refresh    Configure Session    Configure Source    Remove Source

Use the buttons to perform the following tasks:

- To configure the administrative mode for a port mirroring session, click **Configure Session** and configure the desired settings.
- To configure the port mirroring destination, click the **Edit** icon in the Destination field and configure the desired settings.
- To configure one or more source ports for the mirroring session and to determine which traffic is mirrored (Tx, Rx, or both), click **Configure Source** and configure the desired settings.
- To remove one or more source ports from the port mirroring session, select the check box associated with each source port to remove and click **Remove Source**.

**Table 75.** *Multiple Port Mirroring Fields*

Field	Description
Session ID	The port mirroring session ID. The number of sessions allowed is platform specific.
Mode	The administrative mode for the selected port mirroring session. If the mode is disabled, the configured source is not mirroring traffic to the destination.
Destination	The interface to which traffic is mirrored, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Remote VLAN</b> – Traffic is mirrored to the VLAN on the system that is configured as the RSPAN VLAN. In an RSPAN configuration, the destination should be the Remote VLAN on any device that does not have a port connected to the network traffic analyzer. This destination has to be configured with RSPAN VLAN membership.</li> <li>• <b>Interface</b> – Traffic is mirrored to a physical port on the local device. The interface is the probe port that is connected to a network traffic analyzer.</li> <li>• <b>None</b> – The destination is not configured.</li> </ul> <p><b>Note:</b> This field also identifies the status of the Remove RSPAN Tag option, which can be configured in the Destination Configuration window. When this option is set as False, packets received at the RSPAN destination port are double tagged. When the Remove RSPAN Tag option is True, the RSPAN VLAN ID tag is removed for the mirroring session.</p>
IP ACL	The IP access-list ID or name attached to the port mirroring session.
MAC ACL	The MAC access-list name attached to the port mirroring session.
Source	The ports or VLAN configured to mirror traffic to the destination. You can configure multiple source ports or one source VLAN per session. The source VLAN can also be a remote VLAN.
Direction	The direction of traffic on the source port(s) that is sent to the probe port. Possible values are: <ul style="list-style-type: none"> <li>• <b>Tx and Rx</b> – Both ingress and egress traffic.</li> <li>• <b>Rx</b> – Ingress traffic only.</li> <li>• <b>Tx</b> – Egress traffic only.</li> </ul>

## Configuring a Port Mirroring Session

**Note:** If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

1. From the Multiple Port Mirroring page, select the Session ID of the port mirroring session to configure and click **Configure Session** to display the **Session Configuration** page.

2. Configure the following fields:

**Table 76.** Multiple Port Mirroring—Session Configuration

Field	Description
Session ID	The port mirroring session ID. The number of sessions allowed is platform specific.
Mode	The administrative mode for the selected port mirroring session. If the mode is disabled, the configured source is not mirroring traffic to the destination.

3. Click **Submit** to apply the changes to the system.

## Configuring a Port Mirroring Source

**Note:** If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

1. From the Multiple Port Mirroring page, click **Configure Source** to display the **Source Configuration** page.



2. Configure the following fields:

**Table 77.** *Multiple Port Mirroring—Source Configuration*

Field	Description
Session ID	The port mirroring session ID. The number of sessions allowed is platform specific.
Type	The type of interface to use as the source: <ul style="list-style-type: none"> <li>• <b>None</b> – The source is not configured.</li> <li>• <b>Remote VLAN</b> – The VLAN configured as the RSPAN VLAN is the source. In an RSPAN configuration, the remote VLAN is the source on the destination device that has a physical port connected to the network traffic analyzer.</li> <li>• <b>VLAN</b> – Traffic to and from a configured VLAN is mirrored. In other words, all the packets sent and received on all the physical ports that are members of the VLAN are mirrored.</li> <li>• <b>Interface</b> – Traffic is mirrored from one or more physical ports on the device.</li> </ul>
Remote VLAN	The VLAN that is configured as the RSPAN VLAN.
VLAN ID	The VLAN to use as the source. Traffic from all physical ports that are members of this VLAN is mirrored. This field is available only when the selected Type is VLAN.
Available Source port(s)	The physical port or ports to use as the source. To select multiple ports, <b>CTRL</b> + click each port. This field is available only when the selected Type is Interface.
Direction	The direction of traffic on the source port (or source ports) or VLAN that is sent to the specified destination. A source VLAN mirrors all received and transmitted packets to the destination. Possible values for source ports are: <b>Tx and Rx</b> – Both ingress and egress traffic. <b>Rx</b> – Ingress traffic only. <b>Tx</b> – Egress traffic only.

3. Click **Submit** to apply the changes to the system.

### *Configuring the Destination Port for a Port Mirroring Session*

**Note:** A port will be removed from a VLAN or LAG when it becomes a destination mirror.

1. From the Multiple Port Mirroring page, select the Session ID of the port mirroring session to configure and click **the Edit icon in the Destination field.**

2. Configure the following fields:

**Table 78.** Multiple Port Mirroring—Session Configuration

Field	Description
Session ID	The port mirroring session ID. The number of sessions allowed is platform specific.
Type	The type of interface to use as the destination: <ul style="list-style-type: none"> <li>• <b>None</b> – The destination is not configured.</li> <li>• <b>Remote VLAN</b> – Traffic is mirrored to the VLAN on the system that is configured as the RSPAN VLAN. In an RSPAN configuration, the destination should be the Remote VLAN on any device that does not have a port connected to the network traffic analyzer.</li> <li>• <b>Interface</b> – Traffic is mirrored to a physical port on the local device. The interface is the probe port that is connected to a network traffic analyzer.</li> </ul>
Remote VLAN	The VLAN that is configured as the RSPAN VLAN.
Port	The port to which traffic is mirrored. If the Type is Remote VLAN, the selected port is a reflector port. The reflector port is a trunk port that carries the mirrored traffic towards the destination device. If the Type is Interface, the selected port is the probe port that is connected to a network traffic analyzer.
Remove RSPAN Tag	The packets received at RSPAN destination port are double tagged. Enable this option to remove RSPAN VLAN ID tag for mirroring session.

3. Click **Submit** to apply the changes to the system.

## Removing or Modifying a Port Mirroring Session

1. From the Port Mirroring page, click **Remove Source Port.**
2. Select one or more source ports to remove from the session.  
Use the **CTRL** key to select multiple ports to remove.
3. Click **Remove.**

The source ports are removed from the port mirroring session, and the device is updated.

## Mirroring Summary

Use the Multiple Port Mirroring Summary page to view the port mirroring summary.

To access the Multiple Port Mirroring Summary page, click **System > Port > Mirroring Summary** in the navigation menu.

**Figure 80.** Multiple Port Mirroring Summary

Session ID	Admin Mode	Probe Port	Remove RSPAN Tag	Src VLAN	Mirrored Port	Reflector Port	Src RVLAN
1	Disabled						
2	Disabled						
3	Disabled						
4	Disabled						

**Table 79.** Multiple Port Mirroring Summary Fields

Field	Description
Session ID	The port mirroring session ID. The number of sessions allowed is platform specific.
Admin Mode	The administrative mode for the selected port mirroring session. If the mode is disabled, the configured source is not mirroring traffic to the destination.
Probe Port	The interface that receives traffic from all configured source ports.
Remove RSPAN Tag	The packets received at an RSPAN destination port are double tagged. If this option is True, the RSPAN VLAN ID tag is removed for the mirroring session.
Src VLAN	The VLAN configured to mirror traffic to the destination. You can configure one source VLAN per session. The source VLAN can also be a remote VLAN.
Mirrored Port	The ports configured to mirror traffic to the destination. You can configure multiple source ports per session.
Reflector Port	This port carries all the mirrored traffic at source switch.
Src RVLAN	The VLAN configured as the RSPAN VLAN is the source. In an RSPAN configuration, the remote VLAN is the source on the destination device that has a physical port connected to the network traffic analyzer.

**Table 79.** Multiple Port Mirroring Summary Fields (continued)

Field	Description
Dst RVLAN	Traffic is mirrored to the VLAN on the system that is configured as the RSPAN VLAN. In an RSPAN configuration, the destination should be the Remote VLAN on any device that does not have a port connected to the network traffic analyzer.
Type	The type of traffic on the source port (or source ports) or VLAN that is sent to the specified destination. A source VLAN mirrors all received and transmitted packets to the destination. Possible values for source ports are: <ul style="list-style-type: none"> <li>• <b>Tx and Rx</b> – Both ingress and egress traffic.</li> <li>• <b>Rx</b> – Ingress traffic only.</li> <li>• <b>Tx</b> – Egress traffic only.</li> </ul>
IP ACL	The ID of the IP ACL to apply to traffic from the source. Only traffic that matches the rules in the ACL is mirrored to the destination.
MAC ACL	The ID of the MAC ACL to apply to traffic from the source. Only traffic that matches the rules in the ACL is mirrored to the destination.

- Click **Refresh** to redisplay the page with the latest information from the router.

## Port Green Mode Statistics

For platforms that include Green Energy features, the Green Mode Statistics page shows information about the amount of energy saved for each port. This page also allows you to enable or disable the green mode features that the switch supports. The green mode features can be controlled on a port-by-port basis.

To access the Green Mode Statistics page, click **System > Advanced Configuration > Green Ethernet > Statistics**.

**Figure 81.** Port Green Ethernet Statistics

Interface	Rx Low Power Idle Event Count	Rx Low Power Idle Duration	Tx Low Power Idle Event Count	Tx Low Power Idle Duration	Time Since Counters Last Cleared
1	0		0		3d:06:32:40
2	0		0		3d:06:32:40
3	0		0		3d:06:32:40
4	0		0		3d:06:32:40
5	0		0		3d:06:32:40
6	0		0		3d:06:32:40
7	0		0		3d:06:32:40
8	0		0		3d:06:32:40
9	0		0		3d:06:32:40
10	0		0		3d:06:32:40

**Table 80.** *Green Ethernet Statistics Fields*

Field	Description
Interface	The interface associated with the rest of the data in the row. The table includes all interfaces that are enabled for EEE.
Rx Low Power Idle Event Count	The number of times the local interface has entered a low-power idle state.
Rx Low Power Idle Duration	The amount of time (in 10 microsecond increments) the local interface has spent in a low-power idle state.
Tx Low Power Idle Event Count	The number of times the link partner has entered a low-power idle state.
Tx Low Power Idle Duration	The amount of time (in 10 microsecond increments) the link partner has spent in a low-power idle state.
Time Since Counters Last Cleared	The amount of time since the statistics on this page were reset to zero.

### Command Buttons

This page has the following command buttons:

- **Clear**—Resets all Green Ethernet statistics counters on this page to 0.
- **Refresh**—Refresh the data on the screen with the present state of the data in the switch.

## Port Green Mode EEE History

Use the Green Mode EEE History page to set the sampling interval for EEE LPI data and to specify the number of samples to keep. From this page, you can also view per-port EEE LPI data.

To access the Green Mode Statistics page, click **System > Advanced Configuration > Green Ethernet > EEE History**.

**Figure 82.** Green Mode EEE History



**Table 81.** *Green Mode EEE History Fields*

Field	Description
Interface	Select the interface with the green mode information to view or configure.

**Table 81.** *Green Mode EEE History Fields (continued)*

<b>Field</b>	<b>Description</b>
EEE LPI History Sampling Interval	The amount of time to wait between collecting LPI samples on the device.
EEE LPI History Maximum	The maximum number of samples maintained in the LPI history table.
EEE Low Power Idle	The administrative status of EEE on the device.
Sample No.	A unique number that identifies the sample.
Age	The amount of time that has passed since the sample was recorded.
% Time in LPI since last sample	The percentage of time the interface has spent in LPI mode since the last sample was taken.
% Time in LPI since last reset	The percentage of time the interface has spent in LPI mode since the last time the EEE statistics were cleared.

---

## Configuring sFlow

sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a standalone probe) and a central sFlow Collector. The sFlow Agent uses sampling technology to capture traffic statistics from the device it is monitoring. sFlow datagrams are used to immediately forward the sampled traffic statistics to an sFlow Collector for analysis.

The sFlow Agent uses two forms of sampling: statistical packet-based sampling of switched or routed Packet Flows, and time-based sampling of counters.

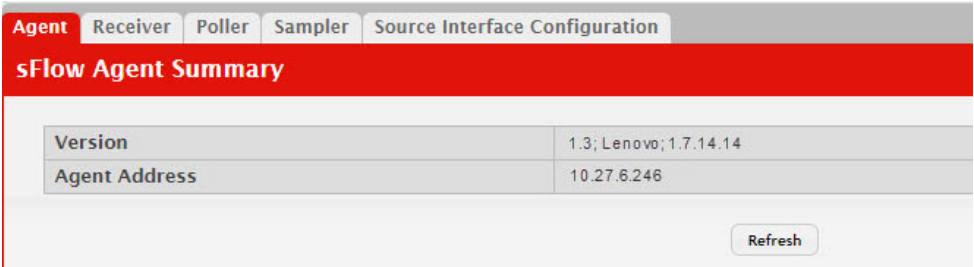
### sFlow Agent Summary

Packet Flow Sampling and Counter Sampling are performed by sFlow Instances associated with individual Data Sources within the sFlow Agent. Packet Flow Sampling and Counter Sampling are designed as part of an integrated system. Both types of samples are combined in sFlow datagrams. Packet Flow Sampling will cause a steady, but random, stream of sFlow datagrams to be sent to the sFlow Collector. Counter samples may be taken opportunistically in order to fill these datagrams.

In order to perform Packet Flow Sampling, an sFlow Sampler Instance is configured with a Sampling Rate. The Packet Flow sampling process results in the generation of Packet Flow Records. In order to perform Counter Sampling, the sFlow Poller Instance is configured with a Polling Interval. The Counter Sampling process results in the generation of Counter Records. The sFlow Agent collects Counter Records and Packet Flow Records and sends them in the form of sFlow datagrams to sFlow Collectors.

To access the sFlow Agent Summary page, click **System > Advanced Configuration > sFlow > Agent** in the navigation menu.

**Figure 83.** sFlow Agent Summary



sFlow Agent Summary	
Version	1.3; Lenovo; 1.7.14.14
Agent Address	10.27.6.246

**Table 82.** *sFlow Agent Summary Fields*

Field	Description
Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: <ul style="list-style-type: none"> <li>• MIB Version: '1.3', the version of this MIB.</li> <li>• Organization: Lenovo</li> <li>• Revision: 1.0</li> </ul>
Agent Address	The IP address associated with this agent.

Use the **Refresh** button to refresh the page with the most current data from the switch.

## sFlow Receiver Configuration

Use the sFlow Receiver Configuration page to configure the sFlow Receiver.

To access the sFlow Receiver Configuration page, click **System > Advanced Configuration > sFlow > Receiver** in the navigation menu.

**Figure 84.** sFlow Receiver Configuration

Index	Owner String	Time Remaining	Maximum Datagram Size	Address	Port	Datagram Version
1		0	1400	0.0.0.0	6343	5
2		0	1400	0.0.0.0	6343	5
3		0	1400	0.0.0.0	6343	5
4		0	1400	0.0.0.0	6343	5
5		0	1400	0.0.0.0	6343	5
6		0	1400	0.0.0.0	6343	5
7		0	1400	0.0.0.0	6343	5
8		0	1400	0.0.0.0	6343	5

**Table 83.** *sFlow Receiver Configuration Fields*

Field	Description
Index	Selects the receiver for which data is to be displayed or configured. The allowed range is 1 to 8.
Owner String	The entity making use of this sFlowRcvrTable entry. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string. The entry must be claimed before any changes can be made to other sampler objects.



**Table 83.** sFlow Receiver Configuration Fields

Field	Description
Time Remaining	The time (in seconds) remaining before the sampler is released and stops sampling. A value of 0 essentially means the receiver is not configured. When configuring the sFlow receiver settings, you must select the Timeout Mode option before you can configure a Timeout Value.
Maximum Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. The manager should set this value to avoid fragmentation of the sFlow datagrams. The default value is 1400. The allowed range is 200 to 9116.
Address	The IP address of the sFlow collector. If set to 0.0.0.0 no sFlow datagrams will be sent.
Port	The destination port for sFlow datagrams. The allowed range is 1 to 65535.
Datagram Version	The version of sFlow datagrams that should be sent.
Monitor Session	Monitor session to enable sFlow hardware feature.

- Use the **Submit** button to sent updated data to the switch and cause the changes to take effect on the switch.
- Use the **Refresh** button to refresh the page with the most current data from the switch.

Use the **Edit** button to configure the monitor session for a specific receiver (only for IPv4). After successful configuration, the sFlow packet processing will be done in hardware.

**Figure 85.** Edit Receiver Configuration

Edit Receiver Configuration	
Index	3
Owner String	<input type="text"/> (Max 127 characters)
Timeout Mode	<input checked="" type="checkbox"/>
Timeout Value (Seconds)	0 (0 to 2147483647)
Maximum Datagram Size	1400 (200 to 9316)
Host IP Address	0.0.0.0 (x.x.x.x or x:x:x:x:x:x:x)
Port	6343 (1 to 65535)
Datagram Version	5
Monitor Session	0

- Use the **Submit** button to sent updated data to the switch and cause the changes to take effect on the switch.

## sFlow Poller Configuration

The sFlow agent collects time-based sampling of network interface statistics and sends them to the configured sFlow receivers. A data source configured to collect counter samples is called a poller.

### Counter Sampling

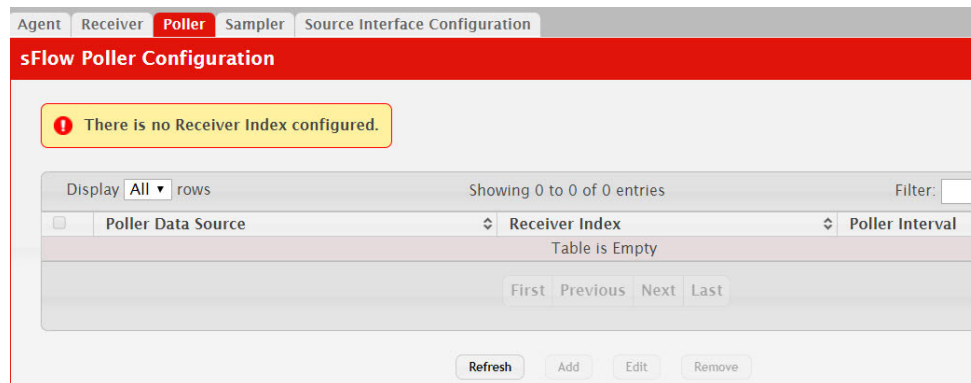
The primary objective of Counter Sampling is to efficiently, periodically export counters associated with Data Sources. A maximum Sampling Interval is assigned to each sFlow instance associated with a Data Source.

Counter Sampling is accomplished as follows:

The sFlow Agent keeps a list of counter sources being sampled. When a Packet Flow Sample is generated, the sFlow Agent examines the list and adds counters to the sample datagram, least recently sampled first. Counters are only added to the datagram if the sources are within a short period, i.e. five seconds, of failing to meet the required Sampling Interval. Periodically, i.e. every second, the sFlow Agent examines the list of counter sources and sends any counters that need to be sent to meet the sampling interval requirement.

To access the sFlow Poller Configuration page, click **System > Advanced Configuration > sFlow > Poller** in the navigation menu.

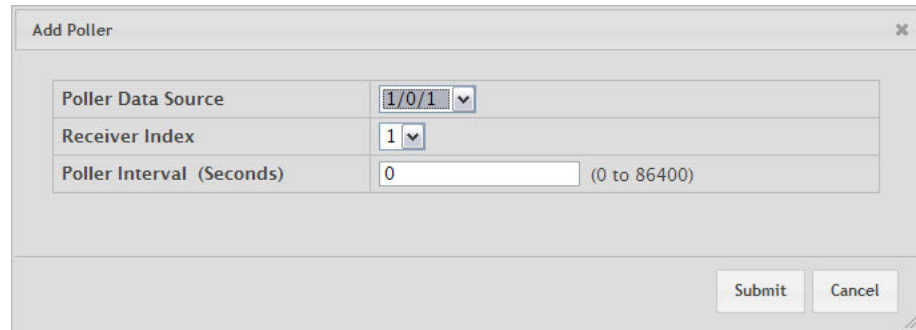
**Figure 86.** sFlow Poller



Use the buttons to perform the following tasks:

- To add an sFlow poller instance, click **Add** and complete the required information.
- To edit an existing sFlow poller instance, select the appropriate check box or click the row to select the sFlow poller instance and click **Edit**. Modify the sFlow poller configuration information as needed.
- To delete an sFlow poller instance, select one or more table entries and click **Remove**.

**Figure 87.** sFlow Poller Configuration



**Table 84.** sFlow Poller Configuration Fields

Field	Description
Poller Data-Source	The sFlow Sampler Datasource for this flow sampler. This Agent will support Physical ports only.
Receiver Index	The sFlowReceiver for this sFlow Counter Poller. If set to zero, the poller configuration is set to the default and the poller is deleted. Only active receivers can be set. If a receiver expires, then all pollers associated with the receiver will also expire. The allowed range is 1 to 8.
Poller Interval	The maximum number of seconds between successive samples of the counters associated with this data source

Click **Refresh** to refresh the page with the most current data from the switch.

## sFlow Sampler Configuration

The sFlow Agent collects a statistical packet-based sampling of the switched flows and sends them to the configured receivers. A data source configured to collect flow samples is called a sampler.

### Packet Flow Sampling

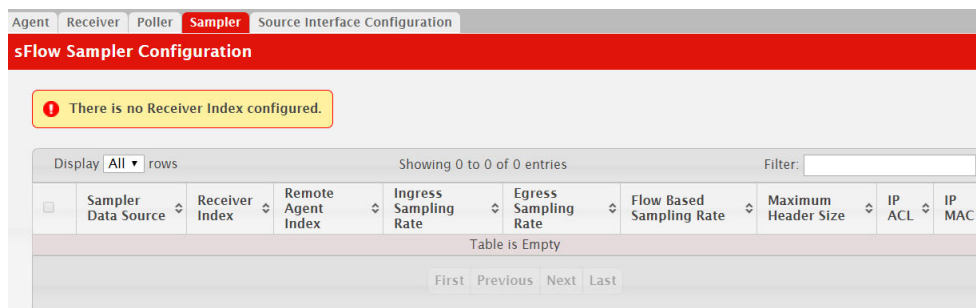
The Packet Flow Sampling mechanism carried out by each sFlow instance ensures that any packet observed at a Data Source has an equal chance of being sampled, irrespective of the Packet Flow(s) to which it belongs.

Packet Flow Sampling is accomplished as follows:

- When a packet arrives on an interface, the Network Device makes a filtering decision to determine whether the packet should be dropped.
- If the packet is not filtered (dropped), a destination interface is assigned by the switching/routing function.
- At this point, a decision is made on whether or not to sample the packet. The mechanism involves a counter that is decremented with each packet. When the counter reaches zero, a sample is taken. When a sample is taken, the counter that indicates how many packets to skip before taking the next sample is reset. The value of the counter is set to a random integer where the sequence of random integers used over time is the Sampling Rate.

To access the sFlow Sampler Configuration page, click **System > Advanced Configuration > sFlow > Sampler** in the navigation menu.

**Figure 88.** sFlow Sampler



**Table 85.** sFlow Sampler Configuration Fields

Field	Description
Sampler Data Source	The sFlowDataSource for this sFlow sampler. The sFlow agent supports physical ports as sFlow data sources.
Receiver Index	The sFlowReceiver for this sFlow sampler. The specified Receiver Index must be associated with an active sFlow receiver. If a receiver expires, all samplers associated with the receiver will also expire.
Remote Agent Index	The remote agent index.
Ingress Sampling Rate	sFlow instance packet Sampling Rate for Ingress sampling.
Egress Sampling Rate	sFlow instance egress packet Sampling Rate.
Flow-based Sampling Rate	sFlow instance flow based packet Sampling Rate.
Maximum Header Size	The maximum number of bytes that should be copied from a sampled packet.
IP ACL	The ID of the IP ACL to apply to traffic from the sampler.
IP MAC	The ID of the MAC ACL to apply to traffic from the sampler.

Click **Refresh** to refresh the page with the most current data from the switch.

Use the buttons to perform the following tasks:

- To add an sFlow sampler instance, click **Add** and complete the required information.
- To edit an existing sFlow sampler instance, select the appropriate check box or click the row to select the sFlow sampler instance and click **Edit**. Modify the sFlow sampler configuration information as needed.
- To delete an sFlow sampler instance, select one or more table entries and click **Remove**.

The **Add Sampler** page lets you configure the sampling rate for ingress/egress/flow based sampling. After successful configuration, the sFlow packet sampling is performed based on sampling rate.

**Figure 89.** Add Sampler

Sampler Data Source	1/0/1	
Receiver Index	1	
Remote Agent Index	0	
Ingress Sampling Rate		(1024 to 65536)
Egress Sampling Rate		(1024 to 65536)
Flow Based Sampling Rate		(1024 to 65536)
Maximum Header Size	128	(20 to 256, 128 = Default)
IP ACL	0	
IP MAC	0	

**Table 86.** sFlow Sampler Configuration Fields

Field	Description
Sampler Data Source	The sFlowDataSource for this sFlow sampler. The sFlow agent supports physical ports as sFlow data sources.
Receiver Index	The sFlow Receiver for this sFlow sampler. If set to zero, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. The allowed range is 1 to 8.
Ingress Sampling Rate	sFlow instance packet Sampling Rate for Ingress sampling.
Egress Sampling Rate	sFlow instance egress packet Sampling Rate.
Flow-based Sampling Rate	sFlow instance flow based packet Sampling Rate.
Maximum Header Size	The maximum number of bytes that should be copied from a sampled packet. The allowed range is 20 to 256.

## sFlow Source Interface Configuration

Use this page to specify the physical or logical interface to use as the sFlow client source interface. When an IP address is configured on the source interface, this address is used for all sFlow communications between the local sFlow client and the remote sFlow server. The IP address of the designated source interface is used in the IP header of sFlow management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device.

To access the sFlow Source Interface Configuration page, click **System > Advanced Configuration > sFlow > Source Interface Configuration** in the navigation menu.

**Figure 90.** sFlow Source Interface Configuration

**Table 87.** sFlow Source Interface Configuration Fields

Field	Description
Type	The type of interface to use as the source interface: <ul style="list-style-type: none"> <li>• <b>None</b> – The primary IP address of the originating (outbound) interface is used as the source address.</li> <li>• <b>Interface</b> – The primary IP address of a physical port is used as the source address.</li> <li>• <b>Loopback</b> – The primary IP address of the loopback interface is used as the source address. A loopback is always reachable, as long as any routing interface is up.</li> <li>• <b>VLAN</b> – The primary IP address of a VLAN routing interface is used as the source address.</li> </ul>
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
Loopback Interface	When the selected Type is Loopback, select the loopback interface to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.
Tunnel ID	The primary IP address of a tunnel interface is used as the source address.

If you make any changes to the page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a **save**.

---

## Defining SNMP Parameters

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports SNMP version 1, SNMP version 2, and SNMP version 3.

### SNMP v1 and v2

The SNMP agent maintains a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agent are controlled by access strings.

### SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, the User Security Model (USM) is defined for SNMPv3 and includes:

- **Authentication:** Provides data integrity and data origin authentication.
- **Privacy:** Protects against disclosure of message content. Cipher-Block-Chaining (CBC) is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness:** Protects against message delay or message redundancy. The SNMP agent compares incoming message to the message time information.
- **Key Management:** Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage device features. SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

Authentication or Privacy Keys are modified in the SNMPv3 User Security Model (USM).

Use the SNMP page to define SNMP parameters. To display the SNMP page, click **System > Advanced Configuration > SNMP** in the navigation menu.

## SNMP Community Configuration

Access rights are managed by defining communities on the SNMPv1, 2 Community page. When the community names are changed, access rights are also changed. SNMP Communities are defined only for SNMP v1 and SNMP v2.

**Note:** No SNMP communities exist by default.

Use the Community Configuration page to enable SNMP and Authentication notifications.

To display the Community Configuration page, click **System > Advanced Configuration > SNMP > Community** in the navigation menu.

**Figure 91.** SNMP Community



Use the buttons to perform the following tasks:

- To add a community, click **Add** and configure the desired settings.
- To change information for an existing community, select the check box associated with the entry and click **Edit**.
- To delete a configured community from the list, select the check box associated with each entry to delete and click **Remove**.

**Figure 92.** SNMP Community Configuration

**Table 88.** Community Configuration Fields

Field	Description
Community Name	Community name used on SNMP v1/v2 packets. A community string can contain a maximum of 20 characters.
Security Name	Identifies the Security entry that associates Communities and Groups for a specific access type.
Group Name	Identifies the Group associated with this Community entry.



**Table 88.** Community Configuration Fields (continued)

Field	Description
Community Access	Specifies the access control policy for the community. <ul style="list-style-type: none"> <li>• <b>public:</b> The SNMP community has Read Only privileges and its status set to enable.</li> <li>• <b>private:</b> The SNMP community has Read/Write privileges and its status set to enable.</li> </ul>
Community View	Specifies the community view for the community. If the value is empty, then no access is granted.
IP Address	Specifies the IP address that can connect with this community.

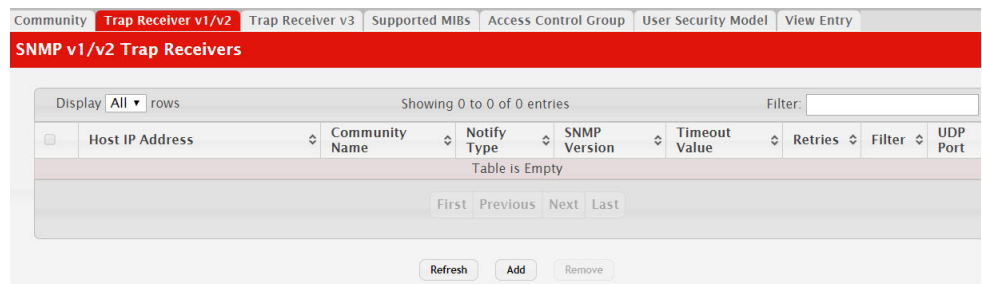
- If you make any changes to the page, click **Submit** to apply the changes to the system. If you create a new Community, it is added to the table below the **Submit** button.
- Click **Remove** to delete the selected SNMP Community.

## Trap Receiver v1/v2 Configuration

Use the Trap Receiver v1/v2 Configuration page to configure settings for each SNMPv1 or SNMPv2 management host that will receive notifications about traps generated by the device. The SNMP management host is also known as the SNMP trap receiver.

To access the Trap Receiver v1/v3 Configuration page, click **System > Advanced Configuration > SNMP > Trap Receiver V1/V2** from the navigation menu.

**Figure 93.** Trap v1/v2 Receiver



Use the buttons to perform the following tasks:

- To add an SNMP trap receiver and configure its settings, click **Add** and complete the required information.
- To delete one or more SNMP trap receivers from the list, select each entry to delete and click **Remove**.

**Figure 94.** Trap Receiver v1/v2 Configuration

**Table 89.** Trap Receiver v1/v2 Configuration Fields

Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the device.
Community Name	The name of the SNMP community that includes the SNMP management host and the SNMP agent on the device.
Notify Type	The type of SNMP notification to send the SNMP management host: <ul style="list-style-type: none"> <li>• <b>Inform</b> – An SNMP message that notifies the host when a certain event has occurred on the device. The message is acknowledged by the SNMP management host. This type of notification is not available for SNMPv1.</li> <li>• <b>Trap</b> – An SNMP message that notifies the host when a certain event has occurred on the device. The message is not acknowledged by the SNMP management host.</li> </ul>
SNMP Version	The version of SNMP to use, which is either SNMPv1 or SNMPv2.
Timeout Value	The number of seconds to wait for an acknowledgment from the SNMP management host before resending an inform message.
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP management host.
Filter	The name of the filter for the SNMP management host. The filter is configured by using the CLI and defines which MIB objects to include or exclude from the view. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

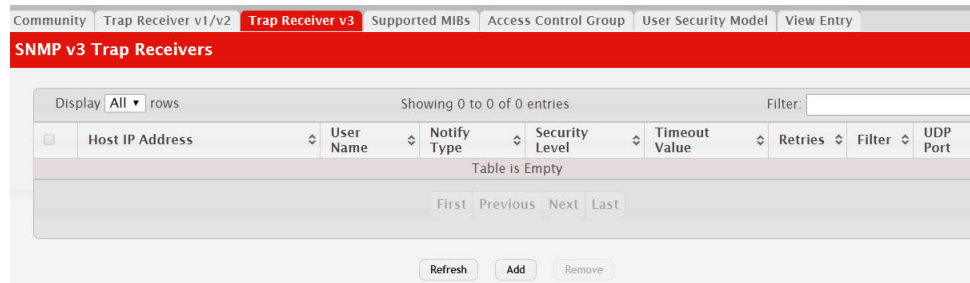
If you make any changes to the page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a **save**.

## Trap Receiver v3 Configuration

Use the Trap Receiver V3 Configuration v3 page to configure settings for each SNMPv3 management host that will receive notifications about traps generated by the device. The SNMP management host is also known as the SNMP trap receiver.

To access the Trap Receiver v3 Configuration page, click **System > Advanced Configuration > SNMP > Trap Receiver V3** from the navigation menu.

**Figure 95.** Trap Receiver v3



Use the buttons to perform the following tasks:

- To add an SNMP trap receiver and configure its settings, click **Add** and complete the required information.
- To delete one or more SNMP trap receivers from the list, select each entry to delete and click **Remove**.

**Figure 96.** Trap Receiver v3 Configuration

The screenshot shows the 'Add SNMP v3 Host' configuration form. It has a title bar 'Add SNMP v3 Host' with a close button. The form contains the following fields:
 

- Host IP Address: Text input field with a placeholder '(x.x.x.x or x::x::x::x::x::x)'
- User Name: Text input field with a placeholder '(1 to 30 characters)'
- Notify Type: Radio buttons for 'Trap' (selected) and 'Inform'
- Security Level: Radio buttons for 'No Auth No Priv' (selected), 'Auth No Priv', and 'Auth Priv'
- Retries: Text input field with value '3' and a placeholder '(1 to 255)'
- Timeout Value (Seconds): Text input field with value '15' and a placeholder '(1 to 300)'
- Filter: Text input field with a placeholder '(0 to 30 characters)'
- UDP Port: Text input field with value '162' and a placeholder '(1 to 65535)'

 At the bottom right, there are two buttons: 'Submit' and 'Cancel'.

**Table 90.** Trap Receiver v3 Configuration Fields

Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the device.
User Name	The name of the SNMP user that is authorized to receive the SNMP notification.

**Table 90.** *Trap Receiver v3 Configuration Fields (continued)*

Field	Description
Notify Type	The type of SNMP notification to send the SNMP management host: <ul style="list-style-type: none"><li>• <b>Inform</b> – An SNMP message that notifies the host when a certain event has occurred on the device. The message is acknowledged by the SNMP management host. This type of notification is not available for SNMPv1.</li><li>• <b>Trap</b> – An SNMP message that notifies the host when a certain event has occurred on the device. The message is not acknowledged by the SNMP management host.</li></ul>
Security Level	The security level associated with the SNMP user, which is one of the following: <ul style="list-style-type: none"><li>• <b>No Auth No Priv</b> – No authentication and no data encryption (no security).</li><li>• <b>Auth No Priv</b> – Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.</li><li>• <b>Auth Priv</b> – Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.</li></ul>
Timeout Value	The number of seconds to wait for an acknowledgment from the SNMP management host before resending an inform message.
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP management host.
Filter	The name of the filter for the SNMP management host. The filter is configured by using the CLI and defines which MIB objects to include or exclude from the view. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

If you make any changes to the page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a **save**.

## Supported MIBs

The Supported MIBs page lists all the MIBs supported by the SNMP management agent running on the device.

To access the Supported MIBs page, click **System > Advanced Configuration > SNMP > Supported MIBs** in the navigation menu.

**Figure 97.** Supported MIBs

Name	Description
CAMPUS-NOS-BONJOUR-MIB	The LENOVO Private MIB for CAMPUS-NOS Bonjour
CAMPUS-NOS-DENIALOFSERVICE-PRIVATE-MIB	The LENOVO Private MIB for CAMPUS-NOS Denial of Service.
CAMPUS-NOS-DHCPCLIENT-PRIVATE-MIB	The LENOVO Private MIB for CAMPUS-NOS DHCP Client
CAMPUS-NOS-DNS-RESOLVER-CONTROL-MIB	Defines a portion of the SNMP MIB under the LENOVO Corporation Client control configuration
CAMPUS-NOS-DOT1X-AUTHENTICATION-SERVER-MIB	The LENOVO Private MIB for CAMPUS-NOS Dot1x Authentication Se
CAMPUS-NOS-INTERFACE-APP-MIB	The LENOVO Private MIB for CAMPUS-NOS Interface Application
CAMPUS-NOS-IPV6-LOOPBACK-MIB	The LENOVO Private MIB for CAMPUS-NOS Loopback IPV6 address
CAMPUS-NOS-IPV6-TUNNEL-MIB	The LENOVO Private MIB for CAMPUS-NOS IPV6 Tunnel.
CAMPUS-NOS-KEYING-PRIVATE-MIB	The LENOVO Private MIB for CAMPUS-NOS Keying Utility
CAMPUS-NOS-LOOPBACK-MIB	The LENOVO Private MIB for CAMPUS-NOS Loopback

**Table 91.** Supported MIBs Fields

Field	Description
Name	The RFC number, if applicable, followed by the defined name of the MIB.
Description	The RFC title, or a brief description of the MIB.

## Access Control Group

Use this page to configure SNMP access control groups. These SNMP groups allow network managers to assign different levels of authorization and access rights to specific device features and their attributes. The SNMP group can be referenced by the SNMP community to provide security and context for agents receiving requests and initiating traps as well as for management systems and their tasks. An SNMP agent will not respond to a request from a management system outside of its configured group, but an agent can be a member of multiple groups at the same time to allow communication with SNMP managers from different groups. Several default SNMP groups are preconfigured on the system.

To access the Access Control Group page, click **System > Advanced Configuration > SNMP > Access Control Group** in the navigation menu. A portion of the web screen is shown [Figure 98, "Access Control Group,"](#) on page 166.

**Figure 98.** Access Control Group

Group Name	Context Name	SNMP Version	Security Level	Read
DefaultRead		SNMP V1	No Auth No Priv	Default
DefaultRead		SNMP V2	No Auth No Priv	Default
DefaultRead		SNMP V3	No Auth No Priv	Default
DefaultRead		SNMP V3	Auth No Priv	Default
DefaultRead		SNMP V3	Auth Priv	Default
DefaultSuper		SNMP V1	No Auth No Priv	DefaultSuper
DefaultSuper		SNMP V2	No Auth No Priv	DefaultSuper
DefaultSuper		SNMP V3	No Auth No Priv	DefaultSuper
DefaultWrite		SNMP V1	No Auth No Priv	Default
DefaultWrite		SNMP V2	No Auth No Priv	Default

Use the buttons to perform the following tasks:

- To add an SNMP group, click **Add** and specify the desired setting.
- To remove one or more SNMP groups, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Figure 99.** Access Control Group Add

**Table 92.** Access Control Group Fields

Field	Description
Group Name	The name that identifies the SNMP group.

**Table 92.** Access Control Group Fields (continued)

Field	Description
Context Name	The SNMP context associated with the SNMP group and its views. A user or a management application specifies the context name to get the performance information from the MIB objects associated with that context name. The Context EngineID identifies the SNMP entity that should process the request (the physical router), and the Context Name tells the agent in which context it should search for the objects requested by the user or the management application.
SNMP Version	The SNMP version associated with the group.
Security Level	The security level associated with the group, which is one of the following: <ul style="list-style-type: none"><li>• <b>No Auth No Priv</b> – No authentication and no data encryption (no security). This is the only Security Level available for SNMPv1 and SNMPv2 groups.</li><li>• <b>Auth No Priv</b> – Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.</li><li>• <b>Auth Priv</b> – Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.</li></ul>
Read	The level of read access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that restricts management access to viewing the contents of the agent.
Write	The level of write access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that permits management read-write access to the contents of the agent but not to the community.
Notify	The level of notify access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that permits sending SNMP traps or informs.

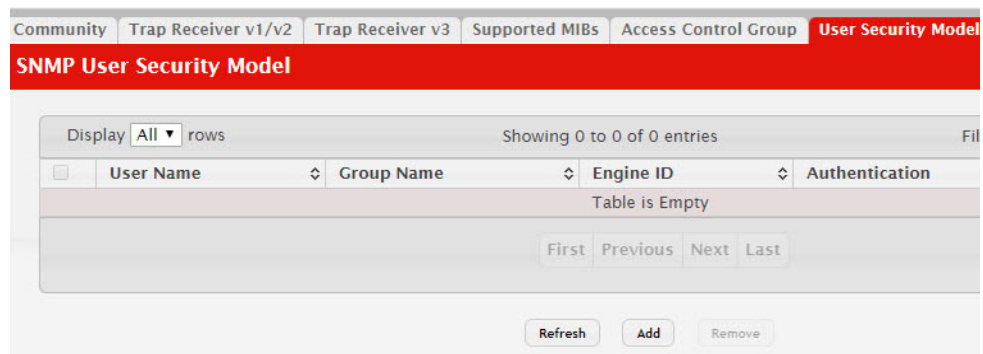
If you make any changes to the page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a **save**.

## User Security Model

The User Security Model page provides the capability to configure the SNMP V3 user accounts.

To access the User Security Model page, click **System > Advanced Configuration > SNMP > User Security Model** in the navigation menu.

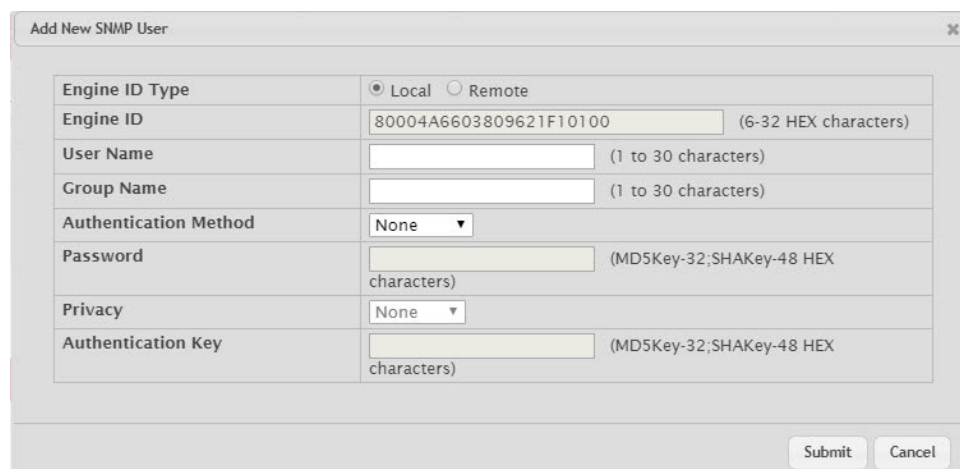
**Figure 100.** SNMP User Security Model



Use the buttons to perform the following tasks:

- To add a user, click **Add**. The Add New SNMP User dialog box opens. Specify the new account information in the available fields.
- To remove a user, select one or more table entries and click **Remove** to delete the selected entries.

**Figure 101.** SNMP User Security Model Add



**Table 93.** SNMP User Security Model Fields

Field	Description
Engine ID	Each SNMPv3 agent has an engine ID that uniquely identifies the agent in the device. If given this entry will be used only for packets whose engine id is this. This field takes a hexadecimal string in the form 0102030405.
User Name	Specifies the name of the SNMP user being added for the User-based Security Model (USM). Each user name must be unique within the SNMP agent user list. A user name cannot contain any leading or embedded blanks.



**Table 93.** *SNMP User Security Model Fields (continued)*

Field	Description
Group Name	A SNMP group is a group to which hosts running the SNMP service belong. A group name parameter is simply the name of that group by which SNMP communities are identified. The use of a group name provides some security and context for agents receiving requests and initiating traps and does the same for management systems and their tasks. An SNMP agent won't respond to a request from a management system outside its configured group, but an agent can be a member of multiple groups at the same time. This allows for communications with SNMP managers from different groups.
Authentication Method	Specifies the authentication protocol to be used on authenticated messages on behalf of the specified user. <ul style="list-style-type: none"><li>• <b>None</b> - No authentication will be used for this user.</li><li>• <b>MD5</b> - MD5 protocol will be used.</li><li>• <b>SHA</b> - SHA protocol will be used.</li><li>• <b>MD5-Key</b> - MD5 protocol will be used. This option requires a pregenerated MD5 authentication key of 32 hexadecimal characters.</li><li>• <b>SHA-Key</b> - SHA protocol will be used. This option requires a pregenerated SHA authentication key of 48 hexadecimal characters.</li></ul>
Password	Specifies the password used to generate the key to be used in authenticating messages on behalf of this user. This parameter must be specified if the Authentication method parameter is not NONE.
Privacy	Specifies the privacy protocol to be used on encrypted messages on behalf of the specified user. This parameter is only valid if the Authentication method parameter is not NONE. <ul style="list-style-type: none"><li>• <b>None</b> - No privacy protocol will be used.</li><li>• <b>DES</b> - DES protocol will be used.</li><li>• <b>DES-Key</b> - DES protocol will be used. This option requires an authentication key of 32 characters if MD5 is selected or 48 characters if SHA is selected.</li></ul>
Authentication Key	Specifies the password used to generate the key to be used in encrypting messages to and from this user. This parameter must be specified if the Privacy parameter is not NONE.

If you make any changes to the page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a **save**.

## Source Interface Configuration

Use this page to specify the physical or logical interface to use as the SNMP client source interface. When an IP address is configured on the source interface, this address is used for all SNMP communications between the local SNMP client and the remote SNMP server. The IP address of the designated source interface is used in the IP header of SNMP management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device.

To access the SNMP Trap Source Interface Configuration page, click **System > Advanced Configuration > SNMP > Source Interface Configuration** in the navigation menu.

**Figure 102.** SNMP Trap Source Interface Configuration

**Table 94.** SNMP Trap Source Interface Configuration Fields

Field	Description
Type	The type of interface to use as the source interface: <ul style="list-style-type: none"> <li>• <b>None</b> – The primary IP address of the originating (outbound) interface is used as the source address.</li> <li>• <b>Interface</b> – The primary IP address of a physical port is used as the source address.</li> <li>• <b>VLAN</b> – The primary IP address of a VLAN routing interface is used as the source address.</li> <li>• <b>Loopback</b> – The primary IP address of the loopback interface is used as the source address. A loopback is always reachable, as long as any routing interface is up.</li> <li>• <b>Network</b> – The network source IP is used as the source address.</li> <li>• <b>Service Port</b> – The management port source IP is used as the source address.</li> </ul>
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
Loopback Interface	When the selected Type is Loopback, select the loopback interface to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.

If you make any changes to the page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a **Save Configuration**.

## Viewing System Statistics

The pages in the Statistics folder contain a variety of information about the number and type of traffic transmitted from and received on the switch.

### Switch Statistics

The Switch Statistics page shows detailed statistical information about the traffic the switch handles.

To access the Switch Statistics page, click **System > Statistics > System > Switch** in the navigation menu.

**Figure 103.** Switch Statistics

Statistics	Transmit	Receive
Octets Without Error	19610547	19596144
Packets Without Errors	18952	161160
Packets Discarded	0	0
Unicast Packets	0	0
Multicast Packets	18952	161160
Broadcast Packets	0	0

Status	FDB Entries	VLANs
Current Usage	2	1
Peak Usage	2	1
Maximum Allowed	16384	4093
Static Entries	0	1
Dynamic Entries	2	0
Total Entries Deleted	N/A	0

System	
Interface	417
Time Since Counters Last Cleared	3d:07:03:09

**Table 95.** Switch Statistics Fields

Field	Description
Statistics	
Octets Without Error	The total number of octets (bytes) of data successfully transmitted or received by the processor (excluding framing bits but including FCS octets).
Packets Without Errors	The total number of packets including unicast, broadcast, and multicast packets, successfully transmitted or received by the processor.
Packets Discarded	The number of outbound (Transmit column) or inbound (Receive column) packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Unicast Packets	The number of subnetwork-unicast packets delivered to or received from a higher-layer protocol.

**Table 95.** *Switch Statistics Fields (continued)*

Field	Description
Multicast Packets	The total number of packets transmitted or received by the device that were directed to a multicast address. <b>Note:</b> This number does not include packets directed to the broadcast address.
Broadcast Packets	The total number of packets transmitted or received by the device that were directed to the broadcast address. <b>Note:</b> This number does not include multicast packets.
Status	
Current Usage	In the FDB Entries column, the value shows the number of learned and static entries in the MAC address table. In the VLANs column, the value shows the total number of static and dynamic VLANs that currently exist in the VLAN database.
Peak Usage	The highest number of entries that have existed in the MAC address table or VLAN database since the most recent reboot.
Maximum Allowed	The maximum number of statically configured or dynamically learned entries allowed in the MAC address table or VLAN database.
Static Entries	The current number of entries in the MAC address table or VLAN database that an administrator has statically configured.
Dynamic Entries	The current number of entries in the MAC address table or VLAN database that have been dynamically learned by the device.
Total Entries Deleted	The number of VLANs that have been created and then deleted since the last reboot. This field does not apply to the MAC address table entries.
System	
Interface	The interface index object value of the interface table entry associated with the Processor of this switch. This value is used to identify the interface when managing the device by using SNMP.
Time Since Counters Last Cleared	The amount of time in days, hours, minutes, and seconds, that has passed since the statistics for this device were last reset.

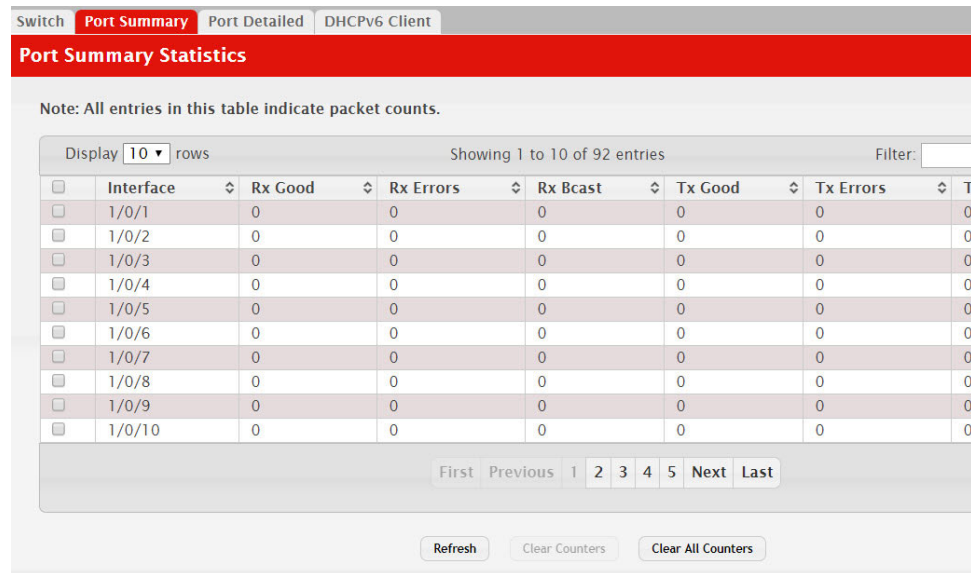
- Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.
- Click **Clear Counters** to clear all the statistics counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.

## Port Summary

This page shows statistical information about the packets received and transmitted by each port and LAG.

To access the Port Summary page, click **System > Statistics > System > Port Summary** in the navigation menu.

**Figure 104.** Port Summary



**Table 96.** Port Summary Fields

Field	Description
Interface	Identifies the port or LAG.
Rx Good	The total number of inbound packets received by the interface without errors.
Rx Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Rx Bcast	The total number of good packets received that were directed to the broadcast address. <b>Note:</b> This number does not include multicast packets.
Tx Good	The total number of outbound packets transmitted by the interface to its Ethernet segment without errors.
Tx Errors	The number of outbound packets that could not be transmitted because of errors.
Tx Collisions	The best estimate of the total number of collisions on this Ethernet segment.

- Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.
- Click **Clear Counters** to clear all the statistics counters, resetting all summary and detailed statistics for this switch to default values. The discarded packets count cannot be cleared.
- Click **Clear All Counters** to clear counters for all switches in the stack.

## Port Detailed Statistics

The Port Detailed page displays a variety of per-port traffic statistics.

To access the Port Detailed page, click **System > Statistics > System > Port Detailed** in the navigation menu.

Figure 105 shows some, but not all, of the fields on the Port Detailed page.

**Figure 105.** Port Detailed Statistics

Switch		Port Summary	Port Detailed	DHCPv6 Client
<b>Port Detailed Statistics</b>				
Interface	1/0/1 ▼			
Maximum Frame Size	1518			
MTU	1500			
Packet Lengths Received and Transmitted				
64 Octets	0			
65-127 Octets	0			
128-255 Octets	0			
256-511 Octets	0			
512-1023 Octets	0			
1024-1518 Octets	0			
1519-1522 Octets				
1523-2047 Octets	0			
2048-4095 Octets	0			
4096-9216 Octets	0			
Basic	Transmit	Receive		
Unicast Packets	0	0		
Multicast Packets	0	0		
Broadcast Packets	0	0		
Total Packets (Octets)	0	0		
Packets > 1518 Octets	0	0		
802.3x Pause Frames	0	0		
FCS Errors	0	0		

**Table 97.** Port Detailed Statistics Fields

Field	Description
Interface	Use the drop-down menu to select the interface for which data is to be displayed or configured. For non-stacking systems, this field is <b>Slot/Port</b> .
Maximum Frame Size	The maximum Ethernet frame size the interface supports or is configured to support. The maximum frame size includes the Ethernet header, CRC, and payload.
MTU	Indicates MTU (Maximum Transmit Unit) of the interface. The actual frame size is calculated by adding Ethernet header size in MTU.
Packet Lengths Received and Transmitted	
64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

**Table 97.** *Port Detailed Statistics Fields (continued)*

Field	Description
256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
1519-1522 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
1523-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
<b>Basic</b>	
Unicast Packets	The Transmit column shows the total number of packets that higher-level protocols requested be transmitted to a subnetwork unicast address, including those that were discarded or not sent. The Receive column shows the number of subnetwork unicast packets delivered to a higher-layer protocol.
Multicast Packets	The Transmit column shows the total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent. The Receive column shows the number of multicast packets delivered to a higher-layer protocol.
Broadcast Packets	The Transmit column shows the total number of packets that higher-level protocols requested be transmitted to a broadcast address, including those that were discarded or not sent. The Receive column shows the number of broadcast packets delivered to a higher-layer protocol.
Total Packets (Octets)	The total number of octets of data (including those in bad packets) transmitted or received on the interface (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets > 1518 Octets	The total number of packets transmitted or received by this interface that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. This counter has a maximum increment rate of 815 counts per sec at 10 Mb/s.
802.3x Pause Frames	The number of MAC Control frames transmitted or received by this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

**Table 97.** *Port Detailed Statistics Fields (continued)*

Field	Description
FCS Errors	The total number of packets transmitted or received by this interface that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.
Protocol	
STP BPDUs	The number of Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) transmitted or received by the interface.
RSTP BPDUs	The number of Rapid STP BPDUs transmitted or received by the interface.
MSTP BPDUs	The number of Multiple STP BPDUs transmitted or received by the interface.
SSTP BPDUs	The number of Shared STP BPDUs transmitted or received by the interface.
GVRP PDUs	The number of Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) PDUs transmitted or received by the interface.
GMRP PDUs	The number of GARP Multicast Registration Protocol (GMRP) PDUs transmitted or received by the interface.
EAPOL Frames	The number of Extensible Authentication Protocol (EAP) over LAN (EAPOL) frames transmitted or received by the interface for IEEE 802.1X port-based network access control.
Advanced - Transmit	
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Underrun Errors	The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.
GMRP Failed Registrations	The number of times attempted GMRP registrations could not be completed.
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed.
Percent Utilization Transmitted (%)	The amount of link utilization, represented as a percentage of total link bandwidth, for the TX direction.
Advanced - Receive	
Total Packets Received Not Forwarded	The number of inbound packets which were chosen to be discarded to prevent them from being delivered to a higher-layer protocol, even though no errors had been detected. One possible reason for discarding such a packet is to free up buffer space.
Total Packets Received With MAC Errors	The total number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.



**Table 97.** Port Detailed Statistics Fields (continued)

Field	Description
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). <b>Note:</b> This definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
Unacceptable Frame Type	The number of frames discarded from this interface due to being a frame type that the interface cannot accept.
Percent Utilization Received (%)	The amount of link utilization, represented as a percentage of total link bandwidth, for the RX direction.
Time Since Counters Last Cleared	The amount of time in days, hours, minutes, and seconds, that has passed since the statistics for this interface were last reset.

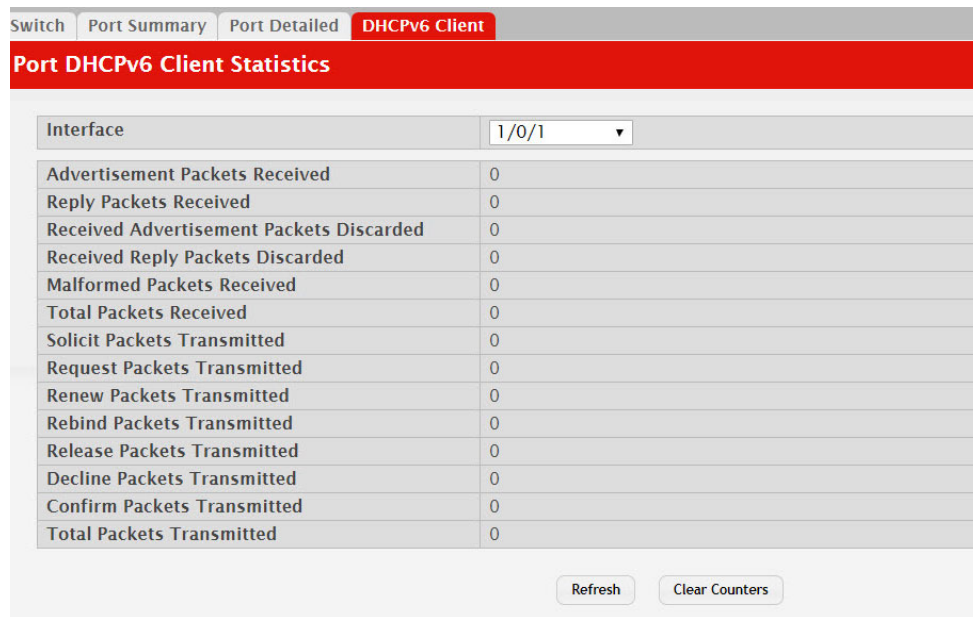
- Click **Clear Counters** to clear all the counters. This resets all statistics for this port to the default values.
- Click **Clear All Counters** to clear all the counters for all ports on the switch. The button resets all statistics for all ports to default values.
- Click **Refresh** to refresh the data on the screen and display the most current statistics.

## Port DHCPv6 Client Statistics

This page displays the DHCPv6 client statistics values for the selected interface. The DHCPv6 client on the device exchanges several different types of UDP messages with one or more network DHCPv6 servers during the process of acquiring address, prefix, or other relevant network configuration information from the server. The values indicate the various counts that have accumulated since they were last cleared.

To display the Port DHCPv6 Client Statistics page, click **System > Statistics > System > DHCPv6**.

**Figure 106.** Port DHCPv6 Client Statistics



**Table 98.** Port DHCPv6 Client Statistics Fields

Field	Description
Interface	Select the interface to view the DHCPv6 client statistics associated with it.
Advertisement Packets Received	Number of DHCPv6 advertisement messages received from one or more DHCPv6 servers in response to the client's solicit message.
Reply Packets Received	Number of DHCPv6 reply messages received from one or more DHCPv6 servers in response to the client's request message.
Received Advertisement Packets Discarded	Number of DHCPv6 advertisement messages received from one or more DHCPv6 servers to which the client did not respond.
Received Reply Packets Discarded	Number of DHCPv6 reply messages received from one or more DHCPv6 servers to which the client did not respond.
Malformed Packets Received	Number of messages received from one or more DHCPv6 servers that were improperly formatted.
Total Packets Received	Total number of messages received from all DHCPv6 servers.
Solicit Packets Transmitted	Number of DHCPv6 solicit messages the client sent to begin the process of acquiring network information from a DHCPv6 server.
Request Packets Transmitted	Number of DHCPv6 request messages the client sent in response to a DHCPv6 server's advertisement message.
Renew Packets Transmitted	Number of renew messages the DHCPv6 client has sent to the server to request an extension of the lifetime of the information provided by the server. This message is sent to the DHCPv6 server that originally assigned the addresses and configuration information.

**Table 98.** Port DHCPv6 Client Statistics Fields (continued)

Field	Description
Rebind Packets Transmitted	Number of rebind messages the DHCPv6 client has sent to any available DHCPv6 server to request an extension of its addresses and an update to any other relevant information. This message is sent only if the client does not receive a response to the renew message.
Release Packets Transmitted	Number of release messages the DHCPv6 client has sent to the server to indicate that it no longer needs one or more of the assigned addresses.
Decline Packets Transmitted	Number of decline messages the DHCPv6 client has sent to the server to indicate that one or more addresses assigned by the server are already in use on the connected link.
Confirm Packets Transmitted	Number of confirm messages the DHCPv6 client has sent to any available DHCPv6 server to determine whether the addresses it is assigned are still valid for the connected link.
Total Packets Transmitted	Total number of messages sent to all DHCPv6 servers.

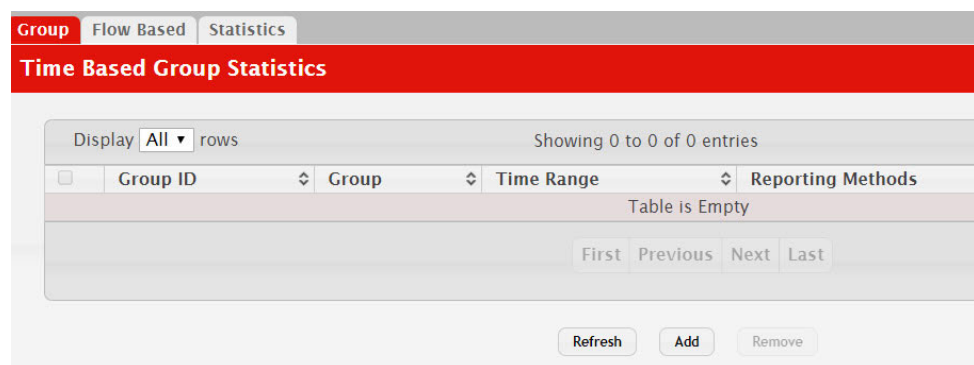
- Click **Clear Counters** to clear all the statistics counters, resetting all switch summary and detailed statistics to default values.

## Time Based Group Statistics

Use this page to define criteria for collecting time-based statistics for interface traffic. The time-based statistics can be useful for troubleshooting and diagnostics purposes. The statistics application uses the system clock for time-based reporting, so it is important to configure the system clock (manually or through SNTP) before using this feature.

To access the Time Based Group Statistics page, click **System > Statistics > Time Based > Group** in the navigation menu.

**Figure 107.** Time Based Group Statistics



Use the buttons to perform the following tasks:

- To add a set of time-based traffic group statistics to collect, click **Add** and configure the desired settings.

- To delete one or more time-based statistics groups, select each entry to delete and click **Remove**.

**Table 99.** *Time Based Group Statistics Fields*

Field	Description
Group	The type of traffic statistics to collect for the group, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Received</b> – The number of packets received on the interfaces within the group.</li> <li>• <b>Received Errors</b> – The number of packets received with errors on the interfaces within the group.</li> <li>• <b>Transmitted</b> – The number of packets transmitted by the interfaces within the group.</li> <li>• <b>Received Transmitted</b> – The number of packets received and transmitted by the interfaces within the group.</li> <li>• <b>Port Utilization</b> – The percentage of total bandwidth used by the port within the specified time period.</li> <li>• <b>Congestion</b> – The percentage of time within the specified time range that the ports experienced congestion.</li> </ul>
Time Range	The name of the periodic or absolute time range to use for data collection. The time range is configured by using the Time Range Summary and Time Range Entry Summary pages. The time range must be configured on the system before the time-based statistics can be collected.
Reporting Methods	The methods for reporting the collected statistics at the end of every configured time range interval. The available options are: <ul style="list-style-type: none"> <li>• <b>None</b> – The statistics are not reported to the console or an external server. They can be viewed only by using the web interface or by issuing a CLI command.</li> <li>• <b>Console</b> – The statistics are displayed on the console.</li> <li>• <b>E-Mail</b> – The statistics are sent to an e-mail address. The SMTP server and e-mail address information is configured by using the appropriate Email Alerts pages.</li> <li>• <b>Syslog</b> – The statistics are sent to a remote syslog server. The syslog server information is configured on the Logging Hosts page.</li> </ul>
Interfaces	The interface or interfaces on which data is collected. To select multiple interfaces when adding a new group, <b>CTRL</b> + click each interface to include in the group.

- Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.
- To add a set of time-based traffic group statistics to collect, click **Add** and configure the desired settings.
- To delete one or more time-based statistics groups, select each entry to delete and click **Remove**.

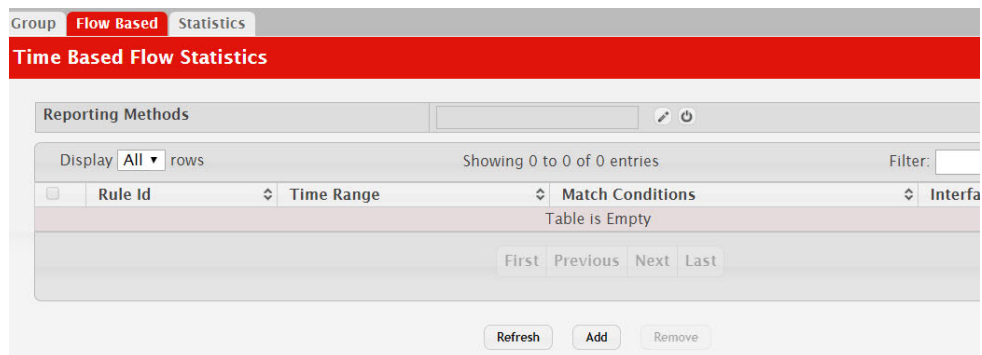
## Time Based Flow Statistics

Use this page to define criteria for collecting time-based statistics for specific traffic flows. The statistics include a per-interface hit count based on traffic that meets the match criteria configured in a rule for the interfaces included in the rule. The hit

count statistics are collected only during the specified time range. The statistics application uses the system clock for time-based reporting. Configure the system clock (manually or through SNTP) before using the time-based statistics feature.

To access the Time Based Flow Statistics page, click **System > Statistics > Time Based > Flow Based** in the navigation menu.

**Figure 108.** Time Based Flow Statistics



Use the buttons to perform the following tasks:

- To add a rule and define criteria for flow-based statistics that are collected within a time range, click **Add** and configure the desired settings.
- To delete one or more flow-based rules for time-based statistics, select each entry to delete and click **Remove**.

**Table 100.** Time Based Flow Statistics Fields

Field	Description
Reporting Methods	The methods for reporting the collected statistics at the end of every configured interval. To change the reporting methods for all flow-based statistics rules, click the Edit icon and select one or more methods. To reset the field to the default value, click the Reset icon. The available reporting methods are: <ul style="list-style-type: none"> <li>• <b>None</b> – The statistics are not reported to the console or an external server. They can be viewed only by using the web interface or by issuing a CLI command.</li> <li>• <b>Console</b> – The statistics are displayed on the console.</li> <li>• <b>E-Mail</b> – The statistics are sent to an e-mail address. The SNTP server and e-mail address information is configured by using the appropriate Email Alerts pages.</li> <li>• <b>Syslog</b> – The statistics are sent to a remote syslog server. The syslog server information is configured on the Logging Hosts page.</li> </ul>
Rule Id	The number that identifies the flow-based statistics collection rule.
Time Range	The name of the periodic or absolute time range to use for data collection. The time range is configured by using the Time Range Summary and Time Range Entry Summary pages. The time range must be configured on the system before the time-based statistics can be collected.
Match Conditions	The criteria a packet must meet to match the rule.

**Table 100.** *Time Based Flow Statistics Fields (continued)*

Field	Description
Interfaces	The interface or interfaces on which the flow-based rule is applied. Only traffic on the specified interfaces is checked against the rule.
After you click <b>Add</b> , the Time Based Flow Configuration window opens and allows you to configure a rule for traffic flow statistics. The match conditions are optional, but the rule must specify at least one match condition. The following information describes the match criteria fields that are available in this window.	
Match All	Select this option to indicate that all traffic matches the rule and is counted in the statistics. This option is exclusive to all other match criteria, so if Match All is selected, no other match criteria can be configured.
Source IP	The source IP address to match in the IPv4 packet header.
Destination IP	The destination IP address to match in the IPv4 packet header.
Source MAC	The source MAC address to match in the ingress frame header.
Destination MAC	The destination MAC address to match in the ingress frame header.
Source TCP Port	The TCP source port to match in the TCP header.
Destination TCP Port	The TCP destination port to match in the TCP header.
Source UDP Port	The UDP source port to match in the UDP header.
Destination UDP Port	The UDP destination port to match in the UDP header.

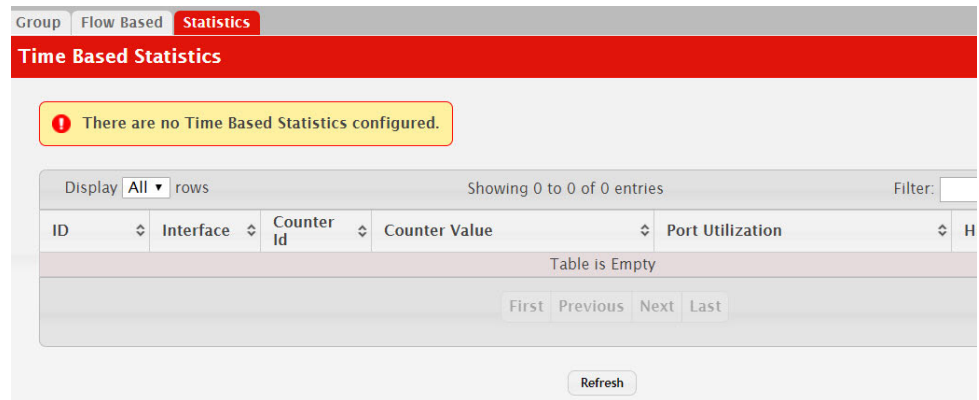
- Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.
- To add a set of time-based traffic group statistics to collect, click **Add** and configure the desired settings.
- To delete one or more time-based statistics groups, select each entry to delete and click **Remove**.

## Time Based Statistics

Use this page to view time-based statistics collected for the configured traffic groups and flow-based rules.

To access the Time Based Statistics page, click **System > Statistics > Time Based > Statistics** in the navigation menu.

**Figure 109.** Time Based Statistics



**Table 101.** Time Based Statistics Fields

Field	Description
ID	The traffic group name or flow-based rule ID associated with the rest of the statistics in the row.
Interface	The interface on which the statistics were reported.
Counter ID	For traffic group statistics, this field identifies the type of traffic.
Counter Value	For traffic group statistics, this field shows the number of packets of the type identified by the Counter Id field that were reported on the interface during the time range.
Port Utilization	For a port utilization traffic group, this field reports the percentage of the total available bandwidth used on the interface during the time range.
Hit Count	For flow-based statistics, this field reports the number of packets that matched the flow-based rule criteria during the time range.

- Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.

## Using System Utilities

The System Utilities feature menu contains links to Web pages that help you configure features that help you manage the switch.

### System Reset

Use the System Reset page to reboot the system. If the platform supports stacking, you can reset any of the switches in the stack, or all switches in the stack from this page.

To access the System Reset page, click **System > Utilities > System Reset** in the navigation menu.

**Figure 110.** System Reset

System Reset | Ping | Ping IPv6 | TraceRoute | TraceRoute IPv6 | IP Address Conflict | Transfer | Core Dump | Core Dump Test

**System Reset**

Generate Core Dump before reset  Yes  No

Switch ID

**!** Resetting the switch will cause all device operations to stop. This web session will be disconnected and you will have to log in again after the device has been restarted. All unsaved changes will be lost. It is possible that the ip address of the switch will change. If this occurs you will need to determine the new ip address to access the device using the web.

Reset

**Table 102.** System Reset Fields

Field	Description
Generate Core Dump before reset	Generates core dump file on demand.
Switch ID	Select the specific switch unit to be reset, or specify <b>All</b> to reset all units in the stack.
Reset (Button)	Initiates the system reset action after displaying a confirmation message. <b>Note:</b> Any configuration changes made since the last successful save are lost whenever a switch is reset. It is possible that the IP address of the switch will change. If this occurs you will need to determine the new IP address to access the device using the web.

For Stacking platforms, you can select one or all switches in the stack to reset from the drop-down menu. For platforms that do not support stacking, this field is not present.

Click **Reset** to initiate the system reset. If you have not saved the changes that you submitted since the last system reset, the changes will not be applied to the system after the reset.



# Ping

Use the Ping page to tell the switch to send a Ping request to a specified IP address. You can use this feature to check whether the switch can communicate with a particular network host.

To access the Ping page, click **System > Utilities > Ping** in the navigation menu.

**Figure 111.** Ping

**Table 103.** Ping Fields

Field	Description
Hostname/IP Address	Enter the IP address or the host name of the station you want the switch to ping. The initial value is blank. This information is not retained across a power cycle.
Count	The number of ICMP echo request packets to send to the host.
Interval	The number of Seconds to wait between sending ping packets.
Size	The size of the ping packet, in bytes. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes, such as large or very large packets.
Source	The source IP address or interface to use when sending the echo request packets. If source is not required, select None as source option.
IP Address	The source IP address to use when sending the Echo requests packets. This field is enabled when IP Address is selected as source option.
Interface	The interface to use when sending the Echo requests packets. This field is enabled when Interface is selected as source option.
Status	Displays the results of the ping.
Results	The results of the ping test, which includes information about the reply (if any) received from the host.

**Table 103.** Ping Fields (continued)

Field	Description
Start (Button)	Starts the ping test. The device sends the specified number of ping packets to the host.
Stop (Button)	Interrupts the current ping test.

## Ping IPv6

Use the Ping IPv6 page to tell the device to send one or more ping requests to a specified IPv6 host. You can use the ping request to check whether the device can communicate with a particular host on an IPv6 network. A ping request is an Internet Control Message Protocol version 6 (ICMPv6) echo request packet. The information you enter on this page is not saved as part of the device configuration.

To access the Ping IPv6 page, click **System > Utilities > Ping IPv6** in the navigation menu.

**Figure 112.** Ping IPv6

**Table 104.** Ping IPv6 Fields

Field	Description
Ping	Select either a global IPv6 address or a link local address to ping. A global address is routable over the Internet, while a link-local address is intended for communication only within the local network. Link local addresses have a prefix of fe80::/64.
Interface	This field displays only when <b>Link Local</b> is selected. Select an IPv6 interface to initiate the ping.

**Table 104.** *Ping IPv6 Fields (continued)*

Field	Description
Host Name or IPv6 Address	Enter the global or link-local IPv6 address, or the DNS-resolvable host name of the station to ping. If the ping type is Link Local, you must enter a link-local address and cannot enter a host name.
Count	Enter the number of ICMP echo request packets to send to the host.
Interval	Enter the number of seconds to wait between sending ping packets.
Size	The size of the ping packet, in bytes. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes, such as large or very large packets.
Source	The source IP address or interface to use when sending the echo request packets. If source is not required, select None as source option.
IPv6 Address	The source IPv6 address to use when sending the Echo requests packets. This field is enabled when IP Address is selected as source option.
Interface	The interface to use when sending the Echo requests packets. This field is enabled when Interface is selected as source option.
Results	The results of the ping test, which includes information about the reply (if any) received from the host.

Click **Submit** to send the specified number of pings. The results display in the Ping Output box.

## TraceRoute

Use this page to determine the layer 3 path a packet takes from the device to a specific IP address or hostname. When you initiate the TraceRoute command by clicking the Start button, the device sends a series of TraceRoute probes toward the destination. The results list the IP address of each layer 3 device a probe passes through until it reaches its destination - or fails to reach its destination and is discarded. The information you enter on this page is not saved as part of the device configuration.

To access the TraceRoute page, click **System > Utilities > TraceRoute** in the navigation menu.

**Figure 113.** TraceRoute

**Table 105.** TraceRoute Fields

Field	Description
Host Name or IP Address	The DNS-resolvable hostname or IP address of the system to attempt to reach.
Probes Per Hop	TraceRoute works by sending UDP packets with increasing Time-To-Live (TTL) values. Specify the number of probes sent with each TTL.
MaxTTL	The maximum Time-To-Live (TTL). The TraceRoute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the TraceRoute will not reach it.
InitTTL	The initial Time-To-Live (TTL). This value controls the maximum number of layer 3 hops that the first set of probes may travel.
MaxFail	The number of consecutive failures that terminate the TraceRoute. If the device fails to receive a response for this number of consecutive probes, the TraceRoute terminates.
Interval	The number of Seconds to wait between sending probes.
Port	The UDP destination port number to be used in probe packets. The port number should be a port that the target host is not listening on, so that when the probe reaches the destination, it responds with an ICMP Port Unreachable message.
Size	The size of probe payload in bytes.
Source	Select None, IP Address, Interface, or Loopback as a source.

**Table 105.** *TraceRoute Fields (continued)*

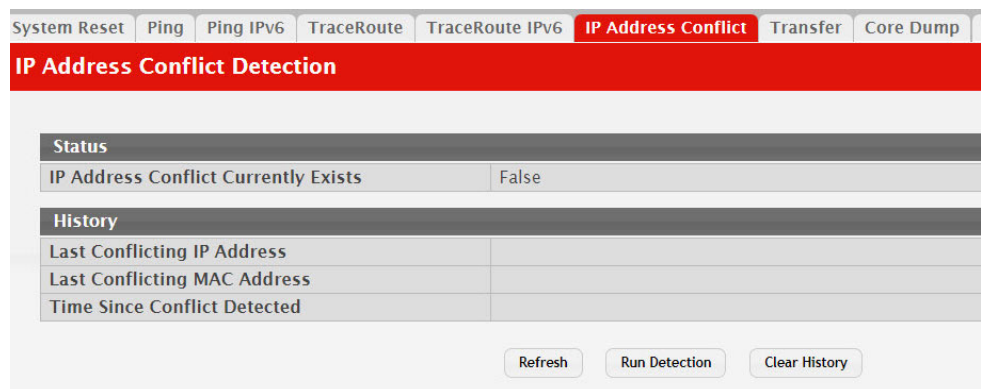
Field	Description
Status	The current status of the TraceRoute, which can be: <ul style="list-style-type: none"> <li>• <b>Not Started</b> – The TraceRoute has not been initiated since viewing the page.</li> <li>• <b>In Progress</b> – The TraceRoute has been initiated and is running.</li> <li>• <b>Stopped</b> – The TraceRoute was interrupted by clicking the Stop button.</li> <li>• <b>Done</b> – The TraceRoute has completed, and information about the TraceRoute is displayed in the Results area.</li> </ul>
Results	The results of the TraceRoute are displayed
Start (Button)	Initiates the TraceRoute.
Stop (Button)	Interrupts the running TraceRoute.

## IP Address Conflict

Use the IP Address Conflict page to determine whether the IP address configured on the device is the same as the IP address of another device on the same LAN (or on the Internet, for a routable IP address) and to help you resolve any existing conflicts. An IP address conflict can make both this system and the system with the same IP address unusable for network operation.

To access the IP Address Conflict page, click **System > Utilities > IP Address Conflict** in the navigation menu.

**Figure 114.** IP Address Conflict



**Table 106.** *IP Address Conflict Fields*

Field	Description
IP Address Conflict Currently Exists	Indicates whether a conflicting IP address has been detected since this status was last reset. <ul style="list-style-type: none"> <li>• <b>False</b> – No conflict detected (the subsequent fields on this page display as N/A).</li> <li>• <b>True</b> – Conflict was detected (the subsequent fields on this page show the relevant information).</li> </ul>
Last Conflicting IP Address	The device interface IP address that is in conflict. If multiple conflicts were detected, only the most recent occurrence is displayed.

**Table 106.** IP Address Conflict Fields (continued)

Field	Description
Last Conflicting MAC Address	The MAC address of the remote host associated with the IP address that is in conflict. If multiple conflicts are detected, only the most recent occurrence is displayed.
Time Since Conflict Detected	The elapsed time (displayed in days, hours, minutes, and seconds) since the last address conflict was detected, provided the <b>Clear History</b> button has not yet been pressed.
Run Detection (Button)	Activates the IP address conflict detection operation in the system.
Clear History (Button)	Resets the IP address conflict detection status information that was last seen by the device.

## Transfer

Use the Transfer page to upload files from the device to a remote system and to download files from a remote system to the device.

To access the Transfer page, click **System > Utilities > Transfer** in the navigation menu.

**Figure 115.** Transfer

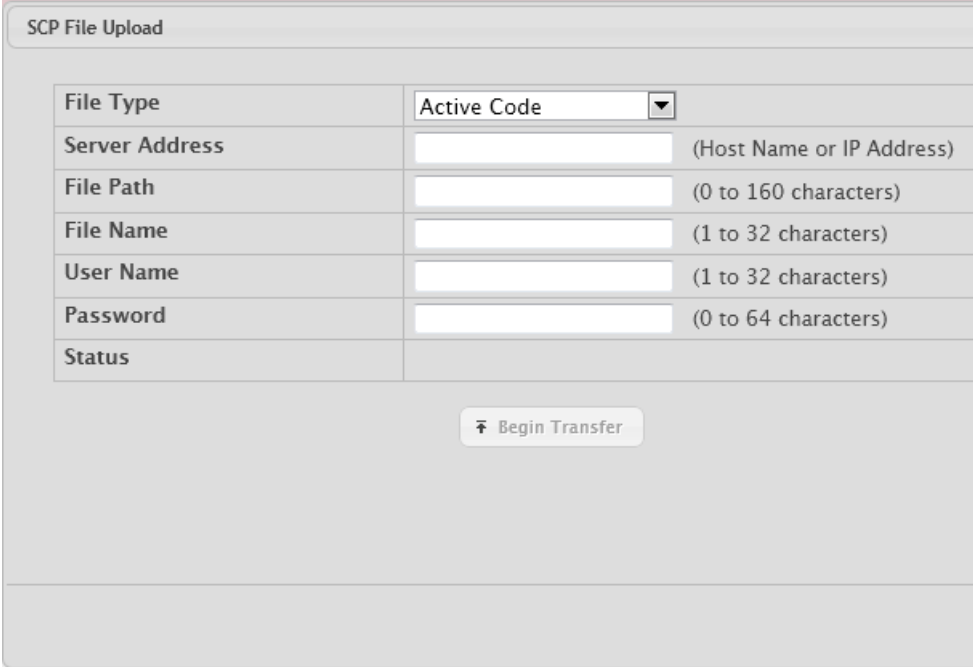


**Table 107.** Transfer Fields

Field	Description
Transfer Protocol	The protocol to use to transfer the file. Files can be transferred from the device to a remote system using TFTP, FTP, SCP or SFTP. Files can be transferred from a remote system to the device using HTTP, TFTP, FTP, SCP or SFTP.
Upload	To transfer a file from the device to a remote system using TFTP, FTP, SCP, or SFTP, click the upload icon in the same row as the desired transfer protocol. The <b>File Upload</b> window appears. Configure the information for the file transfer (described below), and click the upload icon to the right of the Progress field to begin the transfer.
Download	To transfer a file from a remote system to the device using HTTP, TFTP, FTP, SCP, or SFTP, click the download icon in the same row as the desired transfer protocol. The <b>File Download</b> window appears. Configure the information for the file transfer (described below), and click the download icon to the right of the Progress field to begin the transfer.

After you click the upload icon, the File Upload window appears.

**Figure 116.** File Upload



The image shows a dialog box titled "SCP File Upload". It contains a table with the following fields:

File Type	Active Code	
Server Address	<input type="text"/>	(Host Name or IP Address)
File Path	<input type="text"/>	(0 to 160 characters)
File Name	<input type="text"/>	(1 to 32 characters)
User Name	<input type="text"/>	(1 to 32 characters)
Password	<input type="text"/>	(0 to 64 characters)
Status		

Below the table is a button labeled "Begin Transfer" with an upward-pointing arrow icon.

The following information describes the fields in the File Upload window for all protocols.

**Table 108.** *File Upload Fields*

Field	Description
File Type	<p>Specify the type of file to transfer from the device to a remote system.</p> <ul style="list-style-type: none"> <li>• <b>Active Code</b> – Select this option to transfer an active image.</li> <li>• <b>Backup Code</b> – Select this option to transfer a backup image.</li> <li>• <b>Startup Configuration</b> – Select this option to transfer a copy of the stored startup configuration from the device to a remote system.</li> <li>• <b>Backup Configuration</b> – Select this option to transfer a copy of the stored backup configuration from the device to a remote system.</li> <li>• <b>Script File</b> – Select this option to transfer a custom text configuration script from the device to a remote system.</li> <li>• <b>CLI Banner</b> – Select this option to transfer the file containing the text to be displayed on the CLI before the login prompt to a remote system.</li> <li>• <b>Crash Log</b> – Select this option to transfer the system crash log to a remote system.</li> <li>• <b>Operational Log</b> – Select this option to transfer the system operational log to a remote system.</li> <li>• <b>Startup Log</b> – Select this option to transfer the system startup log to a remote system.</li> <li>• <b>Trap Log</b> – Select this option to transfer the system trap records to a remote system.</li> <li>• <b>Factory Defaults</b> – Select this option to transfer the factory default configuration file to a remote system.</li> <li>• <b>Error Log</b> – Select this option to transfer the system error (persistent) log, which is also known as the event log, to a remote system.</li> <li>• <b>Buffered Log</b> – Select this option to transfer the system buffered (in-memory) log to a remote system.</li> <li>• <b>Technical Support Log</b> – Select this option to transfer the technical support log to a remote system.</li> </ul>
Server Address	Specify the IPv4 address, IPv6 address, or DNS-resolvable hostname of the remote server that will receive the file.
File Path	Specify the path on the server where you want to put the file.
File Name	Specify the name that the file will have on the remote server.
User Name	For FTP, SCP, and SFTP transfers, if the server requires authentication, specify the user name for remote login to the server that will receive the file.
Password	For FTP, SCP and SFTP transfers, if the server requires authentication, specify the password for remote login to the server that will receive the file.
Progress	Represents the completion percentage of the file transfer. The file transfer begins after you complete the required fields and click the upload icon to the right of this field.
Status	Provides information about the status of the file transfer.

After you click the download icon, the File Download window appears.



**Figure 117.** File Download

SFTP File Download

File Type	Active Code	
Certificate Index	0	(1 to 8; 0 for None)
Server Address		(Host Name or IP Address)
File Path		(0 to 160 characters)
File Name		(1 to 48 characters)
User Name		(1 to 32 characters)
Password		(0 to 64 characters)
Status		

The following information describes the fields in the File Download window for all protocols.

**Table 109.** *File Download Fields*

Field	Description
File Type	<p>Specify the type of file to transfer to the device:</p> <ul style="list-style-type: none"> <li>• <b>Active Code</b> – Select this option to transfer a new image to the device. The code file is stored as the active image.</li> <li>• <b>Backup Code</b> – Select this option to transfer a new image to the device. The code file is stored as the backup image.</li> <li>• <b>Startup Configuration</b> – Select this option to update the stored startup configuration file. If the file has errors, the update will be stopped.</li> <li>• <b>Backup Configuration</b> – Select this option to update the stored backup configuration file. If the file has errors, the update will be stopped.</li> <li>• <b>Script File</b> – Select this option to transfer a text-based configuration script to the device. You must use the command-line interface (CLI) to validate and activate the script.</li> <li>• <b>CLI Banner</b> – Select this option to transfer the CLI banner file to the device. This file contains the text to be displayed on the CLI before the login prompt.</li> <li>• <b>IAS Users</b> – Select this option to transfer an Internal Authentication Server (IAS) users database file to the device. The IAS user database stores a list of user name and (optional) password values for local port-based user authentication.</li> <li>• <b>Factory Defaults</b> – Select this option to transfer the factory default configuration file to a remote system.</li> <li>• <b>SSL Trusted Root Certificate PEM File</b> – Select this option to transfer an SSL Trusted Root Certificate file (PEM Encoded) to the device. SSL files contain information to encrypt, authenticate, and validate HTTPS sessions.</li> <li>• <b>SSL Server Certificate PEM File</b> – Select this option to transfer an SSL Server Certificate file (PEM Encoded) to the device.</li> <li>• <b>SSL DH Weak Encryption Parameter PEM File</b> – Select this option to transfer an SSL Diffie-Hellman Weak Encryption Parameter file (PEM Encoded) to the device.</li> </ul>
	<ul style="list-style-type: none"> <li>• <b>SSL DH Strong Encryption Parameter PEM File</b> – Select this option to transfer an SSL Diffie-Hellman Strong Encryption Parameter file (PEM Encoded) to the device.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• To download SSH key files, SSH must be administratively disabled, and there can be no active SSH sessions.</li> <li>• To download SSL related files, HTTPS must be administratively disabled.</li> </ul>
Certificate Index	Index used to name a related group of certificate (PEM) or key files.
Select File	If HTTP is the Transfer Protocol, browse to the directory where the file is located and select the file to transfer to the device. This field is not present if the Transfer Protocol is TFTP or FTP.
Server Address	For TFTP, FTP, SCP, or SFTP transfers, specify the IPv4 address, IPv6 address, or DNS-resolvable hostname of the remote server.
File Path	For TFTP, FTP, SCP, or SFTP transfers, specify the path on the server where the file is located.
File Name	For TFTP, FTP, SCP, or SFTP transfers, specify the name of the file you want to transfer to the device.
User Name	For FTP, SCP, or SFTP transfers, if the server requires authentication, specify the user name for remote login to the server where the file resides.

**Table 109.** File Download Fields (continued)

Field	Description
Password	For FTP, SCP, or SFTP transfers, if the server requires authentication, specify the password for remote login to the server where the file resides.
Status	Provides information about the status of the file transfer.

## Core Dump

Use the Core Dump page to configure the Core Dump feature.

To access the Core Dump page, click **System > Utilities > Core Dump** in the navigation menu.

**Figure 118.** Core Dump

**Table 110.** Core Dump Configuration Fields

Field	Description
Protocol	The protocol used to store the core dump file. User can select: <ul style="list-style-type: none"> <li>• <b>None</b>—Disable Core Dump.</li> <li>• <b>TFTP</b>—Configure protocol to upload Core Dump to the TFTP server.</li> <li>• <b>FTP</b>—Configure protocol to upload Core Dump to the FTP server.</li> </ul>
Core Dump File Name Prefix	Prefix for the Core Dump file name. If hostname is configured, it takes else while generating Core Dump file. The prefix length is 15 characters.

**Table 110.** *Core Dump Configuration Fields (continued)*

Field	Description
Use Host Name	To use hostname (or MAC if hostname is not configured) to name Core Dump file.
Use Time Stamp	To use timestamp to name Core Dump file.
TFTP IP Address	IP address of remote TFTP server to dump core file to external server.
FTP IP Address	IP address of remote FTP server to dump core file to external server.
FTP Username	Username of remote FTP server.
FTP Password	Password of remote FTP server.
File Path	File path to dump core file to TFTP server or NFS mount sub-directory.
Compression Mode	To enable or disable compression mode.
Switch Chip Registers Dump	To enable or disable switch-chip-register dump in case of an exception. The switch-chip-register dump is taken only for master unit and not for member units.
Stack IP Address Protocol	Protocol (DHCP or Static) to be used to configure service port when a unit has crashed. If configured as DHCP, the unit gets the IP address from DHCP server available in the network. If configured as Static, an IP address from the Core Dump Stack IP Address Pool is used.

**Table 111.** *Core Dump Stack IP Address Pool Fields*

Field	Description
IP Address	Static IP address to be assigned to individual unit's service port in the stack when the switch has crashed. This IP address is used to perform the core dump.
Host Mask	The subnet mask.
Default Router Address	The IP address of the router.

To add a stack IP address, click **Add** and configure an IP address, netmask, and gateway address.

To delete a configured stack IP, select each entry to delete, click **Remove**, and confirm the action.

## Core Dump Test

Use the Core Dump Test page to test the core dump setup. For example, if protocol is configured as TFTP, it communicates with the TFTP server and informs the user if the TFTP server can be contacted.

To access the Core Dump Test page, click **System > Utilities > Core Dump Test** in the navigation menu.

**Figure 119.** Core Dump Test



**Table 112.** Core Dump Test Fields

Field	Description
Status	Displays test status as <b>OK</b> if test passes and <b>Error</b> if test fails.
Result	Displays detailed error information with logs.

# Managing SNMP Traps

The pages in the Trap Manager folder allow you to view and configure information about SNMP traps the system generates.

## Trap Log

Use the Trap Log page to view the entries in the trap log.

To access the Trap Log page, click **System > Advanced Configuration > Trap Manager > Trap Log** in the navigation menu.

**Figure 120.** Trap Log

The screenshot shows the 'System Trap Log' page. At the top, there are tabs for 'Trap Log' (selected) and 'Trap Flags'. Below the tabs is a summary table:

Trap Log Capacity	256
Number of Traps Since Last Reset	16
Number of Traps Since Log Last Viewed	16

Below the summary table, there is a 'Display' dropdown set to '10' rows and a 'Showing 1 to 10 of 16 entries' indicator. The main table lists trap entries with columns for 'Log', 'System Up Time', and 'Trap'.

Log	System Up Time	Trap
0	Feb 14 22:10:17 2019	Session 0 of type 1 ended for user admin connecte
1	Feb 14 22:05:11 2019	Cold Start: Unit: 0
2	Feb 14 22:04:40 2019	Link Up: 1/0/27
3	Feb 14 22:04:38 2019	Link Up: 1/0/26
4	Feb 14 22:04:38 2019	Link Down: 1/0/26
5	Feb 14 22:04:33 2019	Link Up: 1/0/26
6	Feb 14 22:04:33 2019	Temperature state change alarm: Unit Number: 1 C
7	Feb 14 22:04:33 2019	SFP inserted in 1/0/28
8	Feb 14 22:04:33 2019	SFP inserted in 1/0/27
9	Feb 14 22:04:33 2019	SFP inserted in 1/0/26

At the bottom of the table, there are navigation buttons: 'First', 'Previous', '1', '2', 'Next', and 'Last'.

**Table 113.** Trap Log Fields

Field	Description
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries will overwrite the oldest entries.
Number of Traps Since Last Reset	The number of traps generated since the trap log entries were last cleared.
Number of Traps Since Log Last Viewed	The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, Web display, upload file from switch, etc.) will cause this counter to be cleared to 0.
Log	The sequence number of this trap.
System Up Time	The time at which this trap occurred, expressed in days, hours, minutes and seconds since the last reboot of the switch.
Trap	Displays the information identifying the trap.

Click **Clear Log** to clear all entries in the log. Subsequent displays of the log will only show new log entries.

## Trap Flags

Use the Trap Flags page to enable or disable traps the switch can send to an SNMP manager. When the condition identified by an active trap is encountered by the switch, a trap message is sent to any enabled SNMP Trap Receivers, and a message is written to the trap log.

To access the Trap Flags page, click **System > Advanced Configuration > Trap Manager > Trap Flags** page.

**Figure 121.** Trap Flags Configuration

Field	Status
Authentication	<input checked="" type="checkbox"/>
Link Up/Down	<input checked="" type="checkbox"/>
Multiple Users	<input checked="" type="checkbox"/>
Spanning Tree	<input checked="" type="checkbox"/>
ACL Traps	<input type="checkbox"/>
Fan	<input checked="" type="checkbox"/>
Power Supply Module State	<input checked="" type="checkbox"/>
Temperature	<input checked="" type="checkbox"/>

The fields available on the Trap Flags page depends on the packages installed on your system. [Figure 121](#) and [Table 114](#) shows the fields that are available on a system with all packages installed.

**Table 114.** Trap Flags Configuration Fields

Field	Description
Authentication	Enable or disable activation of authentication failure traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
Link Up/Down	Enable or disable activation of link status traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
Multiple Users	Enable or disable activation of multiple user traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled. This trap is triggered when the same user ID is logged into the switch more than once at the same time (either via telnet or the serial port).
Spanning Tree	Enable or disable activation of spanning tree traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
ACL Traps	Enable or disable activation of ACL traps by selecting the corresponding line on the pull-down entry field. The factory default is disabled.

**Table 114.** *Trap Flags Configuration Fields*

Field	Description
Fan	Specify whether to enable SNMP notifications when fan events occur.
Power Supply Module State	Specify whether to enable SNMP notifications when power supply events occur.
Temperature	Specify whether to enable SNMP notifications when temperature events occur.

- If you make any changes to this page, click **Submit** to apply the changes to the system.
- If you want the device to retain these changes across a reset, you must first save the configuration by clicking **Save Configuration**.
- Click **Refresh** to redisplay the page with the current data from the switch.



## Managing the DHCP Server

DHCP is generally used between clients (e.g., hosts) and servers (e.g., routers) for the purpose of assigning IP addresses, gateways, and other networking definitions such as DNS, NTP, and/or SIP parameters. The DHCP Server folder contains links to web pages that define and display DHCP parameters and data.

### Global Configuration

Use the Global Configuration page to configure DHCP global parameters.

To display the page, click **System > Advanced Configuration > DHCP Server > Global** in the navigation menu.

**Figure 122.** DHCP Server Global Configuration

Global	Excluded Addresses	Pool Summary	Pool Configuration	Pool Options	Bindings	Statistics	Conf
<b>DHCP Server Global Configuration</b>							
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable						
Conflict Logging Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable						
Bootp Automatic Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable						
Ping Packet Count	<input type="text" value="2"/> (0 to 10)						
<input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="Cancel"/>							

**Table 115.** DHCP Server Global Configuration Fields

Field	Description
Admin Mode	Enables or disables the DHCP server administrative mode. When enabled, the device can be configured to automatically allocate TCP/IP configurations for clients.
Conflict Logging Mode	Enables or disables the logging mode for IP address conflicts. When enabled, the system stores information IP address conflicts that are detected by the DHCP server.
Bootp Automatic Mode	Enables or disables the BOOTP automatic mode. When enabled, the DHCP server supports the allocation of automatic addresses for BOOTP clients. When disabled the DHCP server supports only static addresses for BOOTP clients.
Ping Packet Count	The number of packets the server sends to a pool address to check for duplication as part of a ping operation. If the server receives a response to the ping, the address is considered to be in conflict and is removed from the pool.

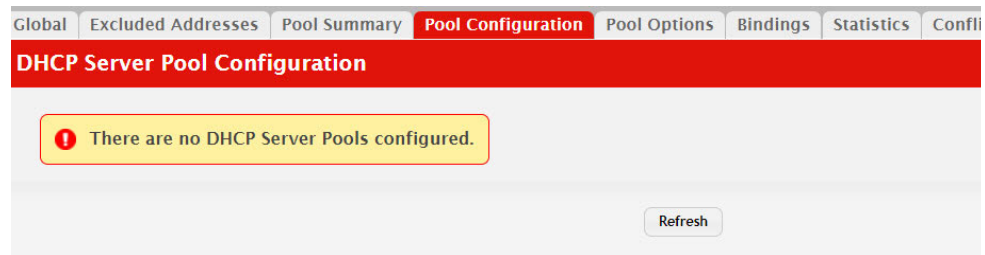
- If you change any settings or add an excluded address range, click **Submit** to apply the changes to the system. Each time you enter a value in the **From** or **To** fields, click **Submit** to add the address or address range to the excluded address list.
- To Delete an address or address range from the excluded address list, select one or more check box beneath the Delete **Excluded Addresses** field and click **Submit**.

## Pool Configuration

Use the DHCP Pool Configuration page to create the pools of addresses that can be assigned by the server.

To access the Pool Configuration page, click **System > Advanced Configuration > DHCP Server > Pool Configuration** in the navigation menu.

**Figure 123.** Pool Configuration



If you select **Automatic** or **Manual** from the **Type of Binding** drop-down menu, the screen refreshes and a slightly different set of fields appears.

**Table 116.** Pool Configuration Fields

Field	Description
Pool Name	For a user with read/write permission, this field would show names of all the existing pools along with an additional option Create. When the user selects Create, another text box, Pool Name, appears where the user may enter name for the Pool to be created. For a user with read-only permission, this field would show names of the existing pools only.
Type of Binding	Specifies the type of binding for the pool. <ul style="list-style-type: none"> <li>• <b>Unallocated:</b> The addresses are not assigned to a client.</li> <li>• <b>Automatic:</b> The IP address is automatically assigned to a client by the DHCP server.</li> <li>• <b>Manual:</b> You statically assign an IP address to a client based on the client's MAC address.</li> </ul>
Network Base Address	(Dynamic pools only) The network portion of the IP address. A DHCP client can be offered any available IP address within the defined network as long as it has not been configured as an excluded address.
Network Mask	For dynamic bindings, this field specifies the subnet mask for a DHCP address of a dynamic pool. You can enter a value in Network Mask <b>or</b> Prefix Length to specify the subnet mask, but do not enter a value in both fields.
Client Name	For manual bindings, this field specifies a name for the client to which the DHCP server will statically assign an IP address. This field is optional.
Hardware Address Type	For manual bindings, this field specifies the protocol of the hardware platform of the DHCP client. Valid types are ethernet and ieee802. Default value is ethernet.
Hardware Address	For manual bindings, this field specifies the MAC address of the hardware platform of the DHCP client.

**Table 116.** Pool Configuration Fields (continued)

Field	Description
Client ID	(Manual pools only) The value some DHCP clients send in the Client Identifier field of DHCP messages. This value is typically identical to the Hardware Address value. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of the hardware address. If the client's DHCP request includes the client identifier, the Client ID field on the DHCP server must contain the same value, and the Hardware Address Type field must be set to the appropriate value. Otherwise, the DHCP server will not respond to the client's request.
Host IP Address	(Manual pools only) The IP address to offer the client.
Host Mask	For manual bindings, this field specifies the subnet mask to be statically assigned to a DHCP client. You can enter a value in Host Mask <b>or</b> Prefix Length to specify the subnet mask, but do not enter a value in both fields.
Lease Expiration	Indicates whether the information the server provides to the client should expire. <ul style="list-style-type: none"> <li>• <b>Enable</b> – Allows the lease to expire. If you select this option, you can specify the amount of time the lease is valid in the Lease Duration field.</li> <li>• <b>Disable</b> – Sets an infinite lease time. For Dynamic bindings, an infinite lease time implies a lease period of 60 days. For a Manual binding, an infinite lease period never expires.</li> </ul>
Lease Duration	<ul style="list-style-type: none"> <li>• The number of Days, Hours, and Minutes the lease is valid. This field cannot be configured if the Lease Expiration is disabled.</li> </ul>
Next Server Address	<p>The IP address of the next server the client should contact in the boot process. For example, the client might be required to contact a TFTP server to download a new image file. To configure this field, click the Edit icon in the row. To reset the field to the default value, click the Reset icon in the row.</p> <p>To configure settings for one or more default routers, DNS servers, or NetBIOS servers that can be used by the client(s) in the pool, use the buttons available in the appropriate table to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• To add an entry to the server list, click the + (plus) button and enter the IP address of the server to add.</li> <li>• To edit the address of a configured server, click the <b>Edit</b> icon associated with the entry to edit and update the address.</li> <li>• To delete an entry from the list, click the – (minus) button associated with the entry to remove.</li> <li>• To delete all entries from the list, click the – (minus) button in the heading row.</li> </ul>
Default Router	Lists the IP address of each router to which the client(s) in the pool should send traffic. The default router should be in the same subnet as the client.
DNS Server	Lists the IP address of each DNS server the client(s) in the pool can contact to perform address resolution.
NetBIOS Server	Lists the IP address of each NetBIOS Windows Internet Naming Service (WINS) name server that is available for the selected pool.

- After you configure values for the DHCP address pool, click **Submit** to create the pool and apply the changes to the system.
- To delete a pool, select the pool from the **Pool Name** drop-down menu and click **Delete**.

## Pool Options

Use the Pool Options page to configure additional DHCP pool options, including vendor-defined options. DHCP options are collections of data with type codes that indicate how the options should be used. When a client broadcasts a request for information, the request includes the option codes that correspond to the information the client wants the DHCP server to supply.

To access the Pool Options page, click **System > Advanced Configuration > DHCP Server > Pool Options** in the navigation menu.

If no DHCP pools exist, the Pool Options page does not display the fields shown in [Figure 124](#).

**Figure 124.** Pool Options

If any DHCP pools are configured on the system, the Pool Options page contains the following fields:

**Table 117.** Pool Options Fields

Field	Description
Pool Name	Select the DHCP pool to with the options you want to view or configure.
Option Code	Displays the DHCP option code configured for the selected Pool.
Option Type	Specifies the type of option associated with the option code configured for the selected pool. The possible values are as follows: <ul style="list-style-type: none"> <li><b>Ascii:</b> The option type is a text string.</li> <li><b>Hex:</b> The option type is a hexadecimal number.</li> <li><b>IP Address:</b> The option type is an IP address.</li> </ul>
ASCII Value	Shows the Option ASCII Value for the selected pool.
Hex Value	Shows the Option Hex Value for the selected pool.
IP Address Value	Shows the Option IP Address Value for the selected pool.

**Table 117.** Pool Options Fields (continued)

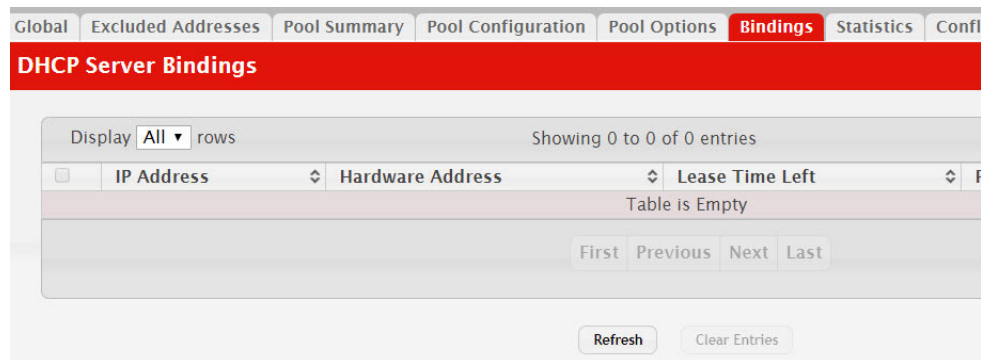
Field	Description
Delete Option Code	To delete an option code for the selected Pool, enter the option code in the folder and click <b>Delete</b> . This button is not visible to a user with read-only permission.

## Bindings Information

Use the Bindings Information page to view information about the IP address bindings in the DHCP server database.

To access the Bindings Information page, click **System > Advanced Configuration > DHCP Server > Bindings** in the navigation menu.

**Figure 125.** Bindings Information



**Table 118.** Bindings Information Fields

Field	Description
IP Address	The IP Address of the DHCP client.
Hardware Address	The MAC address of the DHCP client.
Lease Time Left	The amount of time left until the lease expires in days, hours, and minutes.
Pool Allocation Type	The type of binding used: <ul style="list-style-type: none"> <li>• <b>Dynamic</b> – The address was allocated dynamically from a pool that includes a range of IP addresses.</li> <li>• <b>Manual</b> – A static IP address was assigned based on the MAC address of the client.</li> <li>• <b>Inactive</b> – The pool is not in use.</li> </ul>
Clear Entries (Button)	To remove an entry from the table, select each entry to delete and click <b>Clear Entries</b> . You must confirm the action before the binding is deleted.

If you change any settings, click **Submit** to apply the changes to the system.

## Server Statistics

Use the DHCP Server Statistics page to view information about the DHCP server bindings and messages. To access the Server Statistics page, click **System > Advanced Configuration > DHCP Server > Statistics** in the navigation menu.

**Figure 126.** Server Statistics

Global	Excluded Addresses	Pool Summary	Pool Configuration	Pool Options	Bindings	Statistics	Conflicts
<b>DHCP Server Statistics</b>							
Automatic Bindings		0					
Expired Bindings		0					
Malformed Messages		0					
DHCP DISCOVER packets discarded		0					
<b>Messages Received</b>							
DHCPDISCOVER		0					
DHCPREQUEST		0					
DHCPDECLINE		0					
DHCPRELEASE		0					
DHCPINFORM		0					
<b>Messages Sent</b>							
DHCPOFFER		0					
DHCPACK		0					
DHCPNAK		0					
				Refresh		Clear Counters	

**Table 119.** Server Statistics Fields

Field	Description
Automatic Bindings	Shows the number of automatic bindings on the DHCP server.
Expired Bindings	Shows the number of expired bindings on the DHCP server.
Malformed Messages	Shows the number of the malformed messages.
DHCP DISCOVER Packets Discarded	The number of messages discarded from one or more DHCP Discover.
<b>Message Received</b>	
DHCPDISCOVER	Shows the number of DHCPDISCOVER messages received by the DHCP server.
DHCPREQUEST	Shows the number of DHCPREQUEST messages received by the DHCP server.
DHCPDECLINE	Shows the number of DHCPDECLINE messages received by the DHCP server.
DHCPRELEASE	Shows the number of DHCPRELEASE messages received by the DHCP server.
DHCPINFORM	Shows the number of DHCPINFORM messages received by the DHCP server.
<b>Message Sent</b>	
DHCPOFFER	The number of DHCP offer messages the DHCP server has sent to DHCP clients in response to DHCP discovery messages it has received.
DHCPACK	The number of DHCP acknowledgment messages the DHCP server has sent to DHCP clients in response to DHCP request messages it has received. The server sends this message after the client has accepted the offer from this particular server. The DHCP acknowledgment message includes information about the lease time and any other configuration information that the DHCP client has requested.

**Table 119.** *Server Statistics Fields (continued)*

Field	Description
DHCPNAK	The number of negative DHCP acknowledgment messages the DHCP server has sent to DHCP clients. A server might send this type of message if the client requests an IP address that is already in use or if the server refuses to renew the lease.

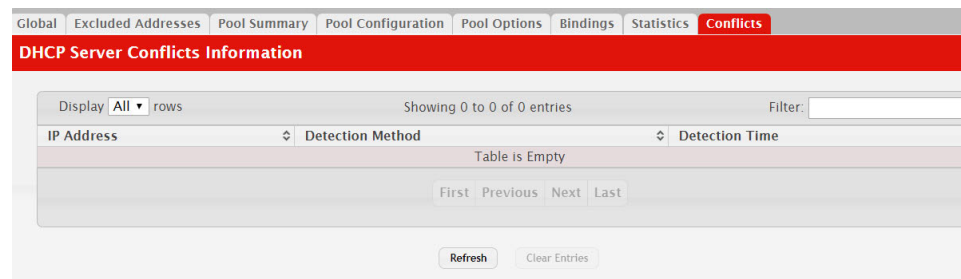
- Click **Refresh** to update the information on the screen.
- Click **Clear Counters** to reset all DHCP server statistics counters.

## Conflicts Information

Use the Conflicts Information page to view information on hosts that have address conflicts; i.e., when the same IP address is assigned to two or more devices on the network.

To access the Conflicts Information page, click **System > Advanced Configuration > DHCP Server > Conflicts Information** in the navigation menu.

**Figure 127.** Conflicts Information



**Table 120.** *Conflicts Information Fields*

Field	Description
IP Address	The IP address that has been detected as a duplicate.
Detection Method	The method used to detect the conflict, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Gratuitous ARP</b> – The DHCP client detected the conflict by broadcasting an ARP request to the address specified in the DHCP offer message sent by the server. If the client receives a reply to the ARP request, it declines the offer and reports the conflict.</li> <li>• <b>Ping</b> – The server detected the conflict by sending an ICMP echo message (ping) to the IP address before offering it to the DHCP client. If the server receives a response to the ping, the address is considered to be in conflict and is removed from the pool.</li> <li>• <b>Host Declined</b> – The server received a DHCPDECLINE message from the host. A DHCPDECLINE message indicates that the host has discovered that the IP address is already in use on the network.</li> </ul>
Detection Time	The time when the conflict was detected in days, hours, minutes and seconds since the system was last reset (i.e., system up time).

**Table 120.** *Conflicts Information Fields (continued)*

Field	Description
Clear Entries (Button)	Clears all of the address conflict entries.



## Configuring Time Ranges

You can use these pages to configure time ranges to use in time-based access control list (ACL) rules. Time-based ACLs allow one or more rules within an ACL to be based on a periodic or absolute time. Each ACL rule within an ACL except for the implicit *deny all* rule can be configured to be active and operational only during a specific time period. The time range pages allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined within an ACL.

### Time Range Configuration

Use this page to create a named time range. Each time range can consist of one absolute time entry and/or one or more periodic time entries.

To access this page, click **System > Advanced Configuration > Time Ranges > Configuration**.

**Figure 128.** Time Range



**Table 121.** Time Range Configuration

Field	Description
Admin Mode	Enables or disables the Time Range administrative mode. When enabled, actions with subscribed components are performed for existing time range entries.
Time Range Name	The unique ID or name that identifies this time range. A time-based ACL rule can reference the name configured in this field.
Time Range Status	Shows whether the time range is Active or Inactive. A time range is Inactive if the current day and time do not fall within any time range entries configured for the time range.
Periodic Entry Count	The number of periodic time range entries currently configured for the time range.
Absolute Entry	Shows whether an absolute time entry is currently configured for the time range.

Use the buttons to perform the following tasks:

- To add a time range, click **Add** and configure a name for the time range configuration.
- To delete a configured time range, select each entry to delete, click **Remove**, and confirm the action.
- Use **Submit** to add a new time range.

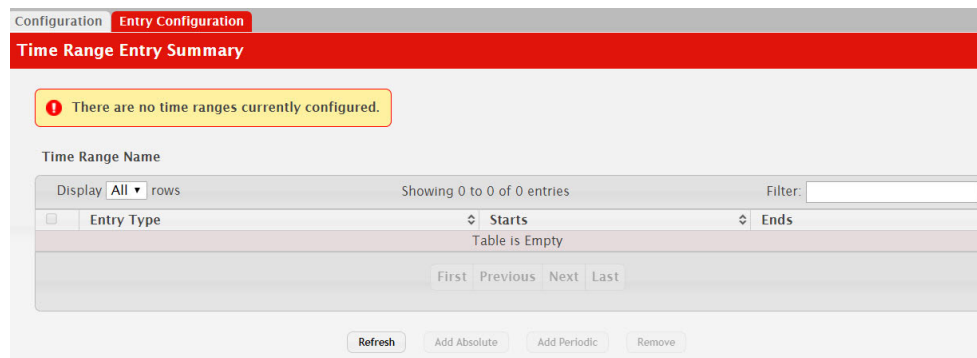
## Time Range Entry Configuration

Use this page to configure periodic and absolute time range entries and add them to named time ranges.

**Note:** The time range entries use the system time for the time periods in which they take effect. Make sure you configure the SNTP server settings so that the SNTP client on the switch can obtain the correct date and time from the server.

To access this page, click **System > Advanced Configuration > Time Ranges > Entry Configuration**.

**Figure 129.** Time Range Entry Configuration



To configure the time range entries for a time range configuration, select the time range configuration from the Time Range Name menu and use the buttons to perform the following tasks:

- To add an Absolute time range entry, click **Add Absolute** and configure information about when the Absolute entry occurs. If the **Add Absolute** button is not available, an Absolute entry already exists for the selected time range configuration.
- To add a Periodic time range entry, click **Add Periodic** and specify the days and times that the entry is in effect.
- To delete a time range entry, select each entry to delete, click **Remove**, and confirm the action.

**Table 122.** Time Range Entry Configuration

Field	Description
Time Range Name	Select the name of the time range to which you want to add a time range entry.
Time Range Entry	Select Create New Time Range Entry to add a new entry to a time range. To view or delete an existing time range entry, select its ID from the menu.
Time Range Entry ID	When creating a new time range entry, assign a unique ID number from 1–10. This field does not appear if the entry has already been configured.
Time Range Entry Type.	Specifies whether the entry is periodic or absolute. A periodic entry occurs at the same time every day or on one or more days of the week. An absolute entry does not repeat.
Periodic Time Range Entry	

**Table 122.** *Time Range Entry Configuration (continued)*

Field	Description
Applicable Days	Specify the day(s) when the time entry occurs: <ul style="list-style-type: none"> <li>• <b>Daily</b>–Has the same start and end time every day</li> <li>• <b>Weekdays</b>–Has the same start and end time Monday through Friday</li> <li>• <b>Weekdays</b>–Has the same start and end time on Saturday and Sunday</li> <li>• <b>Days of the Week</b>–Select the day of the week when the entry starts and stops. You do not need to use the same day of the week for the start and end time.</li> </ul>
Start Day	(Periodic Days of Week only) Select the day the time range entry starts. To select multiple days, hold the <b>CTRL</b> key and click the days.
Start Time	Specify the time when the entry begins. The time is based on a 24-hour clock. For example, 6:00 PM is 18:00.
End Day	(Periodic Days of Week only) Select the day the time range entry ends.
End Time	Specify the time when the entry ends. The time is based on a 24-hour clock. For example, 6:00 PM is 18:00.
<b>Absolute Time Range Entry</b>	
Absolute Start Date and Time	Select the check box to configure the date and time when the time range entry begins.
Start Month	Select the month when the time entry begins.
Start Date	Select the day of the month when the time entry begins.
Start Year	Select the year when the time entry begins.
Start Time	Specify the time when the entry begins. The time is based on a 24-hour clock. For example, 6:00 PM is 18:00.
Absolute End Date and Time	Select the check box to configure the date and time when the time range entry ends.
End Month	Select the month when the time entry ends.
End Date	Select the day of the month when the time entry ends.
End Year	Select the year when the time entry ends.
End Time	Specify the time when the entry ends. The time is based on a 24-hour clock. For example, 6:00 PM is 18:00.

Click **Submit** to create the time range entry. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

## Configuring DNS

You can use these pages to configure information about DNS servers the network uses and how the switch/router operates as a DNS client.

### Global Configuration

Use this page to configure global DNS settings and to view DNS client status information.

To access this page, click **System > Advanced Configuration > DNS > Configuration**.

**Figure 130.** DNS Global Configuration

**Table 123.** DNS Global Configuration Fields

Field	Description
Admin Mode	Select <b>Enable</b> or <b>Disable</b> from the pull-down menu to set the administrative status of DNS Client. The default is Disable.
Default Domain Name	Enter the default domain name for DNS client messages. The name should be no longer than 255 characters. When the system is performing a lookup on an unqualified hostname, this field is provided as the domain name (e.g., if default domain name is <i>is.com</i> and the user enters <i>hotmail</i> , then hotmail is changed to <i>hotmail.com</i> to resolve the name). By default, no default domain name is configured in the system.
Retry Number	Enter the number of times to retry sending DNS queries. The valid values are from 0 to 100. The default value is 2.
Response Timeout	Enter the number of seconds to allow a DNS server to respond to a request before issuing a retry. Valid values are 0 to 3600. The default value is 3.
Domain List	Enter a domain list to define the domain to use when performing a lookup on an unqualified hostname. Each name must be no more than 256 characters. Multiple default domain names can be configured using the default domain-name list. If there is no domain list, the default domain name configured is used.

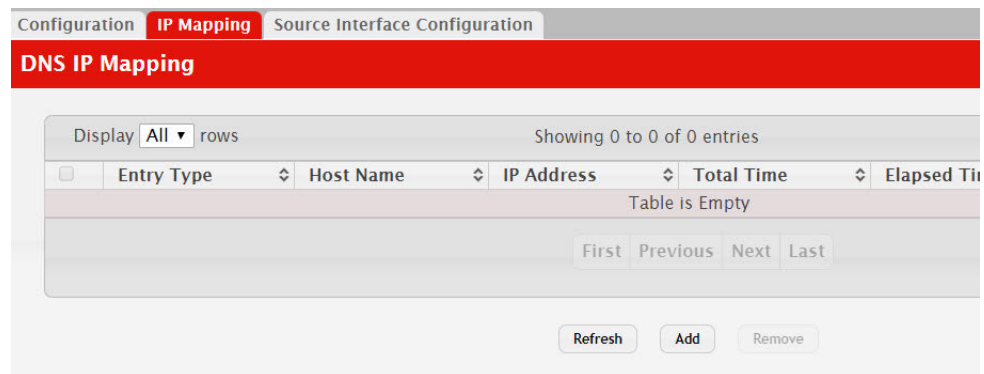
- If you change any settings, click **Submit** to send the information to the system.
- To create a new list of domain names, click **Create**. Then enter a name of the list and click submit. Repeat this step to add multiple domains to the default domain list.
- To remove a domain from the default list select the **Remove** option next to the item you want to remove and click **Submit**.

## DNS Host Name IP Mapping Configuration

Use this page to configure DNS host names for hosts on the network and to view dynamic DNS entries. The host names are associated with IPv4 or IPv6 addresses on the network, which are statically assigned to particular hosts.

To access this page, click **System > Advanced Configuration > DNS > IP Mapping** in the menu.

**Figure 131.** DNS Host Name IP Mapping Summary



**Table 124.** DNS Host Name IP Mapping Summary Fields

Field	Description
DNS Static Entries	
Entry Type	Type of DNS entry: <ul style="list-style-type: none"> <li>• <b>Static</b> – An entry that has been manually configured on the device.</li> <li>• <b>Dynamic</b> – An entry that the device has learned by using a configured DNS server to resolve a hostname.</li> </ul>
Host Name	The name that identifies the system. For Static entries, specify the Host Name after you click <b>Add</b> .
IP Address	The IPv4 or IPv6 address associated with the configured Host Name. For Static entries, specify the IP Address after you click <b>Add</b> . You can specify either an IPv4 or an IPv6 address.
DNS Dynamic Entries	
Total Time	The number of seconds that the entry will remain in the table.
Elapsed Time	The number of seconds that have passed since the entry was added to the table. When the Elapsed Time reaches the Total Time, the entry times out and is removed from the table.
Dynamic Type	The type of address in the entry, for example IP or (less common) X.121.

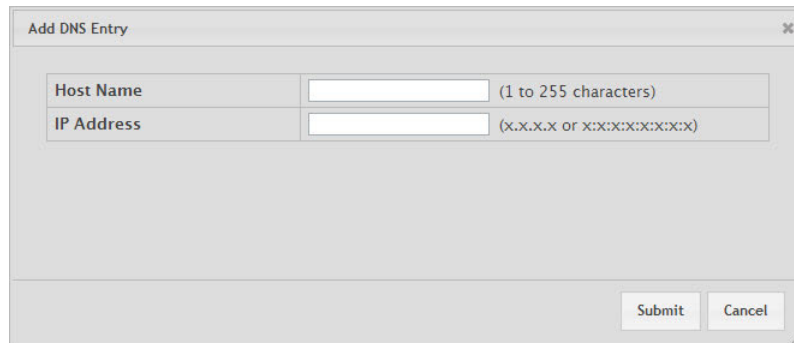
## Command Buttons

The page includes the following command buttons:

- Click **Add Static Entry** to load the Host Name IP Mapping Configuration page in order to configure the Host Name IP Mapping entries.
- Click **Submit** to apply the new configuration and cause the change to take effect immediately. These changes will not be retained across a power cycle unless a Save is performed.
- Click **Clear Dynamic Entries** to remove all Host Name IP Mapping entries. A confirmation prompt will be displayed. Click the button to confirm removal and the Host Name IP Mapping dynamic entries are cleared.
- Click Refresh to refresh the page with the most current data from the switch.

If you click **Add**, the DNS Host Name IP Mapping Configuration page appears.

**Figure 132.** DNS Host Name Mapping Configuration



The screenshot shows a dialog box titled "Add DNS Entry". It has two input fields: "Host Name" and "IP Address". The "Host Name" field has a placeholder text "(1 to 255 characters)". The "IP Address" field has a placeholder text "(x.x.x.x or x:x:x:x:x:x:x:x)". At the bottom right of the dialog box, there are two buttons: "Submit" and "Cancel".

**Table 125.** DNS Host Name Mapping Configuration Fields

Field	Description
Host Name	Enter the host name to assign to the static entry.
IP Address	Enter the IP4 or IPv6 address associated with the host name.

## Command Buttons

The page includes the following command buttons:

- Click **Submit** to apply the new configuration and cause the change to take effect immediately. These changes will not be retained across a power cycle unless a Save is performed.
- Click **Cancel** to cancel and redisplay the hostname IP mapping page to see the configured hostname-IP mapping entries.

## DNS Source Interface Configuration

Use this page to specify the physical or logical interface to use as the DNS client source interface. When an IP address is configured on the source interface, this address is used for all DNS communications between the local DNS client and the

remote DNS server. The IP address of the designated source interface is used in the IP header of DNS management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device.

To access the DNS Source Interface Configuration page, click **System > Advanced Configuration > DNS > Source Interface Configuration** in the menu.

**Figure 133.** DNS Source Interface Configuration

**Table 126.** DNS Source Interface Configuration Fields

Field	Description
Type	The type of interface to use as the source interface: <ul style="list-style-type: none"> <li>• <b>None</b> – The primary IP address of the originating (outbound) interface is used as the source address.</li> <li>• <b>Interface</b> – The primary IP address of a physical port is used as the source address.</li> <li>• <b>VLAN</b> – The primary IP address of a VLAN routing interface is used as the source address.</li> <li>• <b>Loopback</b> – The primary IP address of the loopback interface is used as the source address. A loopback is always reachable, as long as any routing interface is up.</li> <li>• <b>Network</b> – The network source IP is used as the source address.</li> <li>• <b>Service Port</b> – The management port source IP is used as the source address.</li> </ul>
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
VLAN	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.
Loopback Interface	When the selected Type is Loopback, select the loopback interface to use as the source interface.

If you change any of the settings on the page, click **Submit** to apply the changes to system.



---

## Configuring SNTP Settings

CE0128XB/CE0152XB software supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. CE0128XB/CE0152XB software operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by stratum. Stratum defines the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above since it is itself a stratum 2 device.

The following is an example of stratum:

- **Stratum 0:** A real time clock is used as the time source, for example, a GPS system.
- **Stratum 1:** A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2:** The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the time level and server type.

SNTP time definitions are assessed and determined by the following time levels:

- **T1:** Time at which the original request was sent by the client.
- **T2:** Time at which the original request was received by the server.
- **T3:** Time at which the server sent a reply.
- **T4:** Time at which the client received the server's reply.

The device can poll Unicast and Broadcast server types for the server time.

Polling for Unicast information is used for polling a server for which the IP address is known. SNTP servers that have been configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the SNTP Server Configuration page.

Broadcast information is used when the server IP address is unknown. When a Broadcast message is sent from an SNTP server, the SNTP client listens to the message. If Broadcast polling is enabled, any synchronization information is accepted, even if it has not been requested by the device. This is the least secure method.

The device retrieves synchronization information, either by actively requesting information or at every poll interval. If Unicast and Broadcast polling are enabled, the information is retrieved in this order:

- Information from servers defined on the device is preferred. If Unicast polling is not enabled or if no servers are defined on the device, the device accepts time information from any SNTP server that responds.
- If more than one Unicast device responds, synchronization information is preferred from the device with the lowest stratum.
- If the servers have the same stratum, synchronization information is accepted from the SNTP server that responded first.

MD5 (Message Digest 5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

## SNTP Global Configuration

Use the SNTP Global Configuration page to view and adjust SNTP parameters.

To display the SNTP Global Configuration page, click **System > Advanced Configuration > SNTP > Global Configuration** in the navigation menu.

**Figure 134.** SNTP Global Configuration

Field	Value	Range
Client Mode	Disable	
Port	None	
Unicast Poll Interval (Seconds)	6	(6 to 10)
Broadcast Poll Interval (Seconds)	6	(6 to 10)
Unicast Poll Timeout (Seconds)	5	(1 to 30)
Unicast Poll Retry	1	(0 to 10)
Number of Servers Configured	None	

**Table 127.** SNTP Global Configuration Fields

Field	Description
Client Mode	Use drop-down list specify the SNTP client mode, which is one of the following modes: <ul style="list-style-type: none"> <li>• <b>Disable:</b> SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed.</li> <li>• <b>Unicast:</b> SNTP operates in a point to point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally the round-trip delay and local clock offset relative to the server.</li> <li>• <b>Broadcast:</b> SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has Internet wide scope.</li> </ul>

**Table 127.** *SNTP Global Configuration Fields (continued)*

Field	Description
Port	Specifies the local UDP port to listen for responses/broadcasts. Allowed range is (1 to 65535). Default value is 123.
Unicast Poll Interval	Specifies the number of seconds between unicast poll requests expressed as a power of two when configured in unicast mode. Allowed range is (6 to 10). Default value is 6.
Broadcast Poll Interval	Specifies the number of seconds between broadcast poll requests expressed as a power of two when configured in broadcast mode. Broadcasts received prior to the expiry of this interval are discarded. Allowed range is (6 to 10). Default value is 6.
Unicast Poll Timeout	Specifies the number of seconds to wait for an SNTP response when configured in unicast mode. Allowed range is (1 to 30). Default value is 5.
Unicast Poll Retry	Specifies the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode. Allowed range is (0 to 10). Default value is 1.
Number of Servers Configured	Specifies the number of current valid unicast server entries configured for this client.

If you change any of the settings on the page, click **Submit** to apply the changes to system.

## SNTP Global Status

Use the SNTP Global Status page to view information about the system's SNTP client.

To access the SNTP Global Status page, click **System > Advanced Configuration > SNTP > Global Status** in the navigation menu.

**Figure 135.** Global Status

SNTP Global Status	
Version	4
Supported Mode	Unicast and Broadcast
Last Update Time	Jan 1 00:00:00 1970
Last Attempt Time	Jan 1 00:00:00 1970
Last Attempt Status	Other
Server IP Address	
Address Type	Unknown
Server Stratum	0
Reference Clock ID	
Server Mode	Reserved
Unicast Server Max Entries	3
Unicast Server Current Entries	0
Broadcast Count	0

**Table 128.** *Global Status Fields*

Field	Description
Version	Specifies the SNTP Version the client supports.
Supported Mode	Specifies the SNTP modes the client supports. Multiple modes may be supported by a client.
Last Update Time	Specifies the local date and time (UTC) the SNTP client last updated the system clock.
Last Attempt Time	Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.
Last Attempt Status	Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes: <ul style="list-style-type: none"> <li>• <b>Other:</b> None of the following enumeration values.</li> <li>• <b>Success:</b> The SNTP operation was successful and the system time was updated.</li> <li>• <b>Request Timed Out:</b> A directed SNTP request timed out without receiving a response from the SNTP server.</li> <li>• <b>Bad Date Encoded:</b> The time provided by the SNTP server is not valid.</li> <li>• <b>Version Not Supported:</b> The SNTP version supported by the server is not compatible with the version supported by the client.</li> <li>• <b>Server Unsynchronized:</b> The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message.</li> <li>• <b>Server Kiss Of Death:</b> The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.</li> </ul>
Server IP Address	Specifies the IP address of the server for the last received valid packet. If no message has been received from any server, an empty string is shown.
Address Type	Specifies the address type of the SNTP Server address for the last received valid packet.
Server Stratum	Specifies the claimed stratum of the server for the last received valid packet.
Reference Clock Id	Specifies the reference clock identifier of the server for the last received valid packet.
Server Mode	Specifies the mode of the server for the last received valid packet.
Unicast Sever Max Entries	Specifies the maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	Specifies the number of current valid unicast server entries configured for this client.
Broadcast Count	Specifies the number of unsolicited broadcast SNTP messages that have been received and processed by the SNTP client since last reboot.

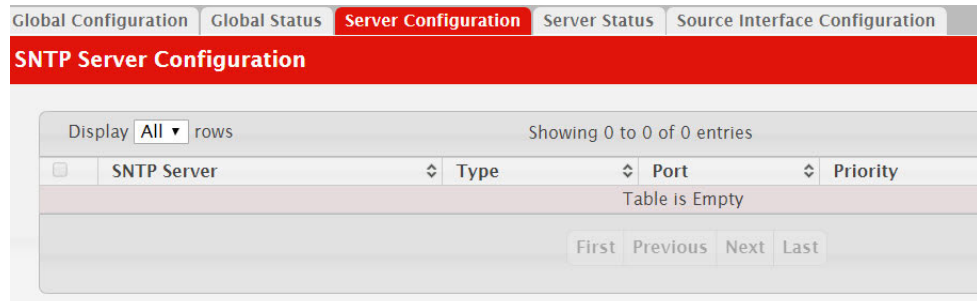
Click **Refresh** to display the latest information from the router.

## SNTP Server Configuration

Use the SNTP Server Configuration page to view and modify information for adding and modifying Simple Network Time Protocol SNTP servers.

To display the SNTP Server Configuration page, click **System > Advanced Configuration > SNTP > Server Configuration** in the navigation menu.

**Figure 136.** SNTP Server Configuration



**Table 129.** SNTP Server Configuration Fields

Field	Description
SNTP Server	Select the IP address of a user-defined SNTP server to view or modify information about an SNTP server, or select <b>Add</b> to configure a new SNTP server. You can define up to three SNTP servers.
Type	Select <b>IPv4</b> if you entered an IPv4 address, <b>IPv6</b> if you entered an IPv6 address or <b>DNS</b> if you entered a hostname.
Port	Enter a port number from 1 to 65535. The default is 123.
Priority	Enter a priority from 1 to 3, with 1 being the highest priority. The switch will attempt to use the highest priority server and, if it is not available, will use the next highest server.
Version	Enter the protocol version number.

- To add an SNTP server, select **Add** from the **Server** list, complete the remaining fields as desired, and click **Submit**. The SNTP server is added, and is now reflected in the Server list. You must perform a save to retain your changes over a power cycle.
- To removing an SNTP server, select the IP address of the server to remove from the **Server** list, and then click **Remove**. The entry is removed, and the device is updated.

## SNTP Server Status

The SNTP Server Status page displays status information about the SNTP servers configured on your switch.

To access the SNTP Server Status page, click **System > Advanced Configuration > SNTP > Server Status** in the navigation menu.

**Figure 137.** SNTP Server Status



**Table 130.** SNTP Server Status Fields

Field	Description
Address	Specifies all the existing Server Addresses. If no Server configuration exists, a message saying <i>No SNTP server exists</i> flashes on the screen.
Last Update Time	Specifies the local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	Specifies the local date and time (UTC) that this SNTP server was last queried.
Last Attempt Status	Specifies the status of the last SNTP request to this server. If no packet has been received from this server, a status of Other is displayed: <ul style="list-style-type: none"> <li>• <b>Other:</b> None of the following enumeration values.</li> <li>• <b>Success:</b> The SNTP operation was successful and the system time was updated.</li> <li>• <b>Request Timed Out:</b> A directed SNTP request timed out without receiving a response from the SNTP server.</li> <li>• <b>Bad Date Encoded:</b> The time provided by the SNTP server is not valid.</li> <li>• <b>Version Not Supported:</b> The SNTP version supported by the server is not compatible with the version supported by the client.</li> <li>• <b>Server Unsynchronized:</b> The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message.</li> <li>• <b>Server Kiss Of Death:</b> The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.</li> </ul>
Requests	Specifies the number of SNTP requests made to this server since last agent reboot.
Failed Requests	Specifies the number of failed SNTP requests made to this server since last reboot.

Click **Refresh** to display the latest information from the switch.

## SNTP Source Interface Configuration

Use this page to specify the physical or logical interface to use as the SNTP client source interface. When an IP address is configured on the source interface, this address is used for all SNTP communications between the local SNTP client and the remote SNTP server. The IP address of the designated source interface is used

in the IP header of SNTP management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device.

To access the SNTP Source Interface Configuration page, click **System > Advanced Configuration > SNTP > Source Interface Configuration** in the navigation menu.

**Figure 138.** SNTP Source Interface Configuration

**Table 131.** SNTP Source Interface Configuration Fields

Field	Description
Type	The type of interface to use as the source interface: <ul style="list-style-type: none"> <li>• <b>None</b> – The primary IP address of the originating (outbound) interface is used as the source address.</li> <li>• <b>Interface</b> – The primary IP address of a physical port is used as the source address.</li> <li>• <b>VLAN</b> – The primary IP address of a VLAN routing interface is used as the source address.</li> <li>• <b>Loopback</b> – The primary IP address of the loopback interface is used as the source address. A loopback is always reachable, as long as any routing interface is up.</li> <li>• <b>Network</b> – The network source IP is used as the source address.</li> <li>• <b>Service Port</b> – The management port source IP is used as the source address.</li> </ul>
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
Loopback Interface	When the selected Type is Loopback, select the loopback interface to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.

Click **Refresh** to display the latest information from the switch.

Click **Submit** to apply the settings to the running configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save Configuration** is performed.

## Configuring the Time Zone

This page displays information about the current system time, the time zone, and the daylight saving time (also known as summer time) settings configured on the device.

To access the Time Zone Summary page, click **System > Advanced Configuration > Time Zone > Summary** in the navigation menu.

**Figure 139.** Time Zone Summary

Current Time	
Time	17:58:02
Zone	(UTC+0:00)
Date	February 07, 2019
Time Source	No time source

Time Zone	
Zone	
Offset	UTC+0:00

Summer Time	
Summer Time	No Summer Time
Zone	
Offset	
Status	

Refresh

**Table 132.** Time Zone Summary Fields

Field	Description
Current Time	<p>This section contains information about the system time and date on the device. If the current time has not been acquired by the SNTP client on the device or configured manually, this section shows the default time and date plus the amount of time since the system was reset.</p> <ul style="list-style-type: none"> <li>• <b>Time</b> — The current time on the system clock. This time is used to provide time stamps on log messages. Additionally, some CLI show commands include the time in the command output.</li> <li>• <b>Zone</b> — The acronym that represents the time zone.</li> <li>• <b>Date</b> — The current date on the system.</li> <li>• <b>Time Source</b> — The time source from which the time update is taken: <ul style="list-style-type: none"> <li>– <b>SNTP</b> — The time has been acquired from an SNTP server.</li> <li>– <b>No Time Source</b> — The time has either been manually configured or not configured at all.</li> </ul> </li> </ul>
Time Zone	<p>This section contains information about the time zone and offset.</p> <p><b>Zone</b> — The acronym that represents the time zone.</p> <p><b>Offset</b> — The number of hours offset from Coordinated Universal Time (UTC), which is also known as Greenwich Mean Time (GMT).</p>



**Table 132.** *Time Zone Summary Fields (continued)*

Field	Description
Summer Time	<p>The administrative status of summer time (daylight saving time). In some regions, the time shifts by one hour in the fall and spring.</p> <p><b>Summer Time</b> — The summer time mode on the system:</p> <ul style="list-style-type: none"> <li>• <b>Disable</b> — Summer time is not active, and the time does not shift based on the time of year.</li> <li>• <b>Recurring</b> — Summer time occurs at the same time every year. The start and end times and dates for the time shift must be manually configured.</li> <li>• <b>EU</b> — The system clock uses the standard recurring summer time settings used in countries in the European Union. When this field is selected, the rest of the applicable fields on the page except Offset and Zone are automatically populated and cannot be edited.</li> <li>• <b>USA</b> — The system clock uses the standard recurring daylight saving time settings used in the United States. When this field is selected, the rest of the applicable fields on the page except Offset and Zone are automatically populated and cannot be edited</li> <li>• <b>Non-Recurring</b> — Summer time settings are in effect only between the start date and end date of the specified year. When this mode is selected, the summer time settings do not repeat on an annual basis.</li> </ul> <p><b>Zone</b> — The acronym that represents the time zone.</p> <p><b>Offset</b> — The number of hours offset from Coordinated Universal Time (UTC), which is also known as Greenwich Mean Time (GMT).</p> <p><b>Status</b> — Indicates if summer time is currently active.</p>

Click **Refresh** to display the latest information from the router.

## Time Zone Configuration

Use this page to manually configure the system clock settings. The SNTP client must be disabled to allow manual configuration of the system time and date.

To access the Time Zone Configuration page, click **System > Advanced Configuration > Time Zone > Time Zone** in the navigation menu.

**Figure 140.** Time Zone Configuration

Summary **Time Zone** Summer Time

### Time Zone Configuration

Time Zone	
Offset	00:00 (-12:00 to 14:00)
Zone	(0 to 4 characters)

Date and Time	
Time	05:58:32 (00:00:00 to 23:59:59)
Date	February 18, 2019

Submit Refresh Cancel

**Table 133.** *Time Zone Configuration Fields*

Field	Description
Time Zone	<p>The time zone settings include the amount of time the system clock is offset from Coordinated Universal Time (UTC) and the time zone acronym.</p> <ul style="list-style-type: none"><li>• <b>Offset</b> — The number of hours the system clock is offset from UTC, which is also known as Greenwich Mean Time (GMT).</li><li>• <b>Zone</b> — The acronym that represents the time zone. This field is not validated against an official list of time zone acronyms.</li></ul>
Date and Time	<p>Use the fields in this section to manually configure the system time and date. If the SNTP client is enabled (Unicast mode or Broadcast mode), these fields cannot be configured.</p> <ul style="list-style-type: none"><li>• <b>Time</b> — The current time in hours, minutes, and seconds on the system clock.</li><li>• <b>Date</b> — The current date in month, day, and year on the system clock. To change the date, click the calendar icon to the right of the field, select the year from the menu, browse to the desired month, and click the date.</li></ul>

Click **Refresh** to display the latest information from the router.

Click **Submit** to apply the settings to the running configuration and cause the change to take effect.

## Summer Time Configuration

Use this page to configure settings for summer time, which is also known as daylight saving time. Used in some countries around the world, summer time is the practice of temporarily advancing clocks during the summer months. Typically clocks are adjusted forward one or more hours near the start of spring and are adjusted backward in autumn.

To access the Summer Time Configuration page, click **System > Advanced Configuration > Time Zone > Summer Time** in the navigation menu.

**Figure 141.** Summer Time Configuration

**Table 134.** Summer Time Configuration Fields

Field	Description
Summer Time	<p>The summer time mode on the system:</p> <ul style="list-style-type: none"> <li>• <b>Disable</b> – Summer time is not active, and the time does not shift based on the time of year.</li> <li>• <b>Recurring</b> – Summer time occurs at the same time every year. The start and end times and dates for the time shift must be manually configured.</li> <li>• <b>EU</b> – The system clock uses the standard recurring summer time settings used in countries in the European Union. When this field is selected, the rest of the applicable fields on the page are automatically populated and cannot be edited.</li> <li>• <b>USA</b> – The system clock uses the standard recurring daylight saving time settings used in the United States. When this field is selected, the rest of the applicable fields on the page are automatically populated and cannot be edited.</li> <li>• <b>Non-Recurring</b> – Summer time settings are in effect only between the start date and end date of the specified year. When this mode is selected, the summer time settings do not repeat on an annual basis.</li> </ul>

**Table 134.** *Summer Time Configuration Fields (continued)*

Field	Description
Date Range	<p>The fields in this section are available only if the Non-Recurring mode is selected from the Summer Time menu.</p> <ul style="list-style-type: none"><li>• <b>Start Date</b> — The day, month, and year that summer time begins. To change the date, click the calendar icon to the right of the field, select the year from the menu, browse to the desired month, and click the date.</li><li>• <b>Starting Time of Day</b> — The time, in hours and minutes, to start summer time on the specified day.</li><li>• <b>End Date</b> — The day, month, and year that summer time ends. To change the date, click the calendar icon to the right of the field, select the year from the menu, browse to the desired month, and click the date.</li><li>• <b>Ending Time of Day</b> — The time, in hours and minutes to end summer time on the specified day.</li></ul>
Recurring Date	<p>The fields in this section are available only if the Recurring mode is selected from the Summer Time menu.</p> <ul style="list-style-type: none"><li>• <b>Start Week</b> — The week of the month within which summer time begins.</li><li>• <b>Start Day</b> — The day of the week on which summer time begins.</li><li>• <b>Start Month</b> — The month of the year within which summer time begins.</li><li>• <b>Starting Time of Day</b> — The time, in hours and minutes, to start summer time.</li><li>• <b>End Week</b> — The week of the month within which summer time ends.</li><li>• <b>End Day</b> — The day of the week on which summer time ends.</li><li>• <b>End Month</b> — The month of the year within which summer time ends.</li><li>• <b>Ending Time of Day</b> — The time, in hours and minutes, to end summer time.</li></ul>
Zone	<p>The fields in this section are available only if the Recurring or Non-Recurring modes are selected from the Summer Time menu.</p> <ul style="list-style-type: none"><li>• <b>Offset</b> — The number of minutes to shift the summer time from the standard time.</li><li>• <b>Zone</b> — The acronym associated with the time zone when summer time is in effect.</li></ul>

Click **Refresh** to display the latest information from the router.

Click **Submit** to apply the settings to the running configuration and cause the change to take effect.

# Configuring and Viewing ISDP Information

The Industry Standard Discovery Protocol (ISDP) is a proprietary Layer 2 network protocol which inter-operates with Cisco devices running the Cisco Discovery Protocol (CDP). ISDP is used to share information between neighboring devices. CE0128XB/CE0152XB software participates in the CDP protocol and is able to both discover and be discovered by other CDP supporting devices.

## Global Configuration

To access the ISDP Global Configuration page, click **System > Advanced Configuration > ISDP > Global** in the navigation menu.

**Figure 142.** ISDP Global Configuration

The following table describes the fields available on the ISDP **Global Configuration** page.

**Table 135.** ISDP Global Configuration

Field	Description
ISDP Mode	Use this field to enable or disable the Industry Standard Discovery Protocol on the switch.
ISDP V2 Mode	Use this field to enable or disable the Industry Standard Discovery Protocol v2 on the switch.
Message Interval	Specifies the ISDP transmit interval. The range is (5–254). Default value is 30 seconds.
Hold Time Interval	The receiving device holds ISDP message during this time period. The range is (10–255). Default value is 180 seconds.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of Device ID Format object.
Device ID Format Capability	Indicates the possible formats that the device can use for identification purposes. <ul style="list-style-type: none"> <li><b>serialNumber</b>—Indicates that the device uses serial number as the format for its Device ID.</li> <li><b>macAddress</b>—Indicates that the device uses layer 2 MAC address as the format for its Device ID.</li> <li><b>other</b>—Indicates that the device uses its platform specific format as the format for its Device ID.</li> </ul>

**Table 135.** ISDP Global Configuration (continued)

Field	Description
Device ID Format	<p>Indicates the current format of the Device ID.</p> <ul style="list-style-type: none"> <li><b>serialNumber</b>— Indicates that the value is in the form of an ASCII string containing the device serial number.</li> <li><b>macAddress</b>— Indicates that the value is in the form of Layer 2 MAC address.</li> <li><b>other</b>— Indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example: ASCII string contains serialNumber appended/prepended with system name.</li> </ul>

## Cache Table

From the ISDP **Cache Table** page, you can view information about other devices the switch has discovered through the ISDP.

To access the ISDP Cache Table page, click **System > Advanced Configuration > ISDP > Cache Table** in the navigation menu.

**Figure 143.** ISDP Cache Table



The following table describes the fields available on the ISDP **Cache Table** page.

**Table 136.** ISDP Cache Table

Field	Description
Device ID	Displays the string with Device ID which is reported in the most recent ISDP message.
Interface	Displays the interface that this neighbor is attached to.
IP Address	The (first) network-layer address that is reported in the Address TLV of the most recently received ISDP message.
Version	Displays the Version string for the neighbor.
Hold Time	Displays the ISDP hold time for the neighbor.
Capability	Displays the ISDP Functional Capabilities for the neighbor.
Platform	Displays the ISDP Hardware Platform for the neighbor.
Port ID	Displays the ISDP port ID string for the neighbor.
Protocol Version	Displays the ISDP Protocol Version for the neighbor.
Last Time Changed	Displays when entry was last modified.

**Table 136.** ISDP Cache Table (continued)

Field	Description
Clear (Button)	Clears all entries from the table. The table is repopulated as ISDP messages are received from neighbors.

## Interface Configuration

From the ISDP **Interface Configuration** page, you can configure the ISDP settings for each interface.

**Note:** If ISDP is enabled on an interface, it must also be enabled globally in order for the interface to transmit ISDP packets. If the ISDP mode on the ISDP **Global Configuration** page is disabled, the interface will not transmit ISDP packets, regardless of the mode configured on the interface.

To access the ISDP Cache Table page, click **System > Advanced Configuration > ISDP > Interface** in the navigation menu.

**Figure 144.** ISDP Interface Configuration

Interface	ISDP Mode
1/0/1	Enable
1/0/2	Enable
1/0/3	Enable
1/0/4	Enable
1/0/5	Enable
1/0/6	Enable
1/0/7	Enable
1/0/8	Enable
1/0/9	Enable
1/0/10	Enable

The following table describes the fields available on the ISDP **Interface Configuration** page.

**Table 137.** ISDP Interface Configuration

Field	Description
Interface	Select the interface with the ISDP mode status to configure or view.
ISDP Mode	Use this field to enable or disable the Industry Standard Discovery Protocol on the selected interface.

## Statistics

From the ISDP **Statistics** page, you can view information about the ISDP packets sent and received by the switch.

To access the ISDP Cache Table page, click **System > Advanced Configuration > ISDP > Statistics** in the navigation menu.

**Figure 145.** ISDP Statistics

ISDP Statistics	
Packets Received	19104
Packets Transmitted	19104
ISDPv1 Packets Received	0
ISDPv1 Packets Transmitted	0
ISDPv2 Packets Received	19104
ISDPv2 Packets Transmitted	19104
Bad Header	0
Checksum Error	0
Transmission Failure	0
Invalid Format Packets Received	0
Table Full	0
ISDP IP Address Table Full	0

Refresh Clear

The following table describes the fields available on the ISDP **Statistics** page.

**Table 138.** ISDP Statistics

Field	Description
ISDP Packets Received	Displays the number of all ISDP protocol data units (PDUs) received.
ISDP Packets Transmitted	Displays the number of all ISDP PDUs transmitted.
ISDPv1 Packets Received	Displays the number of v1 ISDP PDUs received.
ISDPv1 Packets Transmitted	Displays the number of v1 ISDP PDUs transmitted.
ISDPv2 Packets Received	Displays the number of v2 ISDP PDUs received.
ISDPv2 Packets Transmitted	Displays the number of v2 ISDP PDUs transmitted.
ISDP Bad Header	Displays the number of ISDP PDUs that were received with bad headers.
ISDP Checksum Error	Displays the number of ISDP PDUs that were received with checksum errors.
ISDP Transmission Failure	Displays the number of ISDP PDUs transmission failures.
Invalid Format ISDP Packets Received	Displays the number of ISDP PDUs that were received with an invalid format.
Table Full	Displays the number of times the system tried to add an entry to the ISDP table but was unsuccessful because the table was full.



**Table 138.** *ISDP Statistics (continued)*

Field	Description
ISDP IP Address Table Full	Displays the number of times the system tried to add an entry to the ISDP IP Address table but was unsuccessful because the table was full.
Clear (Button)	Resets all statistics to zero.

## Link Dependency

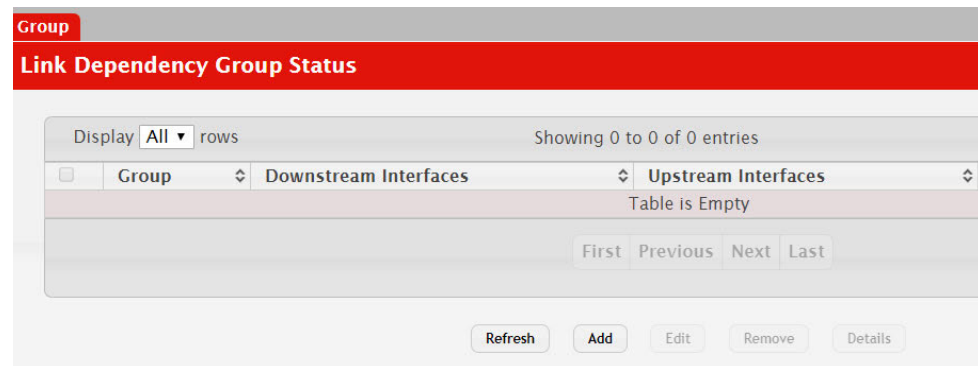
The link dependency feature provides the ability to enable or disable one or more ports based on the link state of one or more different ports. With link dependency enabled on a port, the link state of that port is dependent on the link state of another port. For example, if port A is dependent on port B and the switch detects a link loss on port B, the switch automatically brings down the link on port A. When the link is restored to port B, the switch automatically restores the link to port A.

## Link Dependency Group Status

Use this page to configure link dependency groups. Link dependency allows the link status of one interface to be dependent on the link status of another interface. Link state groups define the interface link dependency.

To access the Link Dependency Group Status page, click **System > Advanced Configuration > Link Dependency > Group** in the navigation menu.

**Figure 146.** Link Dependency Group Status



Use the buttons to perform the following tasks:

- To add a link dependency group, click **Add**. Then, specify a group number, link action, and the interfaces that share a dependency.
- To change the settings for a group, select the check box associated with the group and click **Edit**.
- To delete a link dependency group, select the check box associated with each entry to delete and click **Remove**.
- To view additional information about a group, select the check box associated with the group and click **Details**.

**Table 139.** Link Dependency Group Status

Field	Description
Group	The unique link dependency group identifier.
Downstream Interfaces	The set of interfaces that depend on other interfaces. In other words, the link state of the downstream interfaces depends on the link state of the upstream interfaces.

**Table 139.** *Link Dependency Group Status (continued)*

Field	Description
Upstream Interfaces	The set of interfaces that determine the link state of the downstream interfaces.
Link Action	<p>The action performed on downstream interfaces when the upstream interfaces are down, which can be one of the following:</p> <ul style="list-style-type: none"><li>• <b>Up:</b> Downstream interfaces are up when upstream interfaces are down.</li><li>• <b>Down:</b> Downstream interfaces go down when upstream interfaces are down.</li></ul> <p>Creating a link dependency group with the up link action essentially creates a backup link for the dependent link and alleviates the need to implement STP to handle the fail-over.</p>
State	<p>The group state, which can be one of the following:</p> <ul style="list-style-type: none"><li>• <b>Up:</b> Link action is up, and no upstream interfaces have their link up, or link action is down and there are upstream interfaces that have their link up.</li><li>• <b>Down:</b> Link is down when the above conditions are not true.</li></ul>
Available Interfaces	<p>Available in the Add Group dialog, this field lists the interfaces that can be added to the group. An interface defined as an upstream interface cannot be defined as a downstream interface in the same link state group or in a different group. Similarly, an interface defined as a downstream interface cannot be defined as an upstream interface.</p> <p>To move an interface between the Available Interfaces and Downstream Interfaces or Upstream Interfaces fields, click the interface (or <b>CTRL</b> + click to select multiple interfaces), and then click the appropriate arrow to move the selected interfaces to the desired field.</p>
Link Up	Available in the Group Entry Details dialog, this field lists the upstream and downstream interfaces that currently have their link up.
Link Down	Available in the Group Entry Details dialog, this field lists the upstream and downstream interfaces that currently have their link down.

# Chapter 5. Configuring Switching Information

## Managing VLANs

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You may have many reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

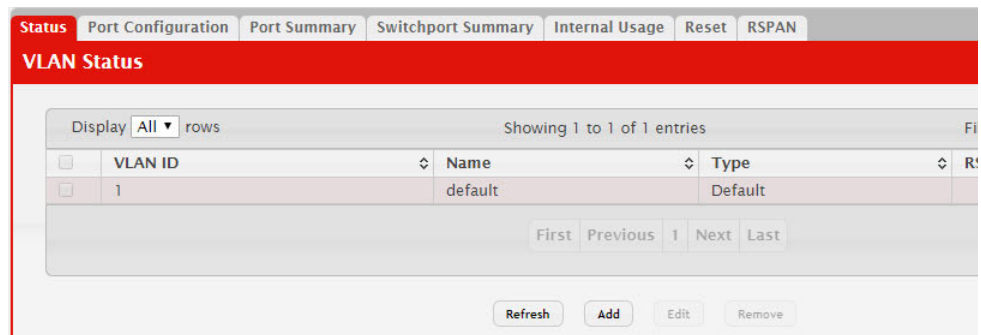
Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

## VLAN Status

Use the VLAN Status page to view information about the VLANs configured on your system, and to configure the statistics collection mode on VLANs.

To access the VLAN Status page, click **Switching > VLAN > Status** in the navigation menu.

**Figure 147.** VLAN Status



**Table 140.** VLAN Status Fields

Field	Description
VLAN ID	The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 4092.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named Default.

**Table 140.** VLAN Status Fields (continued)

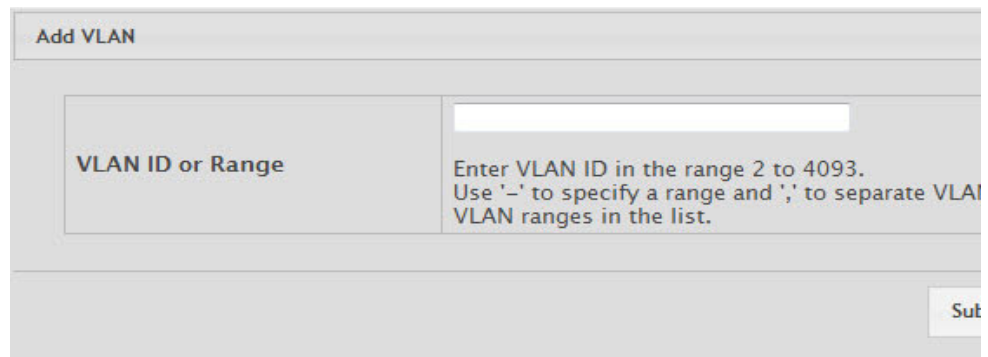
Field	Description
VLAN Type	The VLAN type, which can be one of the following: <ul style="list-style-type: none"><li>• <b>Default:</b> (VLAN ID = 1) -- always present</li><li>• <b>Static:</b> A VLAN you have configured</li><li>• <b>Dynamic:</b> A VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore remove</li></ul>
RSPAN	Lists the status of RSPAN, enabled or disabled.

Click **Refresh** to display the latest information from the router.

## Add a VLAN

To add a VLAN, click the **Add** button and specify a VLAN ID in the available field. For static VLANs, specify a name for the VLAN. This field is optional and is used to help identify the VLAN. This field is not available for other VLAN types.

**Figure 148.** Add VLAN



The screenshot shows a web interface for adding a VLAN. The main heading is "Add VLAN". Below this is a large text input field labeled "VLAN ID or Range". To the right of this field is a smaller text box with the following instructions: "Enter VLAN ID in the range 2 to 4093. Use '-' to specify a range and ';' to separate VLAN ranges in the list." At the bottom right of the form is a "Submit" button.

Click **Submit** to add the VLAN to the system.

## Edit VLAN Configuration

To edit the VLAN Configuration, select the entry to modify and click the **Edit** button.

**Figure 149.** Edit VLAN Configuration

The screenshot shows the 'Edit VLAN Configuration' page in a web GUI. At the top, there are navigation tabs: Status, Port Configuration, Port Summary, Switchport Summary, Internal Usage, Statistics, and Reset. Below the tabs is the 'Edit VLAN Configuration' form. The form contains the following fields:

VLAN ID	3
Name	VLAN0003 (1 to 32 alphanumeric characters)
Type	Static
Convert VLAN Type to Static	<input type="checkbox"/>

At the bottom right of the form, there are two buttons: 'Submit' and 'Cancel'.

Edit the configured VLAN settings, as follows.

**Table 141.** Edit VLAN Configuration

Field	Description
Name	For static VLANs, specify a name for the VLAN. The name can be 1 to 32 alphanumeric characters. This field is optional and is used to help identify the VLAN. This field is not available for other VLAN types.
Convert VLAN Type to Static	For dynamic VLANs, select this option to convert the dynamic VLAN to a static VLAN. This option is not available for other VLAN types. A dynamic VLAN is learned by using GVRP, which is an industry-standard protocol that propagates VLAN information from one network device to another. GVRP can also remove dynamic VLANs. If you convert a dynamic VLAN to a static VLAN, it cannot be removed by GVRP.

Click **Submit** to submit the VLAN configuration changes. Click **Cancel** to cancel the changes.

## Remove VLAN Configuration

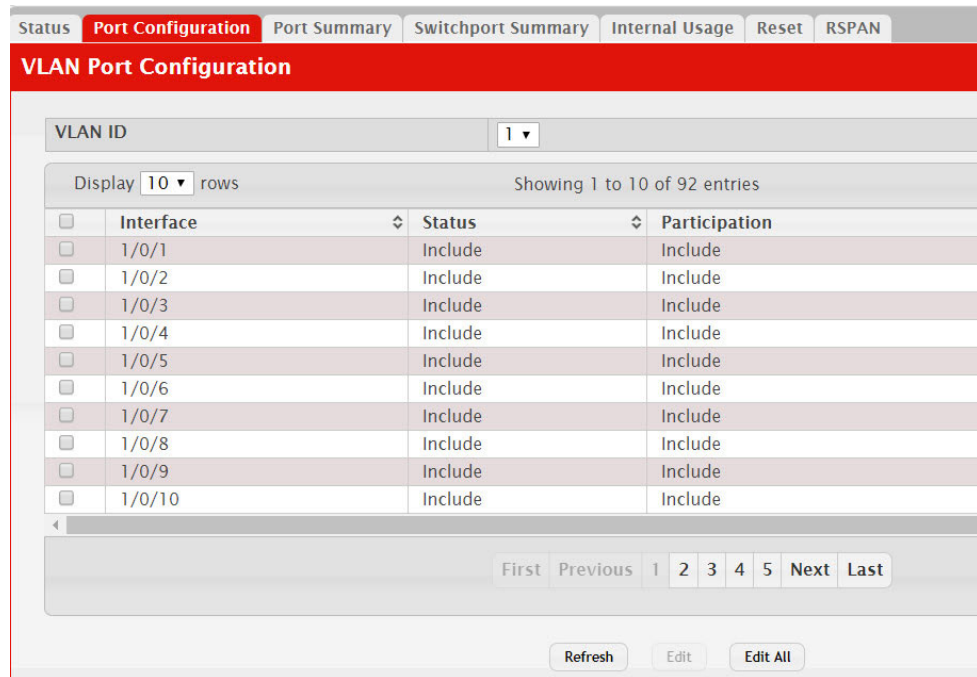
To remove one or more configured VLANs, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

## VLAN Port Configuration

Use the VLAN Port Configuration page to configure a virtual LAN on a port.

To access the VLAN Port Configuration page, click **Switching > VLAN > Port Configuration** in the navigation menu.

**Figure 150.** VLAN Port Configuration



**Table 142.** VLAN Port Configuration Fields

Field	Description
VLAN ID	The menu includes the VLAN ID for all VLANs configured on the device. To view or configure settings for a VLAN, be sure to select the correct VLAN from the menu.
Interface	Select the interface for which you want to display or configure data. Select <b>All</b> to set the parameters for all ports to same values.
Status	The current participation mode of the interface in the selected VLAN. The value of the Status field differs from the value of the Participation field only when the Participation mode is set to Auto Detect. The Status is one of the following: <ul style="list-style-type: none"> <li>• <b>Include</b> – The port is a member of the selected VLAN.</li> <li>• <b>Exclude</b> – The port is not a member of the selected VLAN.</li> </ul>
Participation	The participation mode of the interface in the selected VLAN, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Include</b> – The port is always a member of the selected VLAN. This mode is equivalent to registration fixed in the IEEE 802.1Q standard.</li> <li>• <b>Exclude</b> – The port is never a member of the selected VLAN. This mode is equivalent to registration forbidden in the IEEE 802.1Q standard.</li> <li>• <b>Auto Detect</b> – The port can be dynamically registered in the selected VLAN through GVRP. The port will not participate in this VLAN unless it receives a GVRP request. This mode is equivalent to registration normal in the IEEE 802.1Q standard.</li> </ul>

**Table 142.** VLAN Port Configuration Fields (continued)

Field	Description
Tagging	The tagging behavior for all the ports in this VLAN, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Tagged</b> – The frames transmitted in this VLAN will include a VLAN ID tag in the Ethernet header.</li> <li>• <b>Untagged</b> – The frames transmitted in this VLAN will be untagged.</li> </ul>

Use the buttons to perform the following tasks:

- To configure settings for one or more interfaces, select each interface to configure and click **Edit**. The same settings are applied to all selected interfaces.
- To apply the same settings to all interfaces, click **Edit All** and configure the desired settings.
- To reload the page and view the most current information, click **Refresh**.

## VLAN Port Summary

Use the VLAN Port Summary page to view VLAN configuration information for all the ports on the system.

To access the VLAN Port Summary page, click **Switching > VLAN > Port Summary** in the navigation menu.

**Figure 151.** VLAN Port Summary

Interface	Port VLAN ID	Port VLAN ID Current	Acceptable Frame Type	Ingress Filtering	Untagged VLANs	Tagged VLANs	Forbid VLANs
1/0/1	1	1	Admit All	Disabled	1		
1/0/2	1	1	Admit All	Disabled	1		
1/0/3	1	1	Admit All	Disabled	1		
1/0/4	1	1	Admit All	Disabled	1		
1/0/5	1	1	Admit All	Disabled	1		
1/0/6	1	1	Admit All	Disabled	1		
1/0/7	1	1	Admit All	Disabled	1		
1/0/8	1	1	Admit All	Disabled	1		
1/0/9	1	1	Admit All	Disabled	1		
1/0/10	1	1	Admit All	Disabled	1		

**Table 143.** VLAN Port Summary Fields

Field	Description
Interface	Identifies the physical interface associated with the rest of the data in the row.



**Table 143.** *VLAN Port Summary Fields (continued)*

Field	Description
Port VLAN ID	The VLAN ID assigned to untagged or priority tagged frames received on this port. This value is also known as the Port VLAN ID (PVID). In a tagged frame, the VLAN is identified by the VLAN ID in the tag.
Port VLAN ID Current	The current VLAN ID assigned to packets received on this port. This value may differ from the configured VLAN, for example, when access to the port is managed by a Radius server in an 802.1x configuration.
Acceptable Frame Types	Indicates how the interface handles untagged and priority tagged frames. The options include the following: <ul style="list-style-type: none"> <li>• <b>Admit All</b> – Untagged and priority tagged frames received on the interface are accepted and assigned the value of the Port VLAN ID for this interface.</li> <li>• <b>Only Tagged</b> – The interface discards any untagged or priority tagged frames it receives.</li> <li>• <b>Only Untagged</b> – The interface discards any tagged frames it receives.</li> </ul> For all options, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard.
Ingress Filtering	Shows how the port handles tagged frames. <ul style="list-style-type: none"> <li>• <b>Enable:</b> A tagged frame is discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag.</li> <li>• <b>Disable:</b> All tagged frames are accepted, which is the factory default.</li> </ul>
Untagged VLANs	VLANs that are configured on the port to transmit egress packets as untagged.
Tagged VLANs	VLANs that are configured on the port to transmit egress packets as tagged.
Forbidden VLANs	When configuring port memberships in VLANs, you can specify one or more VLANs to be excluded from the available VLANs for the port. The forbidden VLANs list shows the VLANs to which the port cannot be assigned membership.
Dynamic VLANs	The list of VLANs of which the port became a member as result of the operations of dynamic VLAN protocols. When a VLAN is created as a dynamic VLAN, any port that is configured as switchport type Trunk or General automatically becomes a member of the VLAN, unless the VLAN port is excluded from the VLAN.
Priority	Identifies the default 802.1p priority assigned to untagged packets arriving at the port.

Use the buttons to perform the following tasks:

- To configure settings for one or more interfaces, select each interface to configure and click **Edit**. The same settings are applied to all selected interfaces.
- To apply the same settings to all interfaces, click **Edit All** and configure the desired settings.
- To reload the page and view the most current information, click **Refresh**.

## Switchport Summary

Use the Switchport Summary page to configure switchport mode settings on interfaces. The switchport mode defines the purpose of the port based on the type of device it connects to and constraints the VLAN configuration of the port accordingly. Assigning the appropriate switchport mode helps simplify VLAN configuration and minimize errors.

To access the Switchport Summary page, click **Switching > VLAN > Switchport Summary** in the navigation menu.

**Figure 152.** VLAN Switchport Summary

Interface	Switchport Mode	Access VLAN ID	Native VLAN ID	Native VLAN Tagging
1/0/1	General	1	1	Disabled
1/0/2	General	1	1	Disabled
1/0/3	General	1	1	Disabled
1/0/4	General	1	1	Disabled
1/0/5	General	1	1	Disabled
1/0/6	General	1	1	Disabled
1/0/7	General	1	1	Disabled
1/0/8	General	1	1	Disabled
1/0/9	General	1	1	Disabled
1/0/10	General	1	1	Disabled

**Table 144.** VLAN Switchport Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When editing information for one or more interfaces, this field identifies the interfaces that are being configured.
Switchport Mode	The switchport mode of the interface, which is one of the following: <ul style="list-style-type: none"> <li><b>Access</b>—Access mode is suitable for ports connected to end stations or end users. Access ports participate only in one VLAN. They accept both tagged and untagged packets, but always transmit untagged packets.</li> <li><b>Trunk</b>—Trunk mode is intended for ports that are connected to other switches. Trunk ports can participate in multiple VLANs and accept both tagged and untagged packets.</li> <li><b>General</b>—General mode enables a custom configuration of a port. The user configures the General port VLAN attributes such as membership, PVID, tagging, ingress filter, etc., using the settings on the Port Configuration page. By default, all ports are initially configured in General mode.</li> </ul>
Access VLAN ID	The access VLAN for the port, which is valid only when the port switchport mode is Access.

**Table 144.** VLAN Switchport Summary Fields (continued)

Field	Description
Native VLAN ID	The native VLAN for the port, which is valid only when the port switchport mode is Trunk.
Native VLAN Tagging	When enabled, if the trunk port receives untagged frames, it forwards them on the native VLAN with no VLAN tag. When disabled, if the port receives untagged frames, it includes the native VLAN ID in the VLAN tag when forwarding.
Trunk Allowed VLANs	The set of VLANs of which the port can be a member, when configured in Trunk mode. By default, this list contains all possible VLANs even if they have not yet been created.

Use the buttons to perform the following tasks:

- To configure settings for one or more interfaces, select each interface to configure and click **Edit**. The same settings are applied to all selected interfaces.
- To apply the same settings to all interfaces, click **Edit All** and configure the desired settings.
- To reload the page and view the most current information, click **Refresh**.

## VLAN Internal Usage

Use the VLAN Internal Usage Configuration page to assign a Base VLAN ID for internal allocation of VLANs to the routing interface.

To access the VLAN Internal Usage page, click **Switching > VLAN > Internal Usage** in the navigation menu.

**Figure 153.** VLAN Internal Usage Configuration

**Table 145.** VLAN Internal Usage Configuration Fields

Field	Description
Base VLAN ID	The first VLAN ID to be assigned to a port-based routing interface.
Allocation Policy	Determines whether VLAN IDs assigned to port-based routing interfaces start at the base and decrease in value (Descending) or start at the base and increase in value (Ascending).

**Table 145.** *VLAN Internal Usage Configuration Fields (continued)*

Field	Description
VLAN ID	The VLAN ID assigned to a port-based routing interface. The device automatically assigns an unused VLAN ID when the routing interface is created.
Routing Interface	The port-based routing interface associated with the VLAN.

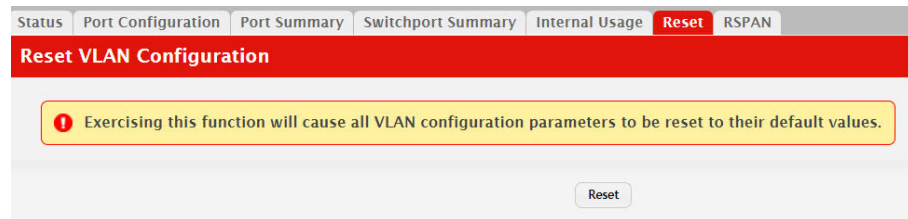
If you change any information on the page, click **Submit** to apply the changes to the system.

## Reset VLAN Configuration

Use the Reset Configuration page to return all VLAN parameters for all interfaces to the factory default values.

To access the Reset Configuration page, click **Switching > VLAN > Reset** in the navigation menu.

**Figure 154.** Reset VLAN Configuration



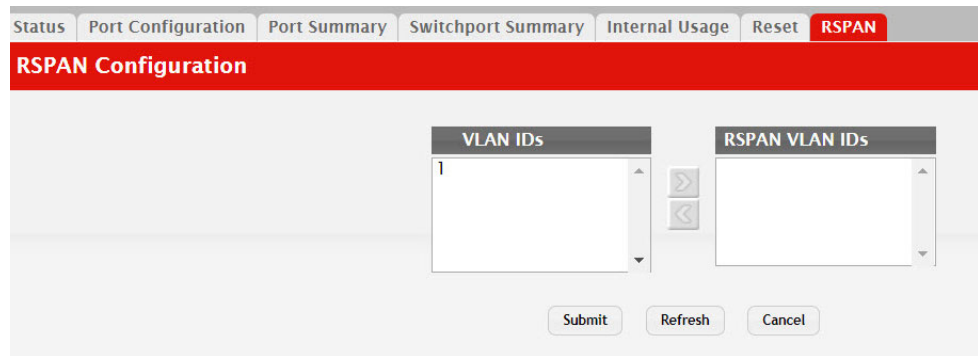
When you click **Reset**, the screen refreshes, and you are asked to confirm the reset. Click **Reset** again to restore all default VLAN settings for the ports on the system.

## RSPAN Configuration

Use this page to configure the VLAN to use as the Remote Switched Port Analyzer (RSPAN) VLAN. RSPAN allows you to mirror traffic from multiple source ports (or from all ports that are members of a VLAN) from different network devices and send the mirrored traffic to a destination port (a probe port connected to a network analyzer) on a remote device. The mirrored traffic is tagged with the RSPAN VLAN ID and transmitted over trunk ports in the RSPAN VLAN.

To access the RSPAN page, click **Switching > VLAN > RSPAN** in the navigation menu.

**Figure 155.** RSPAN VLAN Configuration



**Table 146.** RSPAN VLAN Configuration Fields

Field	Description
VLAN IDs	The VLANs configured on the system that are not currently enabled as Private VLANs. To enable a VLAN as a RSPAN VLAN, click the VLAN ID to select it (or <b>CTRL</b> + click to select multiple VLAN IDs). Then, click the appropriate arrow to move the selected VLAN or VLANs to the RSPAN VLAN IDs window.
RSPAN VLAN IDs	The VLANs that are enabled as RSPAN VLAN. To disable a VLAN as a RSPAN VLAN, click the VLAN ID to select it (or <b>CTRL</b> + click to select multiple VLAN IDs). Then, click the appropriate arrow to move the selected VLAN or VLANs to the VLAN IDs window.

Click **Refresh** to display the latest information from the router.

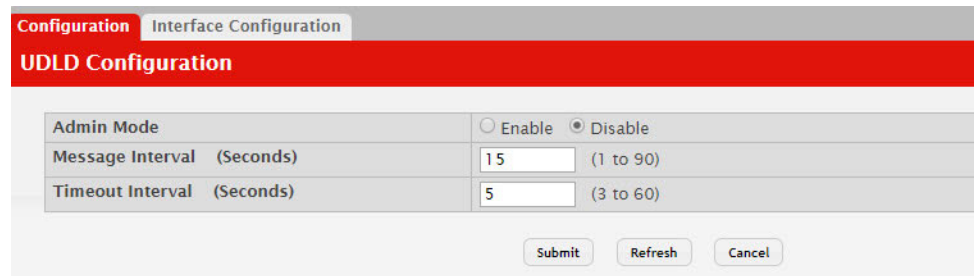
If you change any information on the page, click **Submit** to apply the changes to the system.

## Configuring UDLD

The UDLD feature detects unidirectional links on physical ports by exchanging packets containing information about neighboring devices. The purpose of the UDLD feature is to detect and avoid unidirectional links. A unidirectional link is a forwarding anomaly in a Layer 2 communication channel in which a bidirectional link stops passing traffic in one direction.

To access the UDLD Configuration page, click **Switching > UDLD > Configuration** in the navigation menu.

**Figure 156.** UDLD Configuration



**Table 147.** UDLD Configuration Fields

Field	Description
Admin Mode	The administrative mode of UDLD on the device. UDLD must be administratively enabled on the device and on an interface for that interface to send UDLD messages. Additionally, UDLD must be enabled on the both sides of the link for the device to detect a unidirectional link.
Message Interval (Seconds)	The amount of time to wait between sending UDLD probe messages on ports that are in the advertisement phase.
Timeout Interval (Seconds)	The amount of time to wait to receive a UDLD message before considering the UDLD link to be unidirectional.

Click **Refresh** to display the latest information from the router.

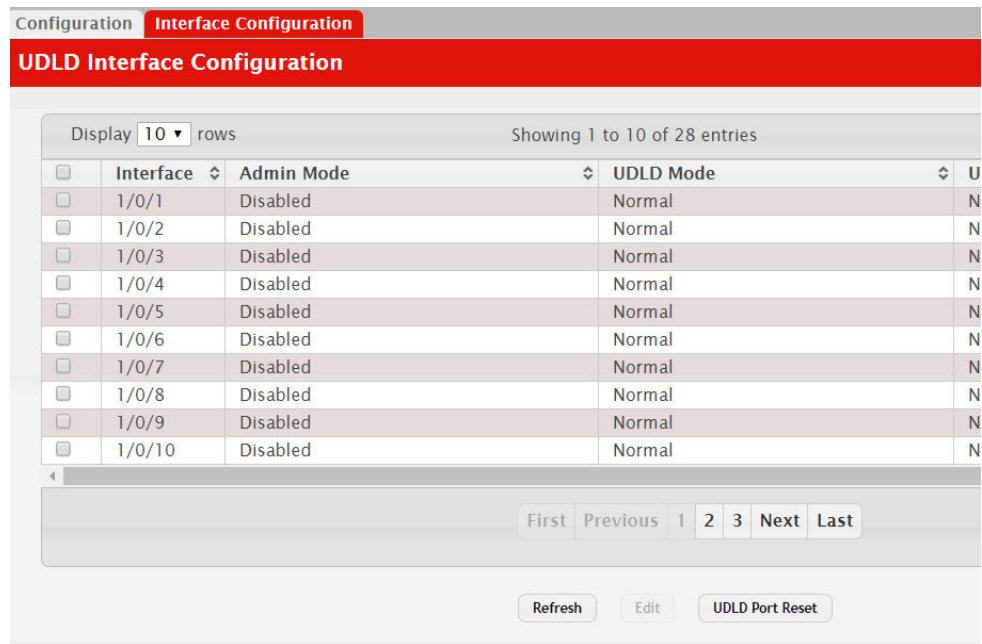
If you change any information on the page, click **Submit** to apply the changes to the system.

## UDLD Interface Configuration

Use this page to configure the per-port UDLD settings.

To access the UDLD Interface Configuration page, click **Switching > UDLD > Interface Configuration** in the navigation menu.

**Figure 157.** UDLD Interface Configuration



Use the buttons to perform the following tasks:

- To configure UDLD settings for one or more interfaces, select each interface to configure and click **Edit**. The same settings are applied to all selected interfaces.
- To reset all UDLD ports that have a UDLD Status of Shutdown, click **UDLD Port Reset**. If the global and interface UDLD administrative mode is enabled and the port link is up, the port restarts the exchange of UDLD messages with its link partner. The UDLD port status is Shutdown if UDLD has detected an unidirectional link and has put the port in a disabled state.

**Table 148.** UDLD Interface Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. In the Edit UDLD Interface Configuration window, this field identifies each interface that is being configured.
Admin Mode	The administrative mode of UDLD on the port.

**Table 148.** UDLD Interface Configuration Fields (continued)

Field	Description
UDLD Mode	<p>The UDLD mode for the port, which is one of the following:</p> <ul style="list-style-type: none"><li>• <b>Normal</b> – The state of the port is classified as Undetermined if an anomaly exists. An anomaly might be the absence of its own information in received UDLD messages or the failure to receive UDLD messages. An Undetermined state has no effect on the operation of the port. The port is not disabled and continues operating. When operating in UDLD normal mode, a port will be put into a disabled (Shutdown) state only in the following situations:<ul style="list-style-type: none"><li>– The UDLD PDU received from a partner does not have its own details (echo).</li><li>– When there is a loopback, and information sent out on a port is received back exactly as it was sent.</li></ul></li><li>• <b>Aggressive</b> – The port is put into a disabled state for the same reasons that it occurs in normal mode. Additionally, a port in UDLD aggressive mode can be disabled if the port does not receive any UDLD echo packets even after bidirectional connection was established. If a bidirectional link is established, and packets suddenly stop coming from partner device, the UDLD aggressive-mode port assumes that link has become unidirectional.</li></ul>
UDLD Status	<p>The UDLD status on the port, which is one of the following:</p> <ul style="list-style-type: none"><li>• <b>Not Applicable</b> – The administrative status of UDLD is globally disabled or disabled on the interface.</li><li>• <b>Bidirectional</b> – UDLD has detected a bidirectional link.</li><li>• <b>Shutdown</b> – UDLD has detected a unidirectional link, and the port is in a disabled state. To clear the disabled state, click UDLD Port Reset.</li><li>• <b>Undetermined</b> – UDLD has not collected enough information to determine the state of the port.</li><li>• <b>Unknown</b> – The port link has physically gone down, but it is not because it was put in a disabled state by the UDLD feature.</li></ul>

Click **Refresh** to display the latest information from the router.

If you change any information on the page, click **Submit** to apply the changes to the system.



## MAC Based VLAN Status

Use this page to add, edit, or remove MAC-based VLANs. MAC-based VLANs allow incoming untagged packets to be assigned to a VLAN based on the source MAC address of the packet. This type of VLAN is useful when a host might not always connect to the network through the same port but needs to be on the same VLAN.

To access the MAC Based VLAN Status page, click **Switching > MAC Based VLAN > Status** in the navigation menu.

**Figure 158.** MAC Based VLAN Status

The screenshot shows the 'MAC Based VLAN Status' page. At the top, there is a red header with the text 'Status' and 'MAC Based VLAN Status'. Below the header, there is a table with two columns: 'MAC Address' and 'VLAN ID'. The table is currently empty, with the text 'Table is Empty' centered in the table area. Above the table, there is a 'Display All rows' dropdown menu and the text 'Showing 0 to 0 of 0 entries'. Below the table, there are four navigation buttons: 'First', 'Previous', 'Next', and 'Last'. At the bottom of the page, there are four buttons: 'Refresh', 'Add', 'Edit', and 'Remove'.

Use the buttons to perform the following tasks:

- To add a MAC-based VLAN, click **Add** and specify a MAC address and a VLAN ID in the available fields.
- To change the VLAN ID of a configured MAC-based VLAN, select the entry to modify and click **Edit**. Then, configure the desired VLAN ID.
- To remove one or more configured MAC-based VLANs, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 149.** *MAC Based VLAN Status Fields*

Field	Description
MAC Address	The source MAC address of the host. All untagged traffic that includes this address in the source MAC address field of the Ethernet frame is placed in the associated VLAN.
VLAN ID	The VLAN ID of the MAC-based VLAN. If an untagged frame received on any port or LAG matches the associated MAC address, it is tagged with this VLAN ID.

Click **Refresh** to display the latest information from the router.

## Double VLAN (DVLAN) Tunneling

DVLAN Tunneling allows the use of a second tag on network traffic. The additional tag helps differentiate between customers in the Metropolitan Area Networks (MAN) while preserving individual customer's VLAN identification when they enter their own 802.1Q domain.

With the introduction of this second tag, you do not need to divide the 4k VLAN ID space to send traffic on an Ethernet-based MAN.

With DVLAN Tunneling enabled, every frame that is transmitted from an interface has a new VLAN tag (S-tag) attached while every packet that is received from an interface has a VLAN tag (S-tag) removed (if one or more tags are present).

DVLAN also supports up to 4 Tag Protocol Identifier (TPID) values per switch and the ability to map these values to ports. This allows you to configure the same or different TPIDs for different ports. Use the DVLAN Tunneling page to configure DVLAN frame tagging on one or more ports.

## DVLAN Configuration

The DVLAN **Config** page allows you to configure the TPID with an associated Global EtherType for all ports on the system.

To access the DVLAN **Configuration** page, click **Switching > DVLAN > Configuration** in the navigation menu.

**Figure 159.** DVLAN Configuration

The screenshot shows the DVLAN Configuration page. At the top, there are three tabs: 'Configuration' (selected), 'Summary', and 'Interface Summary'. Below the tabs is a red header with the text 'DVLAN Configuration'. Underneath, there is a 'Primary TPID' field with a text input containing '0x8100' and an edit icon. Below that is a 'Secondary TPIDs' table with a dropdown arrow, plus and minus icons, and the text 'Table is Empty'. At the bottom right is a 'Refresh' button.

**Table 150.** DVLAN Configuration Fields

Field	Description
Primary TPID	The two-byte hex EtherType value to be used as the first 16 bits of the DVLAN tag. The value configured in this field is used as the primary TPID for all interfaces that are enabled for DVLAN tagging. The Primary TPID can be one of the following: <ul style="list-style-type: none"><li>• <b>0x8100</b> – IEEE 802.1Q customer VLAN tag type</li></ul> To change the Primary TPID, click the Edit icon and select an option from the menu.

**Table 150.** *DVLAN Configuration Fields (continued)*

Field	Description
Secondary TPIDs	<p>The two-byte hex EtherType values available to be configured as secondary TPIDs. Only the options you configure as Secondary TPIDs can be selected as the Primary TPID. To add Secondary TPIDs to the list, click the + (plus) symbol and select one or more of the following options:</p> <ul style="list-style-type: none"> <li>• <b>802.1Q Tag</b> – IEEE 802.1Q customer VLAN tag type, represented by the EtherType value 0x8100. This value indicates that the frame includes a VLAN tag. If this value is already configured as a primary or secondary TPID, it cannot be selected.</li> <li>• <b>vMAN Tag</b> – Virtual Metropolitan Area Network (VMAN) tag type, represented by the EtherType value 0x88a8. This value indicates that the frame is DVLAN tagged. If this value is already configured as a primary or secondary TPID, it cannot be selected.</li> <li>• <b>Custom Tag</b> – User-defined EtherType value. If you select this option, specify the EtherType value in the available field.</li> </ul> <p>To remove a TPID from the list, click the – (minus) symbol associated with the entry. To remove all TPID entries from the list, select the – (minus) symbol in the header row and confirm the action.</p>

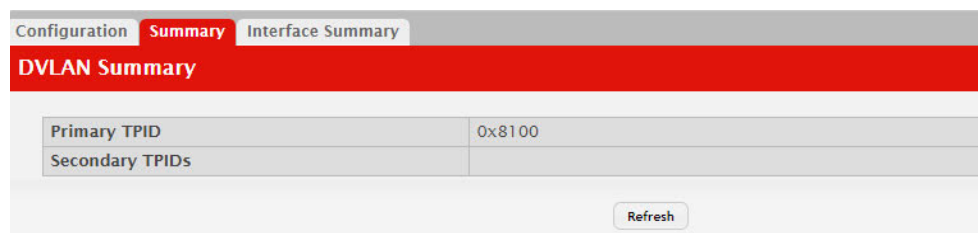
If you make any changes to the page, click **Submit** to apply the changes to the system.

## DVLAN Summary

The DVLAN **Summary** page allows you to view the Global and Default TPIDs configured for all ports on the system.

To access the DVLAN **Summary** page, click **Switching > DVLAN > Summary** in the navigation menu.

**Figure 160.** DVLAN Summary



**Table 151.** *DVLAN Summary Fields*

Field	Description
Primary TPIDs	The two-byte hex EtherType value used as the first 16 bits of the DVLAN tag. This value identifies the frame as one of the following types: <ul style="list-style-type: none"><li>• <b>0x8100</b> – IEEE 802.1Q VLAN tag type. This value indicates that the frame includes a VLAN tag.</li><li>• <b>0x88a8</b> – Virtual Metropolitan Area Network (VMAN) tag type. This value indicates that the frame is double VLAN tagged.</li><li>• <b>Custom Tag</b> – Any TPID value other than 0x8100 or 0x88a8 is a user-defined EtherType value.</li></ul>
Secondary TPID	The two-byte hex EtherType values configured as secondary TPIDs.

Click **Refresh** to display the latest information from the router.

## DVLAN Interface Summary

Use this page to view and configure the double VLAN (DVLAN) tag settings for each interface. Double VLAN tagging allows service providers to create Virtual Metropolitan Area Networks (VMANs). With DVLAN tagging, service providers can pass VLAN traffic from one customer domain to another through a metro core. By using an additional tag on the traffic, the interface can differentiate between customers in the MAN while preserving an individual customer's VLAN identification that is used when the traffic enters the customer's 802.1Q domain.

To access the **DVLAN Interface Summary** page, click **Switching > DVLAN > Interface Summary** in the navigation menu.

To configure the DVLAN settings for an interface, select the interface to configure and click **Edit**.

**Figure 161.** DVLAN Interface Summary

Interface	Interface Mode	Interface EtherType
1/0/1	Disable	0x8100
1/0/2	Disable	0x8100
1/0/3	Disable	0x8100
1/0/4	Disable	0x8100
1/0/5	Disable	0x8100
1/0/6	Disable	0x8100
1/0/7	Disable	0x8100
1/0/8	Disable	0x8100
1/0/9	Disable	0x8100
1/0/10	Disable	0x8100

**Table 152.** DVLAN Interface Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
Interface Mode	The administrative mode of double VLAN tagging on the interface. When DVLAN tagging is enabled, every frame that is transmitted from the interface has a DVLAN tag attached, and every packet that is received from the interface has a tag removed (if one or more tags are present).
Interface EtherType	The EtherType value to be used as the first 16 bits of the DVLAN tag. If one or more secondary TPIDs have been configured for the interface, these EtherType values are also displayed.
EtherType (Primary TPID)	The EtherType value to be used as the first 16 bits of the DVLAN tag. This is a global value that is configured on the DVLAN Configuration page.
Secondary TPIDs	The EtherType value(s) available to be configured as secondary TPIDs. To add a secondary TPID, the DVLAN Interface Mode must first be enabled. Then, select the entry in the Secondary TPIDs field and click the right arrow button. The entry moves into the Configured TPIDs field.
Configured TPIDs	The EtherType value(s) configured as secondary TPIDs. To remove a configured secondary TPID, enable the DVLAN Interface Mode, select the entry to remove from the Configured TPIDs field and click the left arrow button. The entry returns to the Secondary TPIDs field.

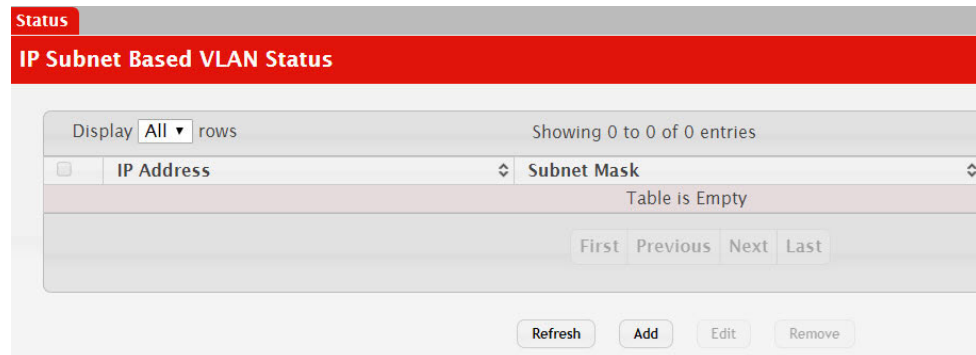
Click **Refresh** to redisplay the most current information from the router.

## IP Subnet Based VLAN

Use this page to add, edit, and remove IP subnet-based VLANs. IP subnet-based VLANs allow incoming untagged packets to be assigned to a VLAN based on the source IP address of the packet. All hosts in the same subnet are members of the same VLAN.

To display the IP Subnet Based VLAN Status page, click **Switching > IP Subnet Based VLAN > Status**.

**Figure 162.** IP Subnet Based VLAN Status



Use the buttons to perform the following tasks:

- To add an IP subnet-based VLAN, click **Add** and specify an IP address, subnet mask, and VLAN ID in the available fields.
- To change the VLAN ID of a configured IP subnet-based VLAN, select the entry to modify and click **Edit**. Then, configure the desired VLAN ID.
- To remove one or more configured IP subnet-based VLANs, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 153.** IP Subnet Based VLAN Status Fields

Field	Description
IP Address	The network address for the IP subnet. All incoming untagged packets that have a source IP address within the defined subnet-network are placed in the same VLAN.
Subnet Mask	The subnet mask that defines the network portion of the IP address.
VLAN ID	The VLAN ID of the IP subnet-based VLAN. If the source IP address of untagged traffic received on any port or LAG is within the associated IP subnet, the traffic is tagged with this VLAN ID.

Click **Refresh** to redisplay the most current information from the router.

# Protocol Based VLAN Configuration

This page is divided into two sections:

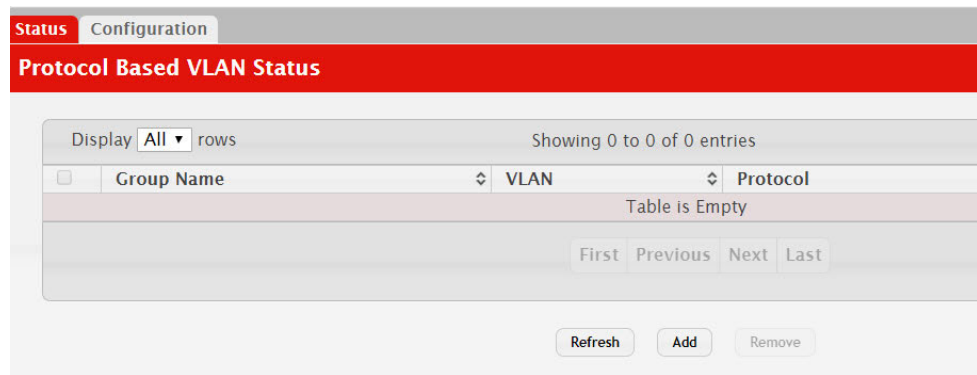
- Status
- Configuration

## Status

Use this page to add and remove Protocol-based Virtual Local Area Networks (PBVLANS). In a PBVLAN, traffic is bridged through specified ports based on the protocol. PBVLANS allow you to define a packet filter that the device uses as the matching criteria to determine whether a particular packet belongs to a particular VLAN. PBVLANS are most often used in environments where network segments contain hosts running multiple protocols. PBVLANS can help optimize network traffic patterns because protocol-specific broadcast messages are sent only to hosts that use the protocols specified in the PBVLAN.

To display the Protocol Based VLAN Status page, click **Switching > Protocol Based VLAN > Status**.

**Figure 163.** Protocol Based VLAN Status



## Adding a PBVLAN

1. To add a PBVLAN, click **Add** and specify a group name, VLAN ID, protocol, and interfaces in the available fields.
2. To remove one or more configured PBVLANS, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 154.** Protocol Based VLAN Status Fields

Field	Description
Group Name	The user-configured name that identifies the PBVLAN group.

**Table 154.** Protocol Based VLAN Status Fields (continued)

Field	Description
VLAN	<p>The VLAN ID associated with the PBVLAN. VLAN tagging for the PBVLAN works as follows:</p> <ul style="list-style-type: none"> <li>• If the frame received over a port is tagged, normal processing takes place.</li> <li>• If the frame received over a port is untagged, the frame type is matched according to the protocol(s) assigned to the group on that port. <ul style="list-style-type: none"> <li>– If a match is found, the frame is assigned the VLAN ID specified for the group.</li> <li>– If a match is not found, the frame is assigned the port VID (PVID) as its VLAN ID.</li> </ul> </li> </ul>
Protocol	<p>The protocol or protocols to use as the match criteria for an Ethernet frame. The protocol is included in the two-byte EtherType field of the frame. When adding a PVBLAN, you can specify the EtherType hex value or (for IP, ARP, and IPX) the protocol keyword.</p>
Interface	<p>The interfaces that are members of the PBVLAN group. An interface can be a member of multiple groups as long as the same protocol is not specified in more than one group that includes the interface. When adding a PBVLAN group, use the Available Interfaces and Group Interfaces fields to configure the interfaces that are members of the PBVLAN group. To move an interface between the Available Interfaces and Group Interfaces fields, click the interface (or <b>CTRL</b> + click to select multiple interfaces), and then click the appropriate arrow to move the selected interfaces to the desired field.</p>

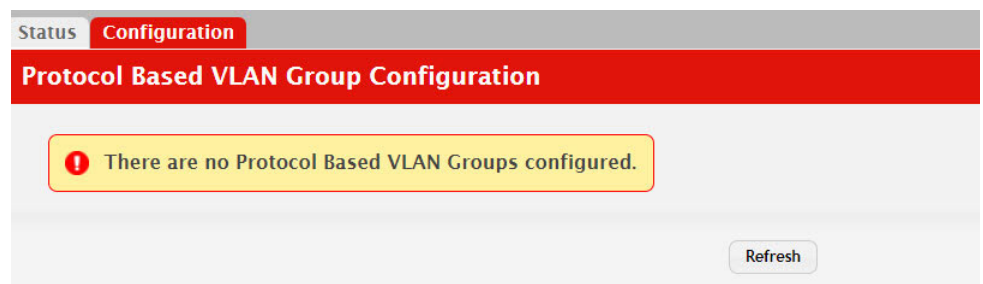
- Click **Refresh** to display the latest information from the router.

## Configuration

Use this page to configure existing Protocol-based VLAN (PBVLAN) groups. You can change the group name, VLAN ID, protocol information, and interfaces associated with the PBVLAN group.

To display the Protocol Based VLAN Status page, click **Switching > Protocol Based VLAN > Configuration**.

**Figure 164.** Protocol Based VLAN Configuration





**Table 155.** *Protocol Based VLAN Configuration Fields*

Field	Description
Group Name	To change the properties of a PBVLAN, select its name from the Group Name menu. The Group Name field allows you to update the name of the PBVLAN group.
VLAN	The VLAN ID associated with the PBVLAN. Untagged traffic that matches the protocol criteria is tagged with this VLAN ID.
Protocol	<p>The protocol or protocols to use as the match criteria to determine whether a particular packet belongs to the PBVLAN. The protocols in this list are checked against the two-byte EtherType field of ingress Ethernet frames on the PBVLAN Group Interfaces. When adding a protocol, you can specify the EtherType hex value or (for IP, ARP, and IPX) the protocol keyword.</p> <p>To configure the protocols associated with a PBVLAN group, use the buttons available in the protocol table:</p> <ul style="list-style-type: none"><li>• To add a protocol to the group, click the + (plus) button and enter the protocol to add.</li><li>• To delete an entry from the list, click the – (minus) button associated with the entry to remove.</li><li>• To delete all entries from the list, click the – (minus) button in the heading row.</li></ul>
Available Interfaces	The interfaces that can be added to the PBVLAN group. An interface can be a member of multiple groups as long as the same protocol is not specified in more than one group that includes the interface. To move an interface between the Available Interfaces and Group Interfaces fields, click the interface (or <b>CTRL</b> + click to select multiple interfaces), and then click the appropriate arrow to move the selected interfaces to the desired field.
Group Interfaces	The interfaces that are members of the PBVLAN group.

- If you make any changes, click **Submit** to apply the change to the system.
- Click **Refresh** to display the latest information from the router.

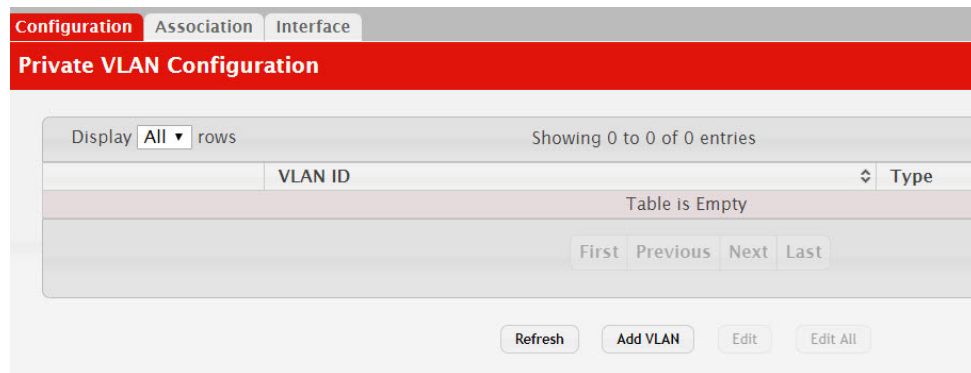
## Private VLAN

Use this screen to add Virtual Local Area Networks (VLANs) to the device and to configure existing VLANs as private VLANs. Private VLANs provide Layer 2 isolation between ports that share the same broadcast domain. In other words, a private VLAN allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer 2 network. Each subdomain is defined (represented) by a primary VLAN and a secondary VLAN. The primary VLAN ID is the same for all subdomains that belong to a private VLAN. The secondary VLAN ID differentiates subdomains from each another and provides Layer 2 isolation between ports that are members of the same private VLAN.

### Private VLAN Configuration

To access the Private VLAN Configuration page, click **Switching > Private VLAN > Configuration** in the navigation menu.

**Figure 165.** Private VLAN Configuration



Use the buttons to perform the following tasks:

- To add a VLAN, click **Add VLAN** and specify the VLAN ID(s) in the available field.
- To configure a private VLAN, select the entry to modify and click **Edit**. Then, configure the desired private VLAN setting.

**Note:** Default VLAN and management VLAN cannot be configured as a private VLANs and hence are not displayed on this page.

**Table 156.** Private VLAN Configuration Fields

Field	Description
VLAN ID	Displays the VLAN ID for which Private VLAN type is being set.

**Table 156.** Private VLAN Configuration Fields (continued)

Field	Description
Type	<p>Use the Private VLAN Type menu to select the type of private VLAN. The factory default is Unconfigured.</p> <ul style="list-style-type: none"> <li>• <b>Primary</b> – A private VLAN that forwards the traffic from the promiscuous ports to isolated ports, community ports, and other promiscuous ports in the same private VLAN. Only one primary VLAN can be configured per private VLAN. All ports within a private VLAN share the same primary VLAN.</li> <li>• <b>Isolated</b> – A secondary VLAN that carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN.</li> <li>• <b>Community</b> – A secondary VLAN that forwards traffic between ports that belong to the same community and to the promiscuous ports. Multiple community VLANs can be configured per private VLAN.</li> <li>• <b>Unconfigured</b> – The VLAN is not configured as a private VLAN.</li> </ul>

Click **Refresh** to display the latest information from the router.

## Private VLAN Association

Use this page to configure the association between the primary VLAN and secondary VLANs. Associating a secondary VLAN with a primary VLAN allows host ports in the secondary VLAN to communicate outside the private VLAN. To configure a primary VLAN association, select the entry to modify and click **Edit**.

To access the Private VLAN Association page, click **Switching > Private VLAN > Association** in the navigation menu.

**Figure 166.** Private VLAN Association



Use the buttons to perform the following tasks:

- To configure a primary VLAN association, select each entry to modify and click **Edit**.

**Note:** Isolated VLANs and Community VLANs are collectively called Secondary VLANs.

**Table 157.** *Private VLAN Association Fields*

Field	Description
Primary VLAN	The VLAN ID of each VLAN configured as a primary VLAN.
Isolated VLAN	The VLAN ID of the isolated VLAN associated with the primary VLAN. If the field is blank, no isolated VLAN has been associated with the primary VLAN. An isolated VLAN is a secondary VLAN that carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN.
Community VLAN	The VLAN ID of each community VLAN associated with the primary VLAN. If the field is blank, no community VLANs have been associated with the primary VLAN. A community VLAN is a secondary VLAN that forwards traffic between ports that belong to the same community and to the promiscuous ports. Multiple community VLANs can be configured per private VLAN.

After you click **Edit**, the Edit Private VLAN Association window opens and allows you to create associations with the selected primary VLAN. The following information describes the field in this window.

- **Secondary VLAN** – The isolated or community VLANs that can be associated with the primary VLAN. Secondary VLANs that are already associated with a primary VLAN do not appear in the list and cannot be associated with another primary VLAN. To select multiple secondary VLANs, Ctrl + click each VLAN to associate with the primary VLAN.

Click **Refresh** to display the latest information from the router.

## Private VLAN Interface

The private VLAN interface association page allows you to configure the port mode for the ports and LAGs that belong to a private VLAN and to configure associations between interfaces and primary/secondary private VLANs.

To access the Private VLAN Interface page, click **Switching > Private VLAN > Interface** in the navigation menu.

**Figure 167.** Private VLAN Interface

	Interface	Mode	Host Primary VLAN	Host Secondary VLAN	Promiscuous Primary VLAN	Promiscuous Secondary VLAN	Promiscuous Trunk Primary VLAN
<input type="checkbox"/>	1/0/1	General					
<input type="checkbox"/>	1/0/2	General					
<input type="checkbox"/>	1/0/3	General					
<input type="checkbox"/>	1/0/4	General					
<input type="checkbox"/>	1/0/5	General					
<input type="checkbox"/>	1/0/6	General					
<input type="checkbox"/>	1/0/7	General					
<input type="checkbox"/>	1/0/8	General					
<input type="checkbox"/>	1/0/9	General					
<input type="checkbox"/>	1/0/10	General					

Use the buttons to perform the following tasks:

- To configure the port mode and private VLAN-to-interface associations, select the entry to modify and click **Edit**.
- To remove the association between an interface and the primary/secondary private VLANs that the interface belongs to when it operates in host mode, select each interface with the association to clear and click **Remove Host Association**. You must confirm the action before the host association for the entry is cleared.
- To remove the association between an interface and the primary/secondary private VLANs that the interface belongs to when it operates in promiscuous mode, select each interface with the association to clear and click **Remove Promiscuous Association**. You must confirm the action before the promiscuous association for the entry is cleared.
- To remove the association between an interface and the primary/secondary promiscuous trunk private VLANs that the interface belongs to when it operates in promiscuous trunk mode, select each interface with the association to clear and click **Remove Promiscuous Trunk Association**. You must confirm the action before the promiscuous association for the entry is cleared.
- To remove the association between an interface and the primary/secondary private VLANs that the interface belongs to when it operates in isolated trunk mode, select each interface with the association to clear and click **Remove Isolated Trunk Association**. You must confirm the action before the isolated association for the entry is cleared.

**Table 158.** *Private VLAN Interface Fields*

Field	Description
Interface	The interface associated with the rest of the data in the row. When editing interface settings, this field identifies the interface being configured.
Mode	The private VLAN mode of the interface, which is one of the following: <ul style="list-style-type: none"> <li>• <b>General</b> – The interface is in general mode and is not a member of a private VLAN.</li> <li>• <b>Promiscuous</b> – The interface belongs to a primary VLAN and can communicate with all interfaces in the private VLAN, including other promiscuous ports, community ports, and isolated ports.</li> <li>• <b>Isolated Trunk</b> – The interface also belongs to a primary VLAN. It carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN. An isolated trunk port carries tagged traffic of multiple isolated VLANs and normal VLANs.</li> <li>• <b>Promiscuous Trunk</b> – The interface belongs to a primary VLAN and can communicate with all interfaces in the private VLAN, including other promiscuous trunk ports, community ports, and isolated ports.</li> <li>• <b>Host</b> – The interface belongs to a secondary VLAN and, depending upon the type of secondary VLAN, can either communicate with other ports in the same community (if the secondary VLAN is a community VLAN) and with the promiscuous ports or is able to communicate only with the promiscuous ports (if the secondary VLAN is an isolated VLAN).</li> </ul>
Host Primary VLAN	The primary private VLAN the port is a member of when it is configured to operate in Host mode.
Host Secondary VLAN	The secondary private VLAN the port is a member of when it is configured to operate in Host mode. The secondary private VLAN is either an isolated or community VLAN.
Isolated Trunk Primary VLAN	The primary private VLAN in which the port is a member when it is configured to operate in Isolated Trunk mode.
Isolated Trunk Secondary VLAN	The secondary private VLAN the port is a member of when it is configured to operate in Isolated Trunk mode. The secondary private VLAN must be an isolated VLAN.
Promiscuous Primary VLAN	The primary private VLAN in which the port is a member when it is configured to operate in Promiscuous mode.
Promiscuous Secondary VLAN	The secondary private VLAN the port is a member of when it is configured to operate in Promiscuous mode. The secondary private VLAN is either an isolated or community VLAN.
Promiscuous Trunk Primary VLAN	The primary private VLAN in which the port is a member when it is configured to operate in Promiscuous Trunk mode.
Promiscuous Trunk Secondary VLAN	The secondary private VLANs the port is a member of when it is configured to operate in Promiscuous Trunk mode. The secondary private VLANs are either isolated or community VLANs.
Trunk Native VLAN	When it is configured to operate in Isolated or Promiscuous Trunk mode, defines VLAN association for untagged packets. If not configured, untagged packets are dropped.
Trunk Allowed VLAN	The list of allowed normal VLANs on the trunk port when it is configured to operate in Promiscuous or Isolated Trunk mode.

**Table 158.** *Private VLAN Interface Fields (continued)*

Field	Description
Operational Private VLAN	The primary and secondary operational private VLANs for the interface. The VLANs that are operational depend on the configured mode for the interface and the private VLAN type.

Click **Refresh** to display the latest information from the router.

## Voice VLAN Configuration

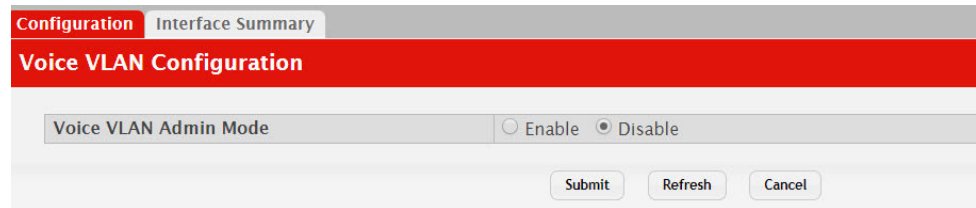
The voice VLAN feature enables switch ports to carry voice traffic with defined settings so that voice and data traffic are separated when coming onto the port. A voice VLAN ensures that the sound quality of an IP phone is safeguarded from deterioration when data traffic on the port is high.

The inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network-attached clients cannot initiate a direct attack on voice components. A QoS protocol based on the IEEE 802.1P class-of-service (CoS) protocol uses classification and scheduling to send network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

Voice VLAN is enabled per-port basis. A port can participate only in one voice VLAN at a time. The Voice VLAN feature is disabled by default.

To display the Voice VLAN Configuration page, click **Switching > Voice VLAN > Configuration**.

**Figure 168.** Voice VLAN Configuration



**Table 159.** Voice VLAN Configuration Fields

Field	Description
Voice VLAN Admin Mode	Click <b>Enable</b> or <b>Disable</b> to administratively turn the Voice VLAN feature on or off for all ports. The administrative mode of the Voice VLAN feature. When Voice VLAN is enabled globally and configured on interfaces that carry voice traffic, this feature can help ensure that the sound quality of an IP phone does not deteriorate when data traffic on the port is high.

- If you make any changes, click **Submit** to apply the change to the system.
- Click **Refresh** to display the latest information from the router.



## Voice VLAN Interface

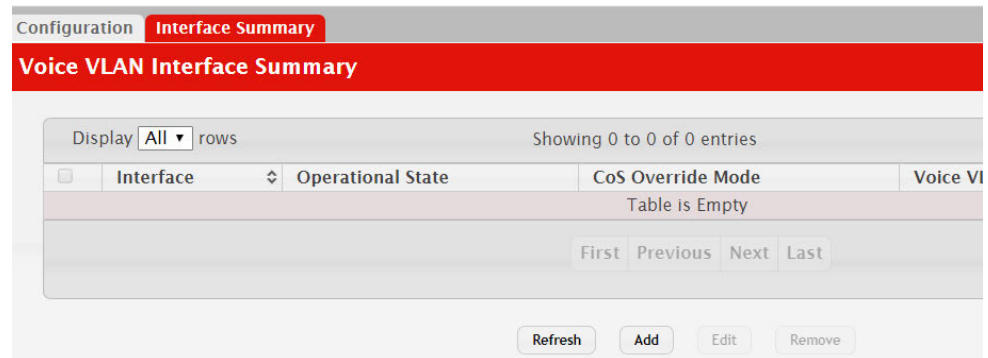
Use this page to configure the per-port settings for the Voice VLAN feature. When Voice VLAN is configured on a port that receives both voice and data traffic, it can help ensure that the voice traffic has priority.

Use the buttons to perform the following tasks:

- To configure Voice VLAN settings on a port, click **Add**. Select the interface to configure from the Interface menu, and then configure the desired settings.
- To change the Voice VLAN settings, select the interface to modify and click **Edit**.
- To remove the Voice VLAN configuration from one or more ports, select each entry to delete and click **Remove**.

To display the Voice VLAN Interface page, click **Switching > Voice VLAN > Interface Summary**.

**Figure 169.** Voice VLAN Interface



**Table 160.** Voice VLAN Interface Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When adding a Voice VLAN configuration to a port, the Interface menu allows you to select the port to configure. Only interfaces that have not been configured with Voice VLAN settings can be selected from the menu.
Operational State	The operational status of the Voice VLAN feature on the interface. To be enabled, Voice VLAN must be globally enabled and enabled on the interface. Additionally, the interface must be up and have a link.
CoS Override Mode	The Class of Service override mode: <ul style="list-style-type: none"> <li>• <b>Enabled</b> – The port ignores the 802.1p priority value in the Ethernet frames it receives from connected devices.</li> <li>• <b>Disabled</b> – The port trusts the priority value in the received frame.</li> </ul>

**Table 160.** *Voice VLAN Interface Fields (continued)*

Field	Description
Voice VLAN Interface Mode	Indicates how an IP phone connected to the port should send voice traffic: <ul style="list-style-type: none"><li>• <b>LAN ID</b> – Forward voice traffic in the specified voice VLAN.</li><li>• <b>Dot1p</b> – Tag voice traffic with the specified 802.1p priority value.</li><li>• <b>None</b> – Use the settings configured on the IP phone to send untagged voice traffic.</li><li>• <b>Untagged</b> – Send untagged voice traffic.</li><li>• <b>Disable</b> – Operationally disables the Voice VLAN feature on the interface.</li></ul>
Voice VLAN Interface Value	When adding or editing Voice VLAN settings for an interface and either VLAN ID or Dot1p is selected as the Voice VLAN Interface Mode, specify the voice VLAN ID or the Dot1p priority value that the connected IP phone should use for voice traffic.

- If you make any changes, click **Submit** to apply the change to the system.
- Click **Refresh** to display the latest information from the router.

---

## Port Auto Recovery

The Auto Recovery feature can automatically enable a disabled interface when the error conditions that caused the interface to be disabled are no longer detected. If Auto Recovery is not used (disabled), the interface remains disabled until an administrator manually enables it.

The switch supports an interface error disable feature that allows an interface to be automatically placed into a diagnostically disabled state when certain error conditions are detected on that interface. When an interface has been placed in a diagnostically disabled state, the interface is shut down, and no traffic is sent or received on that interface until it is either manually enabled by the administrator or re-enabled by the Auto Recovery feature after the recovery time interval has expired.

If the interface continues to encounter errors, it may be placed back into the diagnostically disabled state, and the interface will be disabled (link down). An interface in the diagnostically disabled state may also be manually recovered by enabling it from the Port Status page

## Port Auto Recovery Configuration

Use the Port Auto Recovery Configuration page to allow a port to attempt to become re-enabled if it has been placed into a diagnostically disabled state due to the detection of certain error conditions.

To access the Port Auto Recovery Configuration page, click **Switching > Auto Recovery > Configuration** in the navigation menu.

**Figure 170.** Port Auto Recovery Configuration

**Configuration**

**Port Auto Recovery Configuration**

**Auto Recovery Components**

All Components	<input type="checkbox"/>
ARP Inspection	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
BPDU Guard	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
BPDU Rate Limit	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Broadcast Storm Control	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Denial Of Service	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DHCP Rate Limit	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Keepalive	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
MAC Locking	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Multicast Storm Control	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
UDLD	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Unicast Storm Control	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

**Auto Recovery Parameters**

Recovery Time (Seconds)	<input type="text" value="300"/> (30 to 86400, 300 = Default)
-------------------------	---

**D-Disabled Interface Status**

Display All rows Showing 0 to 0 of 0 entries

Interface	Admin Mode	Port Status	Error Disable Reason	Auto Recover
Table is Empty				

**Table 161.** Port Auto Recovery Configuration Fields

Field	Description
Auto Recovery Components	<p>This field lists all the components that support the Auto Recovery feature. For each component, you can enable or disable Auto Recovery.</p> <p>An interface in the diagnostic disabled state for the configured components is recovered (link up) when the recovery interval expires. If the interface continues to encounter errors (from any listed components), it may be placed back in the diagnostic disabled state, and the interface will be disabled (link down). Interfaces in the diagnostic disabled state may also be manually recovered by enabling them from the Port Summary page.</p> <p>Auto Recovery is available for the following components:</p> <ul style="list-style-type: none"> <li>• ARP Inspection</li> <li>• BPDU Guard</li> <li>• BPDU Rate Limit</li> <li>• Broadcast Storm Control</li> <li>• Denial Of Service</li> <li>• DHCP Rate Limit</li> <li>• Keepalive</li> <li>• MAC Locking</li> <li>• Multicast Storm Control</li> <li>• UDLD</li> <li>• Unicast Storm Control</li> </ul>

**Table 161.** *Port Auto Recovery Configuration Fields (continued)*

Field	Description
Recovery Time	The auto recovery time interval. The auto recovery time interval is common for all components. The default value of the timer is 300 seconds and the range is from 30 to 86400.
D-Disabled Interface Status	This table displays the list of interfaces that are error disabled.
Interface	The interface which is error disabled.
Admin Mode	The administrative mode of the interface.
Port Status	Indicates whether the link is up or down. The link is the physical connection between the port or trunk and the interface on another device.
Error Disable Reason	If the device detects an error condition for an interface, then the device puts the interface in error disabled state by placing the interface in diagnostic disabled state. The interface can go into error disable state for one of the following reasons: <ul style="list-style-type: none"><li>• ARP Inspection</li><li>• BPDU Guard</li><li>• BPDU Storm</li><li>• Broadcast Storm</li><li>• Denial Of Service</li><li>• DHCP Rate Limit</li><li>• Keepalive</li><li>• MAC Locking</li><li>• Multicast Storm</li><li>• UDLD</li><li>• Unicast Storm</li></ul>
Auto Recovery Time Left	When Auto Recovery is enabled and the interface is placed in diagnostic disabled state, then a recovery timer starts for that interface. Once this timer expires, the device checks if the interface is in diagnostic disabled state. If yes, then the device enables the diagnostic disabled interface.

Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.

## Creating MAC Filters

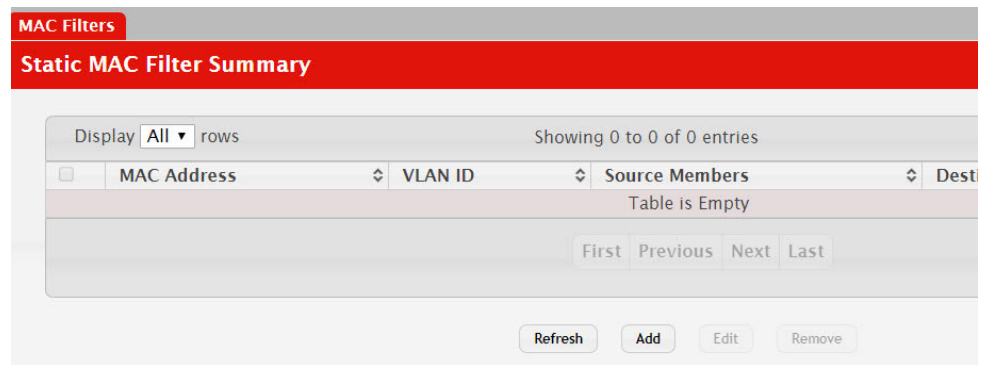
Static MAC filtering allows you to associate a MAC address with a VLAN and set of source ports and destination ports. (The availability of source and destination port filters is subject to platform restrictions). Any packet with a static MAC address in a specific VLAN is admitted only if the ingress port is included in the set of source ports; otherwise the packet is dropped. If admitted, the packet is forwarded to all the ports in the destination list.

## MAC Filter Configuration

Use the MAC Filter Configuration page to associate a MAC address with a VLAN and one or more source and/or destination ports

To access the MAC Filter Configuration page, click **Switching > Filters > MAC Filters** in the navigation menu.

**Figure 171.** MAC Filter Configuration



**Table 162.** MAC Filter Configuration Fields

Field	Description
MAC Address	The MAC address of the filter. The destination MAC address of an Ethernet frame must match this value to be considered for the filter. When adding or editing a filter, note that you cannot configure the following MAC addresses in this field: <ul style="list-style-type: none"> <li>00:00:00:00:00:00</li> <li>01:80:C2:00:00:00 to 01:80:C2:00:00:0F</li> <li>01:80:C2:00:00:20 to 01:80:C2:00:00:21</li> <li>FF:FF:FF:FF:FF:FF</li> </ul>
VLAN ID	The VLAN ID associated with the filter. The VLAN ID is used with the MAC address to fully identify the frames to filter.
Source Port Mask	The port(s) included in the inbound filter. If a frame with the MAC address and VLAN ID combination specified in the filter is received on a port in the Source Members list, it is forwarded to a port in the Destination Members list. If the frame that meets the filter criteria is received on a port that is not in the Source Members list, it is dropped. To add source ports to the filter, select one or more ports from the Available Port List field ( <b>CTRL</b> + click to select multiple ports). Then, use the appropriate arrow icon to move the selected ports to the Source Members field.

**Table 162.** *MAC Filter Configuration Fields (continued)*

Field	Description
Destination Port Mask	The port(s) included in the outbound filter. A frame with the MAC address and VLAN ID combination specified in the filter is transmitted only out of ports in the list. To add destination ports to the filter, select one or more ports from the Available Port List field ( <b>CTRL</b> + click to select multiple ports). Then, use the appropriate arrow icon to add the selected ports to the Source Members field.

### *Adding MAC Filters*

1. To add a MAC filter, click **Add** from the **MAC Filter** summary page.
2. Enter a valid MAC address and select a VLAN ID from the drop-down menu.  
The VLAN ID drop-down menu only lists VLANs currently configured on the system.
3. Select one or more ports to include in the filter. Use **CTRL** + click to select multiple ports.
4. Click **Submit** to apply the changes to the system.

### *Modifying MAC Filters*

To change the port mask(s) for an existing filter, select the entry from the **MAC Filter** field, and click **Edit**. When you have completed the changes, click **Submit**.

To change the MAC address or VLAN associated with a filter, you must remove and re-create the filter.

### *Removing MAC Filters*

To remove a filter, select it from the **MAC Filter** drop-down menu and click **Remove**.

# Configuring Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

## DAI Configuration

Use the DAI Configuration page to configure global DAI settings.

To display the DAI Configuration page, click **Switching > Dynamic ARP Inspection > Global** in the navigation menu.

**Figure 172.** Dynamic ARP Inspection Global Configuration

Global	VLAN	Interface	ACL Summary	ACL Configuration	Statistics
<b>Global Configuration</b>					
Validate Source MAC	<input type="checkbox"/>				
Validate Destination MAC	<input type="checkbox"/>				
Validate IP	<input type="checkbox"/>				
<input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="Cancel"/>					

**Table 163.** Dynamic ARP Inspection Global Configuration

Field	Description
Validate Source MAC	When this option is selected, DAI verifies that the sender hardware address in the ARP packet equals the source MAC address in the Ethernet header. If the addresses do not match, the ARP packet is dropped.
Validate Destination MAC	When this option is selected, DAI verifies that the target hardware address in the ARP packet equals the destination MAC address in the Ethernet header. If the addresses do not match, the ARP packet is dropped. This check applies only to ARP responses because the target MAC address is unspecified in ARP requests.
Validate IP	When this option is selected, DAI drops ARP packets with an invalid IP address. The following IP addresses are considered invalid: <ul style="list-style-type: none"><li>• 0.0.0.0</li><li>• 255.255.255.255</li><li>• All IP multicast addresses</li><li>• All class E addresses (240.0.0.0/4)</li><li>• Loopback addresses (in the range 127.0.0.0/8)</li></ul>



Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.

## DAI VLAN Configuration

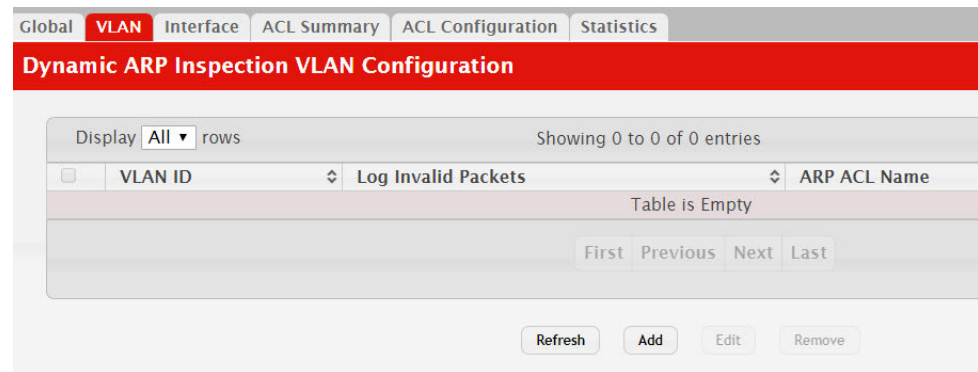
Use the DAI VLAN Configuration page to select the DAI-capable VLANs for which information is to be displayed or configured.

Use the buttons to perform the following tasks:

- To enable DAI on a VLAN and to configure the optional DAI settings, click **Add**.
- To change the DAI settings on VLAN, select the VLAN with the settings to update and click **Edit**.
- To disable DAI on one or more VLANs, select each entry to disable and click **Remove**. After confirming the action, the entries are removed from the table.

To display the DAI Configuration page, click **Switching > Dynamic ARP Inspection > VLAN** in the navigation menu.

**Figure 173.** Dynamic ARP Inspection VLAN Configuration



**Table 164.** Dynamic ARP Inspection VLAN Configuration

Field	Description
VLAN ID	Lists each VLAN that has been enabled for DAI. After you click <b>Add</b> , use the VLAN ID menu to select the VLAN on which to enable DAI. A VLAN does not need to exist on the system to be enabled for DAI.
Logging Invalid Packets	Indicates whether DAI logging is enabled on this VLAN. When logging is enabled, DAI generates a log message whenever an invalid ARP packet is discovered and dropped.
ARP ACL Name	The name of the of ARP access control list (ACL) that the VLAN uses as the filter for ARP packet validation. The ARP ACL must already exist on the system to associate it with a DAI-enabled VLAN. ARP ACLs include permit rules only.

**Table 164.** *Dynamic ARP Inspection VLAN Configuration*

Field	Description
Static	<p>Determines whether to use the DHCP snooping database for ARP packet validation if the packet does not match any ARP ACL rules. The options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b> – The ARP packet will be validated by the ARP ACL rules only. Packets that do not match any ARP ACL rules are dropped without consulting the DHCP snooping database.</li> <li>• <b>Disable</b> – The ARP packet needs further validation by using the entries in the DHCP Snooping database.</li> </ul>

- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Refresh** to refresh the page with the most current data from the switch.

## DAI Interface Configuration

Use the DAI Interface Configuration page to select the DAI Interface for which information is to be displayed or configured.

To display the DAI Interface Configuration page, click **Switching > Dynamic ARP Inspection > Interface Configuration** in the navigation menu.

**Figure 174.** Dynamic ARP Inspection Interface Configuration

Interface	Trust State	Rate Limit
1/0/1	Disabled	15
1/0/2	Disabled	15
1/0/3	Disabled	15
1/0/4	Disabled	15
1/0/5	Disabled	15
1/0/6	Disabled	15
1/0/7	Disabled	15
1/0/8	Disabled	15
1/0/9	Disabled	15
1/0/10	Disabled	15

**Table 165.** *Dynamic ARP Inspection Interface Configuration*

Field	Description
Interface	The interface associated with the rest of the data in the row. In the Edit Interface Configuration window, this field identifies the interface that is being configured.

**Table 165.** *Dynamic ARP Inspection Interface Configuration*

Field	Description
Trust State	Indicates whether the DAI feature should check traffic on the interface for possible ARP packet violations. Trust state can be enabled or disabled after you select an interface and click <b>Edit</b> . This field has one of the following values: <ul style="list-style-type: none"> <li>• <b>Enabled</b> – The interface is trusted. ARP packets arriving on this interface are forwarded without DAI validation.</li> <li>• <b>Disabled</b> – The interface is not trusted. ARP packets arriving on this interface are subjected to ARP inspection.</li> </ul>
Rate Limit	The maximum rate for incoming ARP packets on the interface, in packets per second (pps). If the incoming rate exceeds the configured limit, the ARP packets are dropped. Rate limiting can be enabled or disabled after you select an interface and click <b>Edit</b> .
Burst Interval	The number of consecutive seconds the interface is monitored for incoming ARP packet rate limit violations.
Rate Limiting	Select this option to allow the interface to drop ARP packets if the rate at which they are received on the interface exceeds the configured Rate Limit for the Burst Interval duration. If this option is clear, rate limiting is disabled.

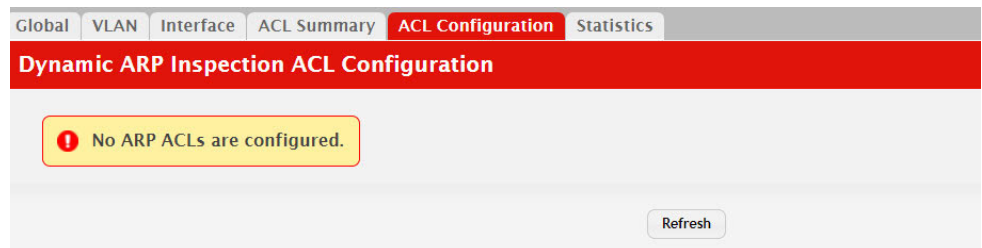
- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Refresh** to refresh the page with the most current data from the switch.

## DAI ARP ACL Configuration

Use the DAI ARP ACL Configuration page to add or remove DAI ARP ACLs.

To display the DAI ARP ACL Configuration page, click **Switching > Dynamic ARP Inspection > ACL Configuration** in the navigation menu.

**Figure 175.** Dynamic ARP Inspection ACL Configuration



**Table 166.** *Dynamic ARP Inspection ARP ACL Configuration*

Field	Description
ACL Name	The menu contains the ARP ACL names that exist on the system.
Sender IP Address	The IP address of a system that is permitted to send ARP packets. The ARP packet must match on both the Sender IP Address and Sender MAC Address values in the rule to be considered valid.

**Table 166.** *Dynamic ARP Inspection ARP ACL Configuration (continued)*

Field	Description
Sender MAC Address	The MAC address of a system that is permitted to send ARP packets. The ARP packet must match on both the Sender IP Address and Sender MAC Address values in the rule to be considered valid.
Remarks	One or more remarks configured for the selected ACL and associated with the rule during rule creation.

Use the buttons to perform the following tasks:

- To create an ARP ACL and configure the first rule, click **Add ACL**.
- To add a new rule to an existing ACL, click **Add Rule** and select the name of the ACL to update from the ACL Name menu. Then, configure the rule.
- To remove one or more ARP ACLs, select each entry to delete and click **Remove**.
- Click **Refresh** to refresh the page with the most current data from the switch.

## DAI ARP ACL Rule Configuration

Use the DAI ARP ACL Rule Configuration page to add or remove DAI ARP ACL Rules.

To display the DAI ARP ACL Rule Configuration page, click **Add Rule** from the Dynamic ARP Inspection ACL Configuration page.

**Figure 176.** Add ACL Rule

The screenshot shows a web form titled "Add ACL Rule". It contains two input fields: "Sender IP Address" with a placeholder "(x.x.x.x)" and "Sender MAC Address" with a placeholder "(xx:xx:xx:xx:xx:xx)". A "Submit" button is located at the bottom right of the form area.

**Table 167.** *Dynamic ARP Inspection ARP ACL Rule Configuration*

Field	Description
Sender IP Address	To create a new rule for the selected ARP ACL, enter in this field the Sender IP Address match value for the ARP ACL.
Sender MAC Address	To create a new rule for the selected ARP ACL, enter in this field the Sender MAC Address match value for the ARP ACL.

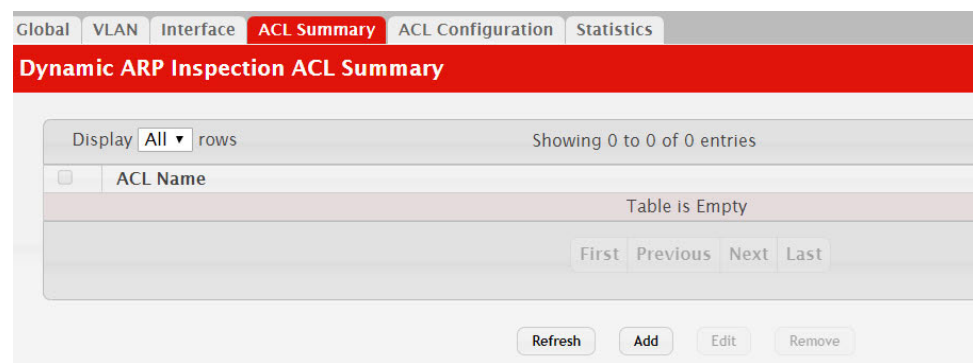
- Click **Submit** to add a new ARP ACL rule.

## DAI ARP ACL Summary

Use this page to configure ARP Access Control Lists (ACLs). An ARP ACL can contain one or more permit rules. Each rule contains the IP address and MAC address of a system allowed to send ARP packets. When an ARP ACL is associated with a DAI-enabled VLAN, and an ARP packet is received on an interface that is a member of that VLAN, DAI validates the address information in the ARP packet against the rules in the ACL. If the sender information in the ARP packet matches a rule in the ARP ACL, DAI considers the packet to be valid, and the packet is forwarded.

To display the DAI ARP ACL Configuration page, click **Switching > Dynamic ARP Inspection > ACL Summary** in the navigation menu.

**Figure 177.** Dynamic ARP Inspection ACL Summary



**Table 168.** Dynamic ARP Inspection ACL Summary Fields

Field	Description
ACL Name	The name of the ACL. Only the ACLs that appear in this column can be referenced by DNI-enabled VLANs.

Use the buttons to perform the following tasks:

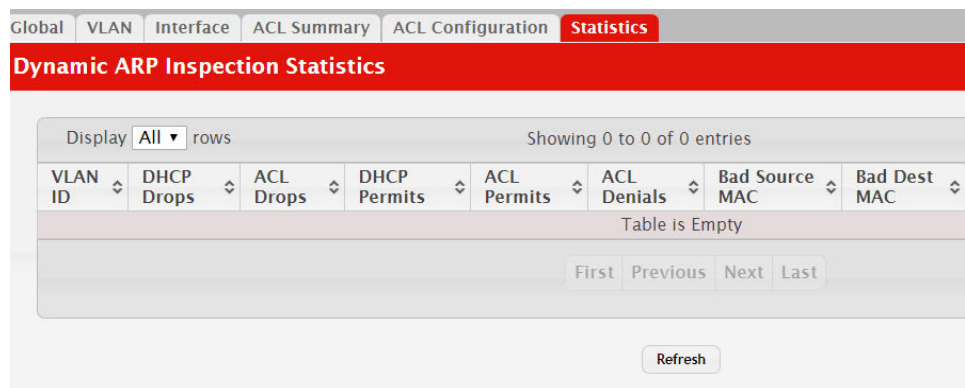
- To add an ARP ACL, click **Add** and configure the ACL name.
- To configure rules for an ARP ACL, select the ACL to configure and click **Edit**. You are redirected to the Dynamic ARP Inspection ACL Configuration page for the selected ACL.
- To remove one or more ARP ACLs, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.
- Click **Refresh** to refresh the page with the most current data from the switch.

## DAI Statistics

Use the DAI Statistics page to display the statistics per VLAN.

To display the DAI Statistics page, click **Switching > Dynamic ARP Inspection > DAI Statistics** in the navigation menu.

**Figure 178.** Dynamic ARP Inspection Statistics



**Table 169.** Dynamic ARP Inspection Statistics

Field	Description
VLAN ID	The DAI-enabled VLAN associated with the rest of the information in the row. When DAI is enabled on a VLAN, DAI is enabled on all interfaces that are members of that VLAN.
DHCP Drops	The number of ARP packets that have been dropped by DAI because no matching DHCP snooping binding entry was found in the DHCP snooping database.
ACL Drops	The number of ARP packets that have been dropped by DAI because the sender IP address and sender MAC address in the ARP packet did not match any rules in the ARP ACL associated with this VLAN. The static flag on this VLAN is enabled, which means ARP packets that fail to match an ARP ACL rule are dropped immediately and are not checked against the DHCP snooping database for further validation.
DHCP Permits	The number of ARP packets that were forwarded by DAI because a matching DHCP snooping binding entry was found in the DHCP snooping database.
ACL Permits	The number of ARP packets that were forwarded by DAI because the sender IP address and sender MAC address in the ARP packet matched a rule in the ARP ACL associated with this VLAN.
Bad Source MAC	The number of ARP packets that were dropped by DAI because the sender MAC address in ARP packet did not match the source MAC address in the Ethernet header.
Bad Dest MAC	The number of ARP packets that were dropped by DAI because the target MAC address in the ARP reply packet did not match the destination MAC address in the Ethernet header.
Invalid IP	The number of ARP packets that were dropped by DAI because the sender IP address in the ARP packet or target IP address in the ARP reply packet was invalid. The following IP addresses are considered invalid: <ul style="list-style-type: none"> <li>• 0.0.0.0</li> <li>• 255.255.255.255</li> <li>• All IP multicast addresses</li> <li>• All class E addresses (240.0.0.0/4)</li> <li>• Loopback addresses (in the range 127.0.0.0/8)</li> </ul>
Forwarded	The total number of valid ARP packets forwarded by DAI.
Dropped	The total number of invalid ARP packets dropped by DAI.

Click **Refresh** to refresh the page with the most current data from the switch.

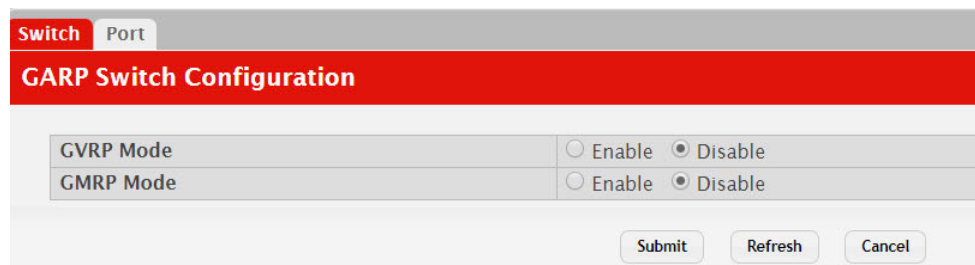
## GARP Configuration

Use this page to set the administrative mode for the features that use the Generic Attribute Registration Protocol (GARP), including GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). GARP is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of switches interested in a given network attribute, such as VLAN ID or multicast address.

## Switch Configuration

To access the GARP Switch Configuration page, click **Switching > GARP > Switch** in the navigation menu.

**Figure 179.** GARP Switch Configuration



**Table 170.** GARP Switch Configuration Fields

Field	Description
GVRP Mode	The administrative mode of GVRP on the system. When enabled, GVRP can help dynamically manage VLAN memberships on trunk ports.
GMRP Mode	The administrative mode of GMRP on the system. When enabled, GMRP can help control the flooding of multicast traffic by keeping track of group membership information. GMRP is similar to IGMP snooping in its purpose, but IGMP snooping is more widely used. GMRP must be running on both the host and the switch to function properly.

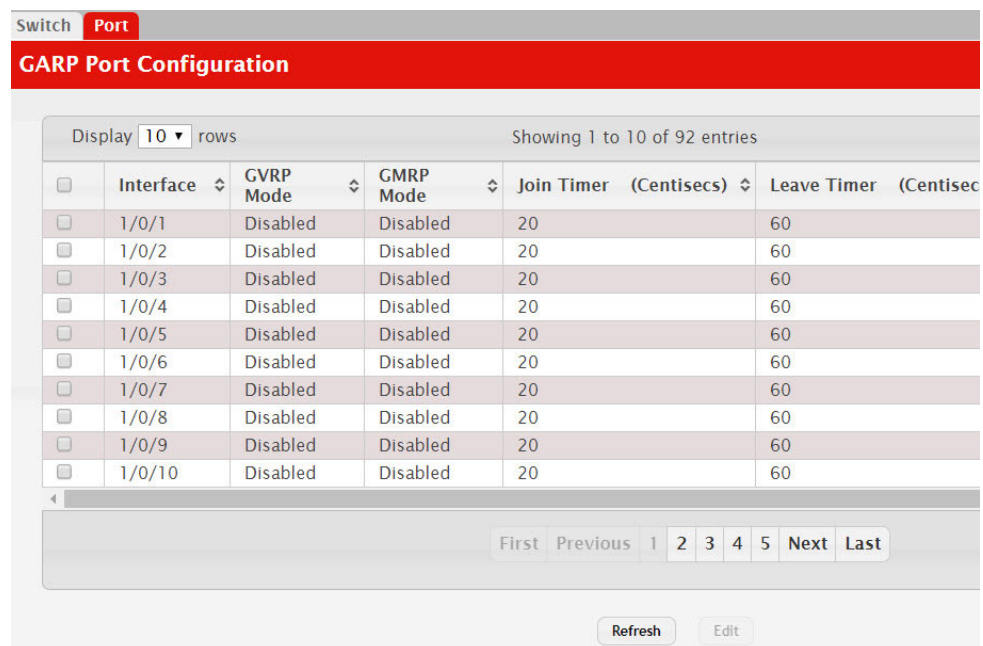
Click **Refresh** to refresh the page with the most current data from the switch.

## Port Configuration

Use this page to set the per-interface administrative mode for GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). On this page, you can also set the GARP timers for each interface. GVRP and GMRP use the same set of GARP timers to specify the amount of time to wait before transmitting various GARP messages.

To access the GARP Port Configuration page, click **Switching > GARP > Port** in the navigation menu.

**Figure 180.** GARP Port Configuration



To change the GARP settings for one or more interfaces, select each interface to configure and click **Edit**. The same settings are applied to all selected interfaces.

**Table 171.** GARP Port Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring one or more interfaces in the Edit GARP Port Configuration window, this field identifies the interfaces that are being configured.
GVRP Mode	The administrative mode of GVRP on the interface. When enabled, GVRP can help dynamically manage VLAN memberships on trunk ports. GVRP must also be enabled globally for the protocol to be active on the interface. When disabled, the protocol will not be active on the interface, and the GARP timers have no effect.
GMRP Mode	The administrative mode of GMRP on the interface. When enabled, GMRP can help control the flooding of multicast traffic by keeping track of group membership information. GMRP must also be enabled globally for the protocol to be active on the interface. When disabled, the protocol will not be active on the interface, and the GARP timers have no effect.
Join Timer (Centisecs)	The amount of time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group.
Leave Timer (Centisecs)	The amount of time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry. This timer allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service.



**Table 171.** *GARP Port Configuration Fields (continued)*

Field	Description
Leave All Timer (Centi-secs)	The amount of time to wait before sending a LeaveAll PDU after the GARP application has been enabled on the interface or the last LeaveAll PDU was sent. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration.

Click **Refresh** to refresh the page with the most current data from the switch.

## Configuring DHCP Snooping

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized. You can enable DHCP snooping globally and on specific VLANs, and configure ports within the VLAN to be trusted or untrusted. If a DHCP message arrives on an untrusted port, DHCP snooping filters messages that are not from authorized DHCP clients. DHCP server messages are forwarded only through trusted ports.

### Global DHCP Snooping Configuration

Use this page to view and configure the global settings for DHCP Snooping.

To access the Global DHCP Snooping Configuration page, click **Switching > DHCP Snooping > Base > Global** in the navigation menu.

**Figure 181.** Global DHCP Snooping Configuration

Global	VLAN Configuration	Interface Configuration	Static Bindings	Dynamic Bindings	Persistent	Statist
<b>DHCP Snooping Configuration</b>						
DHCP Snooping Mode		<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
MAC Address Validation		<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
<input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="Cancel"/>						

**Table 172.** Global DHCP Snooping Configuration Fields

Field	Description
DHCP Snooping Mode	The administrative mode of DHCP snooping on the device.
MAC Address Validation	Enables or Disables the verification of the sender MAC address for DHCP snooping. When enabled, the device checks packets that are received on untrusted interface to verify that the MAC address and the DHCP client hardware address match. If the addresses do not match, the device drops the packet.

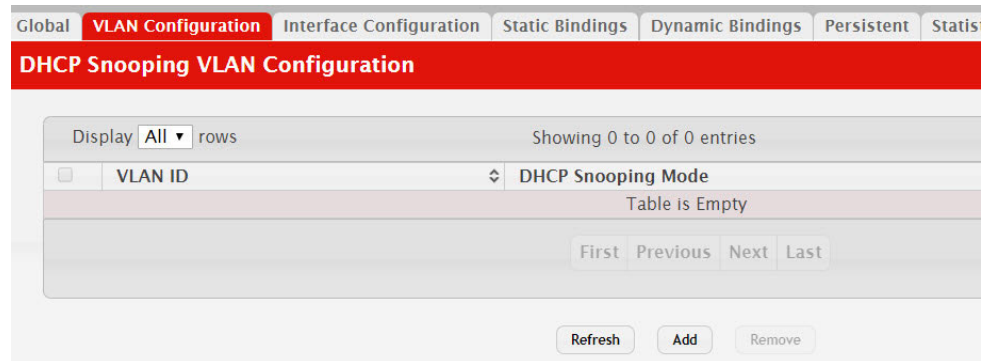
Click **Refresh** to refresh the page with the most current data from the switch.

### DHCP Snooping VLAN Configuration

Use this page to view and configure the DHCP snooping settings on VLANs that exist on the device. DHCP snooping can be configured on switching VLANs and routing VLANs. For Layer 2 (non-routing) VLANs, DHCP snooping forwards valid DHCP client messages received on the VLANs. The message is forwarded on all trusted interfaces in the VLAN. When a DHCP packet is received on a routing VLAN, the DHCP snooping application applies its filtering rules and updates the bindings database. If a client message passes filtering rules, the message is placed into the software forwarding path, where it may be processed by the DHCP relay agent, the local DHCP server, or forwarded as an IP packet.

To access the DHCP Snooping VLAN Configuration page, click **Switching > DHCP Snooping > Base > VLAN Configuration** in the navigation menu.

**Figure 182.** DHCP Snooping VLAN Configuration



Use the buttons to perform the following tasks:

- To enable a VLAN for DHCP snooping, click **Add** and select the VLAN to administratively enable for DHCP snooping. To select multiple VLANs, **CTRL +** click each VLAN to select.
- To disable DHCP snooping on one or more VLANs, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 173.** DHCP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN ID that is enabled for DHCP snooping. In the Add DHCP Snooping VLAN Configuration window, this field lists the VLAN ID of all VLANs that exist on the device.
DHCP Snooping Mode	The current administration mode of DHCP snooping for the VLAN. Only VLANs that are enabled for DHCP snooping appear in the list.

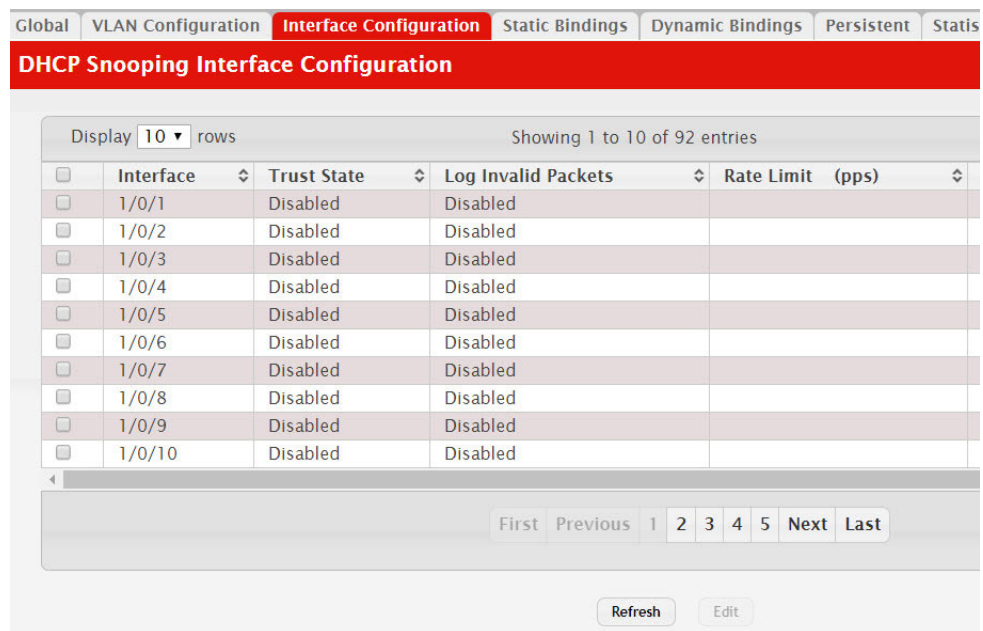
Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP Snooping Interface Configuration

Use this page to view and configure the DHCP snooping settings for each interface. The DHCP snooping feature processes incoming DHCP messages. For DHCPRELEASE and DHCPDECLINE messages, the feature compares the receive interface and VLAN with the client's interface and VLAN in the binding database. If the interfaces do not match, the application logs the event (when logging of invalid packets is enabled) and drops the message. If MAC address validation is globally enabled, messages that pass the initial validation are checked to verify that the source MAC address and the DHCP client hardware address match. Where there is a mismatch, DHCP snooping logs the event (when logging of invalid packets is enabled) and drops the packet. To change the DHCP Snooping settings for one or more interfaces, select each entry to modify and click Edit. The same settings are applied to all selected interfaces.

To access the DHCP Snooping Interface Configuration page, click **Switching > DHCP Snooping > Base > Interface Configuration** in the navigation menu.

**Figure 183.** DHCP Snooping Interface Configuration



**Table 174.** DHCP Snooping Interface Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the settings for one or more interfaces, this field identifies each interface that is being configured.
Trust State	The trust state configured on the interface. The trust state is one of the following: <ul style="list-style-type: none"> <li>• <b>Disabled</b> – The interface is considered to be untrusted and could potentially be used to launch a network attack. DHCP server messages are checked against the bindings database. On untrusted ports, DHCP snooping enforces the following security rules: <ul style="list-style-type: none"> <li>– DHCP packets from a DHCP server (DHCP OFFER, DHCP ACK, DHCP NAK, DHCP RELEASE QUERY) are dropped.</li> <li>– DHCP RELEASE and DHCP DECLINE messages are dropped if the MAC address is in the snooping database but the binding's interface is other than the interface where the message was received.</li> <li>– DHCP packets are dropped when the source MAC address does not match the client hardware address if MAC Address Validation is globally enabled.</li> </ul> </li> <li>• <b>Enabled</b> – The interface is considered to be trusted and forwards DHCP server messages without validation.</li> </ul>
Log Invalid Packets	The administrative mode of invalid packet logging on the interface. When enabled, the DHCP snooping feature generates a log message when an invalid packet is received and dropped by the interface.

**Table 174.** DHCP Snooping Interface Configuration Fields (continued)

Field	Description
Rate Limit (pps)	The rate limit value for DHCP packets received on the interface. To prevent DHCP packets from being used as a DoS attack when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. If the incoming rate of DHCP packets exceeds the value of this object during the amount of time specified for the burst interval, the port will be shutdown. You must administratively enable the port to allow it to resume traffic forwarding.
Burst Interval (Seconds)	The burst interval value for rate limiting on this interface. If the rate limit is unspecified, then burst interval has no meaning.

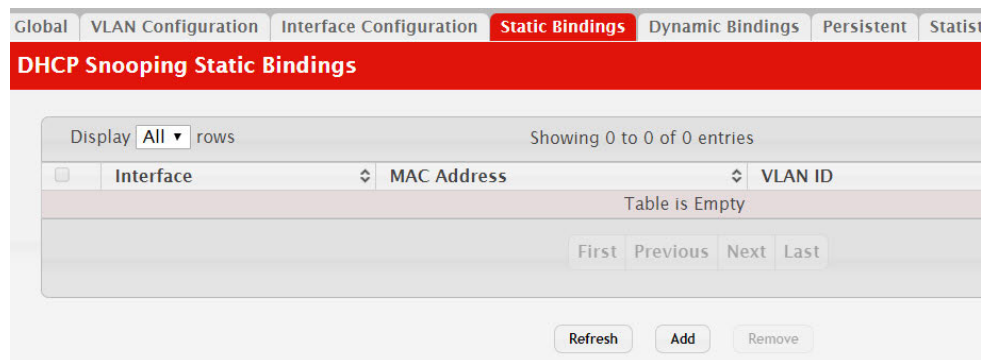
Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP Snooping Static Bindings

Use this page to view, add, and remove static bindings in the DHCP snooping bindings database.

To access the DHCP Snooping Static Bindings page, click **Switching > DHCP Snooping > Base > Static Bindings** in the navigation menu.

**Figure 184.** DHCP Snooping Static Bindings



**Table 175.** DHCP Snooping Static Bindings Fields

Field	Description
Interface	The interface on which the DHCP client is authorized.
MAC Address	The MAC address associated with the DHCP client. This is the Key to the binding database.
VLAN ID	The ID of the VLAN the client is authorized to use.
IP Address	The IP address of the client.

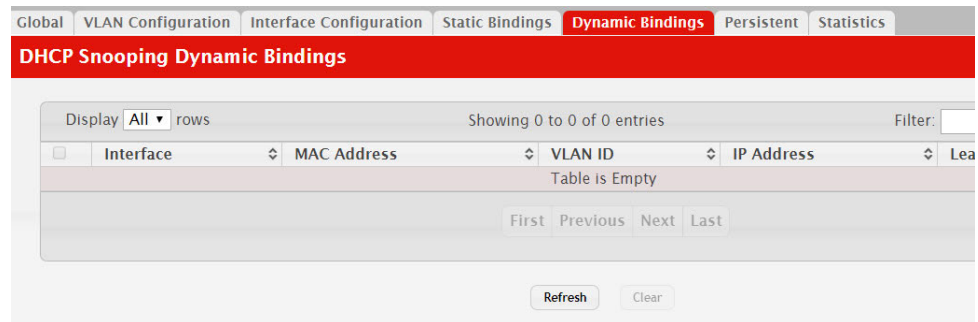
Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP Snooping Dynamic Bindings

Use this page to view and clear dynamic bindings in the DHCP snooping bindings database. The DHCP snooping feature uses DHCP messages to build and maintain the bindings database. The bindings database includes data for clients only on untrusted ports. DHCP snooping creates a tentative binding from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to an interface (the interface where the DHCP client message was received). Tentative bindings are completed when DHCP snooping learns the client's IP address from a DHCP ACK message on a trusted port. DHCP snooping removes bindings in response to DECLINE, RELEASE, and NACK messages. The DHCP snooping feature ignores the ACK messages as a reply to the DHCP Inform messages received on trusted ports.

To access the DHCP Snooping Dynamic Bindings page, click **Switching > DHCP Snooping > Base > Dynamic Bindings** in the navigation menu.

**Figure 185.** DHCP Snooping Dynamic Bindings



**Table 176.** DHCP Snooping Dynamic Bindings Fields

Field	Description
Interface	The interface on which the DHCP client message was received.
MAC Address	The MAC address associated with the DHCP client that sent the message. This is the Key to the binding database.
VLAN ID	The VLAN ID of the client interface.
IP Address	The IP address assigned to the client by the DHCP server.
Lease Time	The remaining IP address lease time for the client.
Clear (Button)	To remove one or more entries in the database, select each entry to delete and click <b>Clear</b> . You must confirm the action before the entry is deleted.

Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP Snooping Persistent Configuration

Use this page to configure the persistent location of the DHCP snooping bindings database. The bindings database can be stored locally on the device or on a remote system somewhere else in the network. The device must be able to reach the IP address of the remote system to send bindings to a remote database.

To access the DHCP Snooping Persistent Configuration page, click **Switching > DHCP Snooping > Base > Persistent** in the navigation menu.

**Figure 186.** DHCP Snooping Persistent Configuration

**Table 177.** DHCP Snooping Persistent Configuration Fields

Field	Description
Store	The location of the DHCP snooping bindings database, which is either locally on the device (Local) or on a remote system (Remote).
Remote IP Address	The IP address of the system on which the DHCP snooping bindings database will be stored. This field is available only if Remote is selected in the Store field.
Remote File Name	The file name of the DHCP snooping bindings database in which the bindings are stored. This field is available only if Remote is selected in the Store field.
Write Delay (Seconds)	The amount of time to wait between writing bindings information to persistent storage. This allows the device to collect as many entries as possible (new and removed) before writing them to the persistent file.

Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP Snooping Statistics

Use this page to configure the persistent location of the DHCP snooping bindings database. The bindings database can be stored locally on the device or on a remote system somewhere else in the network. The device must be able to reach the IP address of the remote system to send bindings to a remote database.

To access the DHCP Snooping Statistics page, click **Switching > DHCP Snooping > Base > Statistics** in the navigation menu.

**Figure 187.** DHCP Snooping Statistics

**Table 178.** DHCP Snooping Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
MAC Verify Failures	The number of DHCP messages that were dropped because the source MAC address and client hardware address did not match. MAC address verification is performed only if it is globally enabled.
Client Ifc Mismatch	The number of packets that were dropped by DHCP snooping because the interface and VLAN on which the packet was received does not match the client's interface and VLAN information stored in the binding database.
DHCP Server Msgs Received	The number of DHCP server messages ((DHCP OFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) that have been dropped on an untrusted port.
Clear Counters (Button)	To reset the statistics to zero for one or more interfaces, select each interface with the data to reset and click Clear Counters. You must confirm the action before the entry is deleted.

Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP L2 Relay Global Configuration

Use this page to control the administrative mode of DHCP Layer 2 Relay on the device. In Layer 2 switched networks, there may be one or more infrastructure devices (for example, a switch) between the client and the L3 Relay agent/DHCP server. In this instance, some of the client device information required by the L3 Relay agent may not be visible to it. When this happens, an L2 Relay agent can be used to add the information that the L3 Relay Agent and DHCP server need to perform their roles in IP address configuration and assignment.

To access the DHCP L2 Relay Global Configuration page, click **Switching > DHCP Snooping > L2 Relay > Global** in the navigation menu.

**Figure 188.** DHCP L2 Relay Global Configuration

**Table 179.** DHCP L2 Relay Global Configuration Fields

Field	Description
Admin Mode	The global mode of DHCP L2 relay on the device. When enabled, the device can act as a DHCP L2 relay agent. This functionality must also be enabled on each port you want this service to operate on.

Click **Refresh** to refresh the page with the most current data from the switch.



## DHCP L2 Relay Interface Configuration

Use this page to enable L2 DHCP relay on individual ports. Note that L2 DHCP relay must also be enabled globally on the device. To change the DHCP L2 relay settings for one or more interfaces, select each entry to modify and click Edit. The same settings are applied to all selected interfaces.

To access the DHCP L2 Relay Interface Configuration page, click **Switching > DHCP Snooping > L2 Relay > Interface Configuration** in the navigation menu.

**Figure 189.** DHCP L2 Relay Interface Configuration

Interface	L2 Relay Mode	Trust Mode
1/0/1	Disabled	Disabled
1/0/2	Disabled	Disabled
1/0/3	Disabled	Disabled
1/0/4	Disabled	Disabled
1/0/5	Disabled	Disabled
1/0/6	Disabled	Disabled
1/0/7	Disabled	Disabled
1/0/8	Disabled	Disabled
1/0/9	Disabled	Disabled
1/0/10	Disabled	Disabled

**Table 180.** DHCP L2 Relay Interface Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the settings for one or more interfaces, this field identifies each interface that is being configured.
L2 Relay Mode	The administrative mode of L2 relay mode on the interface. When enabled, the interface can act as a DHCP relay agent and add information that the L3 relay agent and DHCP server need to perform their roles in IP address configuration and assignment.
Trust Mode	The L2 relay trust mode for the interface, which is one of the following: <ul style="list-style-type: none"> <li><b>Trusted</b> – A trusted interface usually connects to other agents or servers participating in the DHCP interaction (e.g. other L2 or L3 relay agents or servers). An interface in this mode always expects to receive DHCP packets that include Option 82 information. If Option 82 information is not included, these packets are discarded.</li> <li><b>Untrusted</b> – An untrusted interface is generally connected to clients. DHCP packets arriving on an untrusted interface are never expected to carry Option 82 and are discarded if they do.</li> </ul>

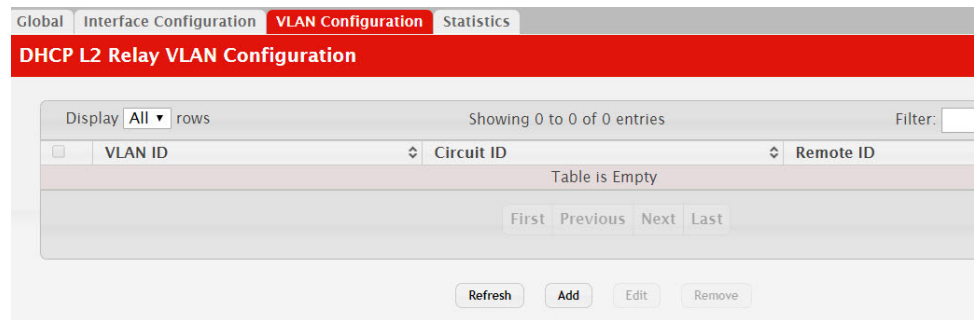
Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP L2 Relay VLAN Configuration

Use this page to control the DHCP L2 relay settings on a particular VLAN. The VLAN is identified by a service VLAN ID (S-VID), which a service provider uses to identify a customer's traffic while traversing the provider network to multiple remote sites. The device uses the VLAN membership of the switch port client (the customer VLAN ID, or C-VID) to perform a lookup on a corresponding S-VID.

To access the DHCP L2 Relay VLAN Configuration page, click **Switching > DHCP Snooping > L2 Relay > VLAN Configuration** in the navigation menu.

**Figure 190.** DHCP L2 Relay VLAN Configuration



Use the buttons to perform the following tasks:

- To enable a VLAN for DHCP L2 relay, click **Add** and select the VLAN from the available menu.
- To update the DHCP L2 relay settings for one or more VLANs, select each entry to update and click **Edit**. The same settings are applied to all selected VLANs.
- To disable one or more VLANs as DHCP L2 relay agents, select the appropriate VLANs and click **Remove**. You must confirm the action.

**Table 181.** DHCP L2 Relay VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN associated with the rest of the data in the row. When configuring the settings for one or more VLANs, this field identifies each VLAN that is being configured.
Circuit ID	The administrative mode of the circuit ID. When enabled, if a client sends a DHCP request to the device and the client is in a VLAN that corresponds to the S-VID, the device adds the client's interface number to the Circuit ID sub-option of Option 82 in the DHCP request packet. This enables the device to reduce the broadcast domain to which the server replies are switched when the broadcast bit is set for DHCP packets. When this bit is set, the server is required to echo Option 82 in replies. Since the circuit-id field contains the client interface number, the L2 relay agent can forward the response to the requesting interface only, rather than to all ports in the VLAN).

**Table 181.** DHCP L2 Relay VLAN Configuration Fields (continued)

Field	Description
Remote ID	The DHCP remote identifier string. When a string is entered here, if a client sends a DHCP request to the device and the client is in a VLAN that corresponds to the S-VID, the device adds the string to the Remote-ID sub-option of Option 82 in the DHCP request packet. This sub-option can be used by the server for parameter assignment. The content of this option is vendor-specific.

Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP L2 Relay Interface Statistics

This page shows statistical information about the L2 DHCP Relay requests received on trusted and untrusted interfaces. An interface is untrusted when the DHCP L2 relay trust mode is disabled.

To access the DHCP L2 Relay Interface Statistics page, click **Switching > DHCP Snooping > L2 Relay > Statistics** in the navigation menu.

**Figure 191.** DHCP L2 Relay Interface Statistics

Interface	Untrusted Server Messages With Option-82	Untrusted Client Messages With Option-82	Trusted Server Messages With Option-82	Trust With
1/0/1	0	0	0	0
1/0/2	0	0	0	0
1/0/3	0	0	0	0
1/0/4	0	0	0	0
1/0/5	0	0	0	0
1/0/6	0	0	0	0
1/0/7	0	0	0	0
1/0/8	0	0	0	0
1/0/9	0	0	0	0
1/0/10	0	0	0	0

**Table 182.** DHCP L2 Relay Interface Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
Untrusted Server Messages With Option-82	The number of messages received on an untrusted interface from a DHCP server that contained Option 82 data. These messages are dropped.
Untrusted Client Messages With Option-82	The number of messages received on an untrusted interface from a DHCP client that contained Option 82 data. These messages are dropped.

**Table 182.** DHCP L2 Relay Interface Statistics Fields (continued)

Field	Description
Trusted Server Messages With Option-82	The number of messages received on a trusted interface from a DHCP server that contained Option 82 data. These messages are forwarded.
Untrusted Client Messages With Option-82	The number of messages received on a trusted interface from a DHCP client that contained Option 82 data. These messages are forwarded.
Clear (Button)	To reset the statistics to zero for one or more interfaces, select each interface with the data to reset and click Clear. You must confirm the action before the entry is deleted.

Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP Snooping IP Source Guard Interface Configuration

Use this page to configure IP Source Guard (IPSG) on each interface. IPSG is a security feature that filters IP packets based on source ID. This feature helps protect the network from attacks that use IP address spoofing to compromise or overwhelm the network. The source ID may be either the source IP address or a {source IP address, source MAC address} pair. The DHCP snooping bindings database, along with IPSG entries in the database, identify authorized source IDs. If you enable IPSG on a port where DHCP snooping is disabled or where DHCP snooping is enabled but the port is trusted, all IP traffic received on that port is dropped depending on the admin-configured IPSG entries. Additionally, IPSG interacts with port security, also known as port MAC locking, to enforce the source MAC address in received packets. Port security controls source MAC address learning in the Layer 2 forwarding database (MAC address table). When a frame is received with a previously unlearned source MAC address, port security queries the IPSG feature to determine whether the MAC address belongs to a valid binding. To change the IPSG configuration on one or more interfaces, select each entry to modify and click **Edit**. The same settings are applied to all selected interfaces.

To access the DHCP Snooping IP Source Guard Interface Configuration page, click **Switching > DHCP Snooping > IP Source Guard > Interface Configuration** in the navigation menu.

**Figure 192.** DHCP Snooping IP Source Guard Interface Configuration

Interface	IP Source Guard	Port Security
1/0/1	Disabled	Disabled
1/0/2	Disabled	Disabled
1/0/3	Disabled	Disabled
1/0/4	Disabled	Disabled
1/0/5	Disabled	Disabled
1/0/6	Disabled	Disabled
1/0/7	Disabled	Disabled
1/0/8	Disabled	Disabled
1/0/9	Disabled	Disabled
1/0/10	Disabled	Disabled

**Table 183.** DHCP Snooping IP Source Guard Interface Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the settings for one or more interfaces in the Edit DHCP Snooping IP Source Guard Interface Configuration window, this field identifies each interface that is being configured.
IP Source Guard	The administrative mode of IPSG on the interface. When enabled, the source IP address is validated against the DHCP snooping bindings database, and DHCP packets will not be forwarded if the sender's IP address is not in the DHCP snooping bindings database.
Port Security	The administrative mode of IPSG Port Security on the interface. When IPSG Port Security is enabled, the packets will not be forwarded if the sender MAC address is not the in forwarding database table or the DHCP snooping bindings database. To enforce filtering based on MAC address, Port Security must be enabled globally and on the interface. IPSG Port Security cannot be enabled if IPSG is disabled.

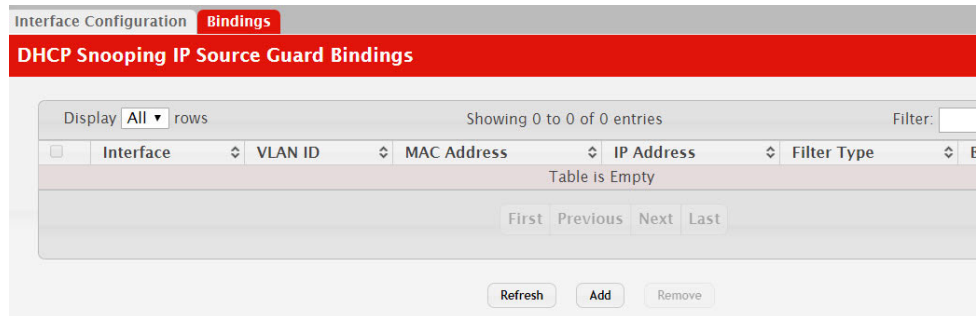
Click **Refresh** to refresh the page with the most current data from the switch.

## DHCP Snooping IP Source Guard Bindings

Use this page to view IPSG bindings in the DHCP snooping IP Source Guard bindings database and to add or remove static bindings.

To access the DHCP Snooping IP Source Guard Bindings page, click **Switching > DHCP Snooping > IP Source Guard > Bindings** in the navigation menu.

**Figure 193.** DHCP Snooping IP Source Guard Bindings



Use the buttons to perform the following tasks:

- To add a static entry to the bindings database, click **Add** and specify the desired settings.
- To remove one or more entries, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted. Only static entries are selectable.

**Table 184.** DHCP Snooping IP Source Guard Bindings Fields

Field	Description
Interface	The interface on which the sender IP address is authorized.
VLAN ID	The authorized VLAN for the binding rule.
MAC Address	The authorized sender MAC address for the binding rule.
IP Address	The authorized source IP address for the binding rule.
Filter Type	The IPSG filter type.
Binding Type	The binding type, which is either dynamically learned or statically configured by an administrator.

Click **Refresh** to refresh the page with the most current data from the switch.

## Configuring IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

A traditional Ethernet network may be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch will forward a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets will be flooded into network segments where no node has any interest in receiving the packet. While nodes will rarely incur any processing overhead to filter packets addressed to un-requested group addresses, they are unable to transmit new packets onto the shared media for the period of time that the multicast packet is flooded. The problem of wasting bandwidth is even worse when the LAN segment is not shared, for example in Full Duplex links.

Allowing switches to snoop IGMP packets is a creative effort to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments should receive packets directed to the group address.

## Global Configuration and Status

Use the IGMP Snooping Global Configuration and Status page to enable IGMP snooping on the switch and view information about the current IGMP configuration.

To access the IGMP Snooping Configuration and Status page, click **Switching > IGMP Snooping > Configuration** in the navigation menu.

**Figure 194.** IGMP Snooping Global Configuration and Status

IGMP Snooping Global Configuration and Status	
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Multicast Control Frame Count	0
Interfaces Enabled for IGMP Snooping	
VLANs Enabled for IGMP Snooping	

Submit Refresh Cancel

**Table 185.** IGMP Snooping Global Configuration and Status Fields

Field	Description
Admin Mode	Select the administrative mode for IGMP Snooping for the switch from the pull-down menu. The default is disable.
Multicast Control Frame Count	Shows the number of multicast control frames that have been processed by the CPU.
Interfaces Enabled for IGMP Snooping	Lists the interfaces currently enabled for IGMP Snooping. To enable interfaces for IGMP snooping, see “ <a href="#">Interface Configuration</a> ” on page 296.
Data Frames Forwarded by the CPU	Shows the number of data frames forwarded by the CPU.

Select **Enable** or **Disable** the **Admin Mode** field and click **Submit** to turn the feature on or off. Perform a save if you want the changes to remain in effect over a power cycle.

## Interface Configuration

Use the IGMP Snooping Interface Configuration page to configure IGMP snooping settings on specific interfaces.

To access the IGMP Snooping Interface Configuration page, click **Switching > IGMP Snooping > Interface Configuration** in the navigation menu.

**Figure 195.** IGMP Snooping Interface Configuration

Interface	Admin Mode	Group Membership Interval	Max Response Time	Multicast Router Expiration Time
1/0/1	Disable	260	10	0
1/0/2	Disable	260	10	0
1/0/3	Disable	260	10	0
1/0/4	Disable	260	10	0
1/0/5	Disable	260	10	0
1/0/6	Disable	260	10	0
1/0/7	Disable	260	10	0
1/0/8	Disable	260	10	0
1/0/9	Disable	260	10	0
1/0/10	Disable	260	10	0

**Table 186.** IGMP Snooping Interface Configuration Fields

Field	Description
Interface	Select the physical or LAG interfaces to configure.
Admin Mode	Select the interface mode for the selected interface for IGMP Snooping for the switch from the pull-down menu. The default is disable.



**Table 186.** IGMP Snooping Interface Configuration Fields (continued)

Field	Description
Group Membership Interval	Specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group. The valid range is from (2 to 3600) seconds. The default is 260 seconds.
Max Response Time	Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds. The default is 10 seconds. The configured value must be less than the Group Membership Interval.
Multicast Router Present Expiration Time	Specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite timeout; i.e., no expiration.
Fast Leave Admin Mode	Select the Fast Leave mode for the a particular interface from the pull-down menu. The default is <b>Disable</b> .

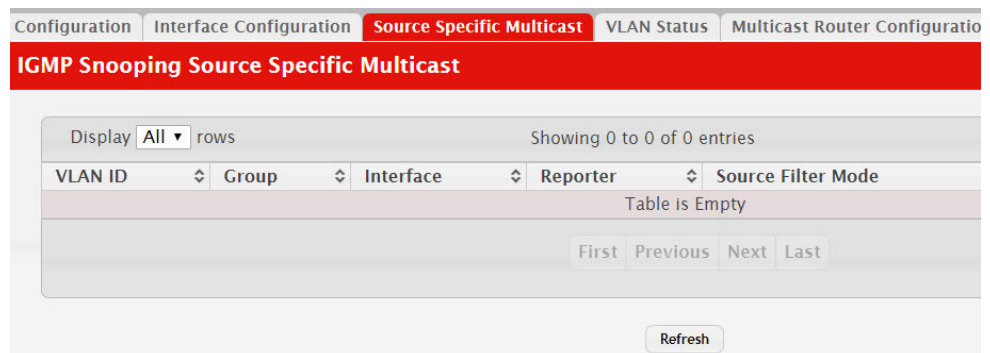
If you make any changes on the page, click **Submit** to apply the new settings to the switch.

## Source Specific Multicast

This page displays information about multicast groups discovered by snooping IGMPv3 reports.

To access the Source Specific Multicast page, click **Switching > IGMP Snooping > Source Specific Multicast** in the navigation menu.

**Figure 196.** IGMP Snooping Source Specific Multicast



**Table 187.** IGMP Snooping Source Specific Multicast Fields

Field	Description
VLAN ID	VLAN on which the IGMP v3 report is received.
Group	The IPv4 multicast group address.
Interface	The interface on which the IGMP v3 report is received.
Reporter	The IPv4 address of the host that sent the IGMPv3 report.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.

**Table 187.** IGMP Snooping Source Specific Multicast Fields (continued)

Field	Description
Source Address List	List of source IP addresses for which source filtering is requested.

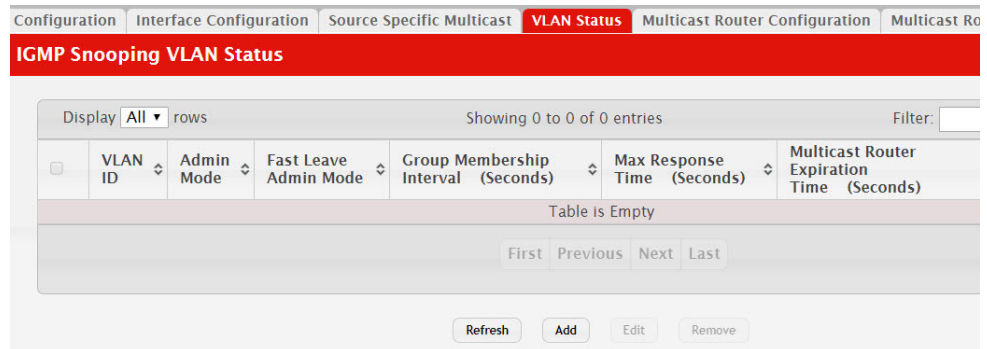
Click **Refresh** to refresh the page with the most current data from the switch.

## VLAN Status

Use this page to enable or disable IGMP snooping on system VLANs and to view and configure per-VLAN IGMP snooping settings. Only VLANs that are enabled for IGMP snooping appear in the table.

To access the VLAN Status page, click **Switching > IGMP Snooping > VLAN Status** in the navigation menu.

**Figure 197.** IGMP Snooping VLAN Status



Use the buttons to perform the following tasks:

- To enable IGMP snooping on a VLAN, click **Add** and configure the settings in the available fields.
- To change the IGMP snooping settings for an IGMP-snooping enabled VLAN, select the entry with the settings to change and click **Edit**.
- To disable IGMP snooping on one or more VLANs, select each VLAN to modify and click **Remove**. You must confirm the action before IGMP snooping is disabled on the selected VLANs. When IGMP snooping is disabled, the VLAN entry is removed from the table, but the VLAN itself still exists on the system.

**Table 188.** IGMP Snooping VLAN Status Fields

Field	Description
VLAN ID	The VLAN associated with the rest of the data in the row. When enabling IGMP snooping on a VLAN, use this menu to select the desired VLAN. Only VLANs that have been configured on the system and are not already enabled for IGMP snooping appear in the menu. When modifying IGMP snooping settings, this field identifies the VLAN that is being configured.

**Table 188.** IGMP Snooping VLAN Status Fields (continued)

Field	Description
Admin Mode	The administrative mode of IGMP snooping on the VLAN. IGMP snooping must be enabled globally and on an VLAN for the VLAN to be able to snoop IGMP packets to determine which network segments should receive multicast packets directed to the group address.
Fast Leave Admin Mode	The administrative mode of Fast Leave on the VLAN. If Fast Leave is enabled, the VLAN can be immediately removed from the layer 2 forwarding table entry upon receiving an IGMP leave message for a multicast group without first sending out MAC-based general queries.
Group Membership Interval (Seconds)	The number of seconds the VLAN should wait for a report for a particular group on the VLAN before the IGMP snooping feature deletes the VLAN from the group.
Max Response Time (Seconds)	The number of seconds the VLAN should wait after sending a query if does not receive a report for a particular group. The specified value should be less than the Group Membership Interval.
Multicast Router Expiration Time (Seconds)	The number of seconds the VLAN should wait to receive a query before it is removed from the list of VLANs with multicast routers attached.
Report Suppression Mode	The IGMPv1 and IGMPv2 report suppression mode. The device uses IGMP report suppression to limit the membership report traffic sent to multicast-capable routers. When this mode is enabled, the device does not send duplicate reports to the multicast router. Note that this mode is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports. The options are as follows: <ul style="list-style-type: none"><li>• <b>Enabled</b> – Only the first IGMP report from all hosts for a group IGMP report is forwarded to the multicast routers.</li><li>• <b>Disabled</b> – The device forwards all IGMP reports from all hosts in a multicast group to the multicast routers.</li></ul>

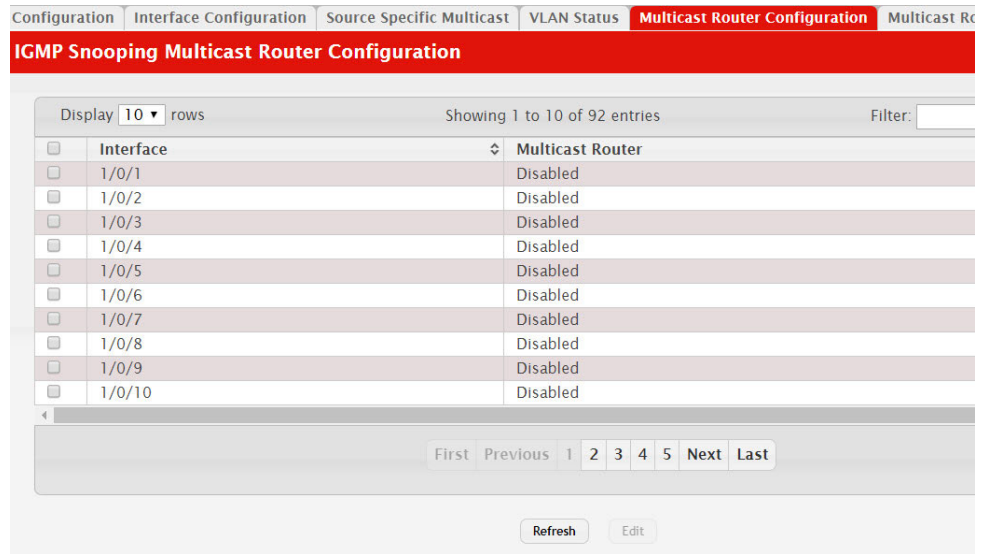
Click **Refresh** to refresh the page with the most current data from the switch.

## Multicast Router Configuration

If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure a switch port as a multicast router interface. Use the Multicast Snooping Multicast Router Configuration page to manually configure an interface as a static multicast router interface.

To access the IGMP Snooping Multicast Router Configuration page, click **Switching > IGMP Snooping > Multicast Router Configuration** in the navigation menu.

**Figure 198.** Multicast Router Configuration



**Table 189.** Multicast Router Configuration Fields

Field	Description
Interface	Select the physical or LAG interface to display.
Multicast Router	Set the multicast router status: <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The port is a multicast router interface.</li> <li>• <b>Disabled:</b> The port does not have a multicast router configured.</li> </ul>

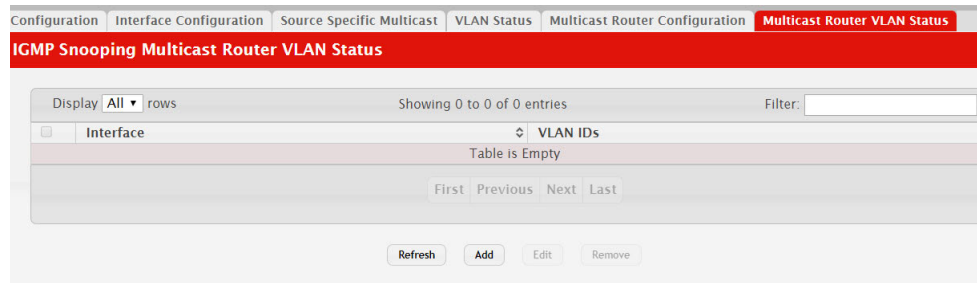
If you enable or disable multicast router configuration on an interface, click **Submit** to apply the new settings to the switch.

## Multicast Router VLAN Status

If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure one or more VLANs on each interface to act as a multicast router interface, which is an interface that faces a multicast router or IGMP querier and receives multicast traffic.

To access the Multicast Router VLAN Status page, click **Switching > IGMP Snooping > Multicast Router VLAN Status** in the navigation menu.

**Figure 199.** IGMP Snooping Multicast Router VLAN Status



**Table 190.** IGMP Snooping Multicast Router VLAN Status Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. Only interfaces that are configured with multicast router VLANs appear in the table.
VLAN IDs	The ID of the VLAN configured as enabled for multicast routing on the associated interface.

Use the buttons as follows:

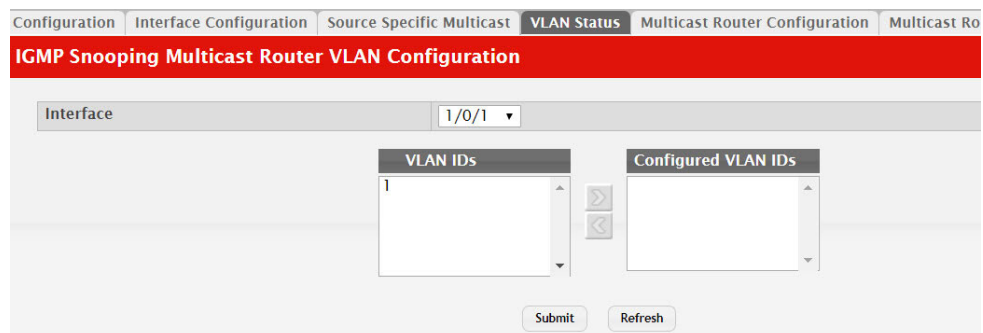
- Click **Refresh** to refresh the page with the most current data from the switch.
- To disable all VLANs as multicast router interfaces for one or more physical ports or LAGs, select each entry to modify and click **Remove**.
- To enable or disable specific VLANs as multicast router interfaces for a physical port or LAG, use the **Add** and **Edit** buttons. A multicast router interface faces a multicast router or IGMP querier and receives multicast traffic.

## Multicast Router VLAN Configuration

Use this page to enable or disable specific VLANs as multicast router interfaces for a physical port or LAG. A multicast router interface faces a multicast router or IGMP querier and receives multicast traffic.

To access the IGMP Snooping Multicast Router VLAN Configuration page, click **Switching > IGMP Snooping > Multicast Router VLAN Configuration** in the navigation menu.

**Figure 200.** IGMP Snooping Multicast Router VLAN Configuration



**Table 191.** *IGMP Snooping Multicast Router VLAN Configuration Fields*

Field	Description
Interface	Select the port or LAG on which to enable or disable a VLAN multicast routing interface.
VLAN IDs	The VLANs configured on the system that are not currently enabled as multicast router interfaces on the selected port or LAG. To enable a VLAN as a multicast router interface, click the VLAN ID to select it (or <b>CTRL</b> + click to select multiple VLAN IDs). Then, click the appropriate arrow to move the selected VLAN or VLANs to the Configured VLAN IDs window.
Configured VLAN IDs	The VLANs that are enabled as multicast router interfaces on the selected port or LAG. To disable a VLAN as a multicast router interface, click the VLAN ID to select it (or <b>CTRL</b> + click to select multiple VLAN IDs). Then, click the appropriate arrow to move the selected VLAN or VLANs to the VLAN IDs window.

Click **Refresh** to refresh the page with the most current data from the switch.

## Configuring IGMP Snooping Querier

Use this page to configure the global IGMP snooping querier settings on the device. IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP querier. When layer 3 IP multicast routing protocols are enabled in a network with IP multicast routing, the IP multicast router acts as the IGMP querier. However, if the IP-multicast traffic in a VLAN needs to be layer 2 switched only, an IP-multicast router is not required. The IGMP snooping querier can perform the IGMP snooping functions on the VLAN.

### Configuration

To access the IGMP Snooping Querier Configuration page, click **Switching > IGMP Snooping Querier > Configuration** in the navigation menu.

**Figure 201.** IGMP Snooping Querier Configuration

Configuration	VLAN Configuration	VLAN Status
<b>IGMP Snooping Querier Configuration</b>		
Admin Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
IP Address	<input type="text" value="0.0.0.0"/>	(x.x.x.x)
IGMP Version	<input type="radio"/> IGMP v1 <input checked="" type="radio"/> IGMP v2	
Query Interval (Seconds)	<input type="text" value="60"/>	(1 to 1800)
Querier Expiry Interval (Seconds)	<input type="text" value="125"/>	(60 to 300)
<input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="Cancel"/>		

**Table 192.** IGMP Snooping Querier Configuration Fields

Field	Description
Admin Mode	The administrative mode for the IGMP snooping querier on the device. When enabled, the IGMP snooping querier sends out periodic IGMP queries that trigger IGMP report messages from the switches that want to receive IP multicast traffic. The IGMP snooping feature listens to these IGMP reports to establish appropriate forwarding.
IP Address	The snooping querier address to be used as source address in periodic IGMP queries. This address is used when no IP address is configured on the VLAN on which the query is being sent.
IGMP Version	The IGMP protocol version used in periodic IGMP queries.
Query Interval (Seconds)	The amount of time the IGMP snooping querier on the device should wait between sending periodic IGMP queries.
Querier Expiry Interval (Seconds)	The amount of time the device remains in non-querier mode after it has discovered that there is a multicast querier in the network.

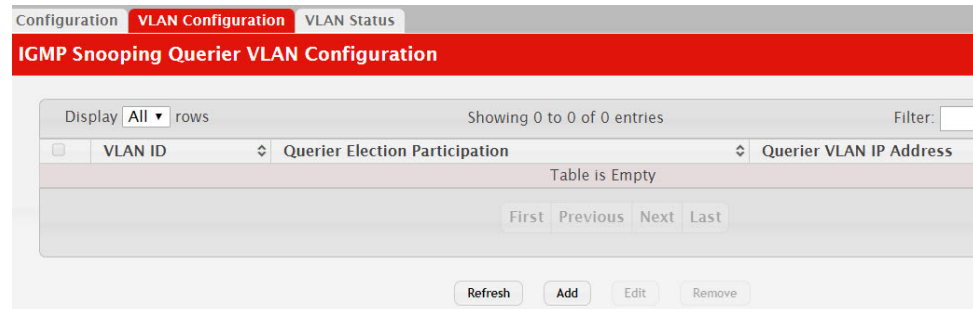
- If you make any changes to this page, click **Submit** to apply the changes to the system.
- Click **Refresh** to refresh the page with the most current data from the switch.

## VLAN Configuration

Use this page to enable the IGMP snooping querier feature on one or more VLANs and to configure per-VLAN IGMP snooping querier settings. Only VLANs that have the IGMP snooping querier feature enabled appear in the table.

To access the IGMP Snooping Querier VLAN Configuration page, click **Switching > IGMP Snooping Querier > VLAN Configuration** in the navigation menu.

**Figure 202.** IGMP Snooping Querier VLAN Configuration



Use the buttons to perform the following tasks:

- To enable the IGMP snooping querier feature on a VLAN, click **Add** and specify the desired settings.
- To change the IGMP snooping querier settings for a VLAN, select the entry to modify and click **Edit**.
- To disable the IGMP snooping querier feature on one or more VLANs, select each entry to change and click **Remove**. You must confirm the action before the entry is deleted. Clicking this button does not remove the VLAN from the system.

**Table 193.** IGMP Snooping Querier VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN on which the IGMP snooping querier is enabled. When enabling the IGMP snooping querier on a VLAN, use this menu to select the desired VLAN. Only VLANs that have been configured on the system and are not already enabled for the IGMP snooping querier appear in the menu. When modifying IGMP snooping querier settings, this field identifies the VLAN that is being configured.
Querier Election Participation	The participation mode for the IGMP snooping querier election process: <ul style="list-style-type: none"> <li>• <b>Enabled</b> – The IGMP snooping querier on this VLAN participates in the querier election process when it discovers the presence of another querier in the VLAN. If the snooping querier finds that the other querier source IP address is lower than its own address, it stops sending periodic queries. If the snooping querier wins the election (because it has the lowest IP address), then it continues sending periodic queries.</li> <li>• <b>Disabled</b> – When the IGMP snooping querier on this VLAN sees other queriers of the same version in the VLAN, the snooping querier moves to the non-querier state and stops sending periodic queries.</li> </ul>



**Table 193.** IGMP Snooping Querier VLAN Configuration Fields (continued)

Field	Description
Querier VLAN IP Address	The IGMP snooping querier address the VLAN uses as the source IP address in periodic IGMP queries sent on the VLAN. If this value is not configured, the VLAN uses the global IGMP snooping querier IP address.

Click **Refresh** to refresh the page with the most current data from the switch.

## VLAN Status

Use this page to view information about the IGMP snooping querier status for all VLANs that have the snooping querier enabled.

To access the IGMP Snooping Querier VLAN Status page, click **Switching > IGMP Snooping Querier > VLAN Status** in the navigation menu.

**Figure 203.** IGMP Snooping Querier VLAN Status

**Table 194.** IGMP Snooping Querier VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN associated with the rest of the data in the row. The table includes only VLANs that have the snooping querier enabled.
State	The operational state of the IGMP snooping querier on the VLAN, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Querier</b> – The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode.</li> <li>• <b>Non-Querier</b> – The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode.</li> <li>• <b>Disabled</b> – The snooping querier is not operational on the VLAN. The snooping querier moves to the disabled mode when IGMP snooping is not operational on the VLAN, when the querier address is not configured, or the network management address is not configured.</li> </ul>
Version	The operational IGMP protocol version of the querier.
Last IP Address	The IP address of the last querier from which a query was snooped on the VLAN.

**Table 194.** *IGMP Snooping Querier VLAN Configuration Fields (continued)*

Field	Description
Last Version	The IGMP protocol version of the last querier from which a query was snooped on the VLAN.
Max Response Time (Seconds)	The maximum response time to be used in the queries that are sent by the snooping querier.

Click **Refresh** to refresh the page with the most current data from the switch.

# Configuring MLD Snooping

Use this page to enable Multicast Listener Discovery (MLD) snooping on the device and to view global status information. In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6 networks, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports intended to receive the data (instead of being flooded to all of the ports in a VLAN). This list is constructed by snooping IPv6 multicast control packets.

## Global Configuration and Status

To access the MLD Snooping Configuration and Status page, click **Switching > MLD Snooping > Configuration** in the navigation menu.

**Figure 204.** MLD Snooping Configuration and Status

Configuration	Interface Configuration	Source Specific Multicast	VLAN Status	Multicast Router Configuration
<b>MLD Snooping Configuration and Status</b>				
MLD Snooping Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
Multicast Control Frame Count	0			
Interfaces Enabled for MLD Snooping				
VLANs Enabled for MLD Snooping				
<input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="Cancel"/>				

**Table 195.** MLD Snooping Configuration and Status Fields

Field	Description
MLD Snooping Admin Mode	The administrative mode of MLD snooping on the device.
Multicast Control Frame Count	The number of multicast control frames that have been processed by the CPU.
Interfaces Enabled for MLD Snooping	One or more interfaces on which MLD snooping is administratively enabled. MLD snooping must be enabled globally and on an interface for the interface to be able to snoop MLD packets to determine which segments should receive multicast packets directed to the group address.
VLANs Enabled for MLD Snooping	One or more VLANs on which MLD snooping is administratively enabled.

Select **Enable** or **Disable** for the **MLD Snooping Admin Mode** field and click **Submit** to turn the feature on or off. Perform a save if you want the changes to remain in effect over a power cycle.

## Interface Configuration

Use this page to configure MLD snooping settings on specific interfaces. To configure the settings for one or more interfaces, select each entry to modify and click **Edit**. The same MLD snooping settings are applied to all selected interfaces.

To access the MLD Snooping Interface Configuration page, click **Switching > MLD Snooping > Interface Configuration** in the navigation menu.

**Figure 205.** MLD Snooping Interface Configuration

Interface	Admin Mode	Group Membership Interval	Max Response Time	Multicast Router Expiration Time	Fast Leave Admin Mode
1/0/1	Disabled	260	10	0	Disabled
1/0/2	Disabled	260	10	0	Disabled
1/0/3	Disabled	260	10	0	Disabled
1/0/4	Disabled	260	10	0	Disabled
1/0/5	Disabled	260	10	0	Disabled
1/0/6	Disabled	260	10	0	Disabled
1/0/7	Disabled	260	10	0	Disabled
1/0/8	Disabled	260	10	0	Disabled
1/0/9	Disabled	260	10	0	Disabled
1/0/10	Disabled	260	10	0	Disabled

**Table 196.** MLD Snooping Interface Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring MLD snooping settings, this field identifies each interface that is being configured.
Admin Mode	The administrative mode of MLD snooping on the interface. MLD snooping must be enabled globally and on an interface for the interface to be able to snoop MLD packets to determine which segments should receive multicast packets directed to the group address.
Group Membership Interval	The number of seconds the interface should wait for a report for a particular group on the interface before the MLD snooping feature deletes the interface from the group.
Max Response Time	The number of seconds the interface should wait after sending a query if it does not receive a report for a particular group. The specified value should be less than the Group Membership Interval.
Multicast Router Present Expiration Time	The number of seconds the interface should wait to receive a query before it is removed from the list of interfaces with multicast routers attached.
Fast Leave Admin Mode	The administrative mode of Fast Leave on the interface. If Fast Leave is enabled, the interface can be immediately removed from the Layer 2 forwarding table entry upon receiving an MLD leave message for a multicast group without first sending out MAC-based general queries.

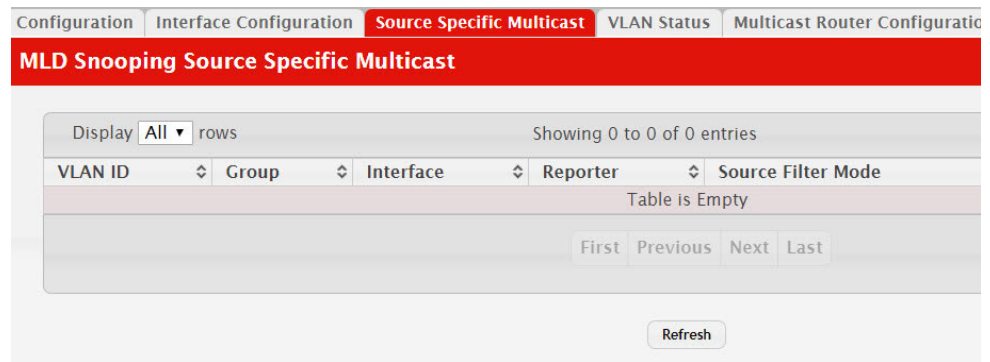
If you make any changes on the page, click **Submit** to apply the new settings to the switch.

## Source Specific Multicast

This page displays Source Specific Multicast (SSM) information learned by snooping MLDv2 reports. MLDv2 includes support for SSM, in which a receiver can request to receive multicast packets from one or more specific source address or from all addresses except one or more specified source addresses. If a host sends an MLDv2 report, the MLD snooping feature records the information and adds an entry to the table on this page.

To access the Source Specific Multicast page, click **Switching > MLD Snooping > Source Specific Multicast** in the navigation menu.

**Figure 206.** MLD Snooping Source Specific Multicast



**Table 197.** MLD Snooping Source Specific Multicast Fields

Field	Description
VLAN ID	The VLAN on which the MLDv2 report is received.
Group	The IPv6 multicast group address of the multicast group the host belongs to.
Interface	The interface on which the MLD v2 report is received.
Reporter	The IPv6 address of the host that sent the MLDv2 report.
Source Filter Mode	The source filter mode for the specified group, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Include</b> – The receiver has expressed interest in receiving multicast traffic for the multicast group from the source or sources in the Source Address List.</li> <li>• <b>Exclude</b> – The receiver has expressed interest in receiving multicast traffic for the multicast group from any source except the source or sources in the Source Address List.</li> </ul>
Source Address List	The source IPv6 address or addresses for which source filtering is requested.

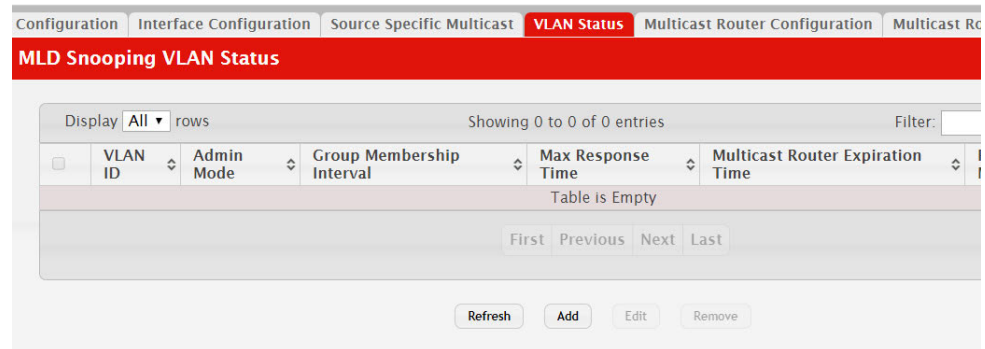
Click **Refresh** to refresh the page with the most current data from the switch.

## VLAN Status

Use this page to enable or disable MLD snooping on system VLANs and to view and configure per-VLAN MLD snooping settings. Only VLANs that are enabled for MLD snooping appear in the table.

To access the VLAN Status page, click **Switching > MLD Snooping > VLAN Status** in the navigation menu.

**Figure 207.** MLD Snooping VLAN Status



Use the buttons to perform the following tasks:

- To enable MLD snooping on a VLAN, click **Add** and configure the settings in the available fields.
- To change the MLD snooping settings for an MLD-snooping enabled VLAN, select the entry with the settings to change and click **Edit**.
- To disable MLD snooping on one or more VLANs, select each VLAN to modify and click **Remove**. You must confirm the action before MLD snooping is disabled on the selected VLANs. When MLD snooping is disabled, the VLAN entry is removed from the table, but the VLAN itself still exists on the system.

**Table 198.** MLD Snooping VLAN Status Fields

Field	Description
VLAN ID	The VLAN associated with the rest of the data in the row. When enabling MLD snooping on a VLAN, use this menu to select the desired VLAN. Only VLANs that have been configured on the system and are not already enabled for MLD snooping appear in the menu. When modifying MLD snooping settings, this field identifies the VLAN that is being configured.
Admin Mode	The administrative mode of MLD snooping on the VLAN. MLD snooping must be enabled globally and on a VLAN for the VLAN to be able to snoop MLD packets and determine which network segments should receive multicast packets directed to the group address.
Group Membership Interval	The number of seconds the VLAN should wait for a report for a particular group on the VLAN before the MLD snooping feature deletes the VLAN from the group.
Max Response Time	The number of seconds the VLAN should wait after sending a query if does not receive a report for a particular group. The specified value should be less than the Group Membership Interval.

**Table 198.** MLD Snooping VLAN Status Fields (continued)

Field	Description
Multicast Router Expiration Time	The number of seconds the VLAN should wait to receive a query before it is removed from the list of VLANs with multicast routers attached.
Fast Leave Admin Mode	The administrative mode of Fast Leave on the VLAN. If Fast Leave is enabled, the VLAN can be immediately removed from the Layer 2 forwarding table entry upon receiving an MLD leave message for a multicast group without first sending out MAC-based general queries.

Click **Refresh** to refresh the page with the most current data from the switch.

## Multicast Router Configuration

Use this page to manually configure an interface as a static MLD snooping multicast router interface. If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure an interface as a multicast router interface, which is an interface that faces a multicast router or MLD querier and receives multicast traffic.

To access the MLD Snooping Multicast Router Configuration page, click **Switching > MLD Snooping > Multicast Router Configuration** in the navigation menu.

**Figure 208.** Multicast Router Configuration

The screenshot shows the 'Multicast Router Configuration' page. At the top, there are navigation tabs: Configuration, Interface Configuration, Source Specific Multicast, VLAN Status, **Multicast Router Configuration**, and Multicast Router VLAN Status. Below the tabs is a red header with the text 'MLD Snooping Multicast Router Configuration'. The main content area has a table with the following data:

Interface	Multicast Router
1/0/1	Disabled
1/0/2	Disabled
1/0/3	Disabled
1/0/4	Disabled
1/0/5	Disabled
1/0/6	Disabled
1/0/7	Disabled
1/0/8	Disabled
1/0/9	Disabled
1/0/10	Disabled

Below the table, there are navigation buttons: First, Previous, 1, 2, 3, 4, 5, Next, Last. At the bottom, there are 'Refresh' and 'Edit' buttons.

Use the buttons to perform the following tasks:

- To change the multicast router mode for one or more interfaces, select each entry to modify and click **Edit**.

**Table 199.** Multicast Router Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the MLD snooping multicast router settings, this field identifies each interface that is being configured.

**Table 199.** *Multicast Router Configuration Fields (continued)*

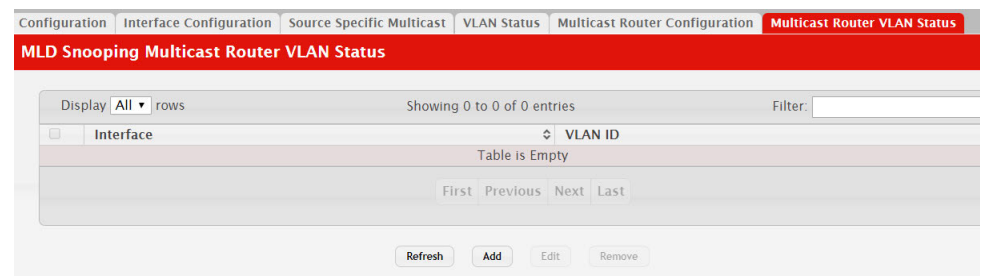
Field	Description
Multicast Router	Indicates whether the interface is enabled or disabled as a multicast router interface.

## Multicast Router VLAN Status

Use this page to enable or disable specific VLANs as static multicast router interfaces for a physical port or LAG and to view the multicast router VLAN status for each interface. A multicast router interface faces a multicast router or MLD querier and receives multicast traffic. If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure one or more VLANs on each interface to act as multicast router interfaces.

To access the Multicast Router VLAN Status page, click **Switching > MLD Snooping > Multicast Router VLAN Status** in the navigation menu.

**Figure 209.** MLD Snooping Multicast Router VLAN Status



Use the buttons to perform the following tasks:

- To enable one or more VLANs as multicast router interfaces on a port or LAG, click **Add** and configure the settings in the available fields.
- To change the VLANs that are enabled as multicast router interfaces for a port or LAG, select the entry with the settings to change and click **Edit**.
- To disable all VLAN multicast routing interfaces for a port or LAG, select each entry to modify and click **Remove**. You must confirm the action.

**Table 200.** *MLD Snooping Multicast Router VLAN Status Fields*

Field	Description
Interface	The interface associated with the rest of the data in the row. Only interfaces that are configured with multicast router VLANs appear in the table. When adding multicast router VLAN information for an interface, use the Interface menu to select the interface on which to enable one or more multicast router VLAN interfaces. When editing multicast router VLAN information, this field shows the interface that is being configured.
VLAN IDs	The ID of each VLAN configured as enabled as a multicast router interface on the associated interface. When changing the multicast routing VLAN interfaces that are associated with an interface, click the VLAN ID to select it (or <b>CTRL</b> + click to select multiple VLAN IDs).



Click **Refresh** to refresh the page with the most current data from the switch.

## Configuring MLD Snooping Querier

Use this page to configure the global MLD snooping querier settings on the device. MLD snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the MLD querier. When Layer 3 IP multicast routing protocols are enabled in a network with IP multicast routing, the IP multicast router acts as the MLD querier. However, if the IP-multicast traffic in a VLAN needs to be Layer 2 switched only, an IP-multicast router is not required. The MLD snooping querier can perform the MLD snooping functions on the VLAN.

### Configuration

To access the MLD Snooping Querier Configuration page, click **Switching > MLD Snooping Querier > Configuration** in the navigation menu.

**Figure 210.** MLD Snooping Querier Configuration

**Table 201.** MLD Snooping Querier Configuration Fields

Field	Description
Admin Mode	The administrative mode for the MLD snooping querier on the device. When enabled, the MLD snooping querier sends out periodic MLD queries that trigger MLD report messages from the switches that want to receive IP multicast traffic. The MLD snooping feature listens to these MLD reports to establish appropriate forwarding.
IPv6 Address	The snooping querier unicast link-local IPv6 address to be used as the source address in periodic MLD queries. This address is used when no IPv6 address is configured on the VLAN on which the query is being sent.
MLD Version	The MLD protocol version used in periodic MLD queries.
Query Interval (Seconds)	The amount of time the MLD snooping querier should wait between sending periodic MLD queries.
Querier Expiry Interval (Seconds)	The amount of time the device remains in non-querier mode after it has discovered that there is a multicast querier in the network.

- If you make any changes to this page, click **Submit** to apply the changes to the system.

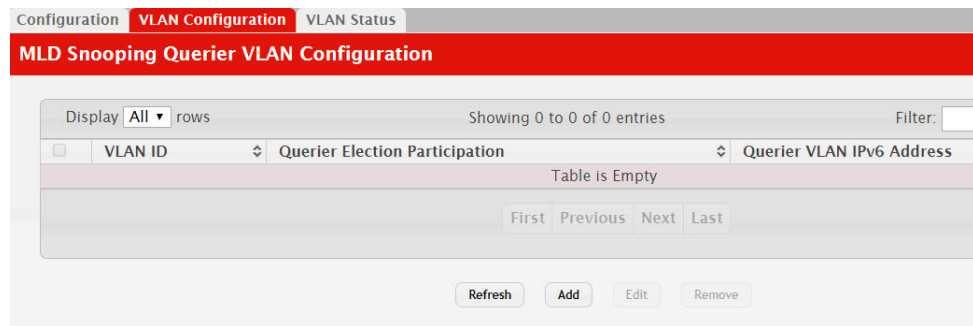
- Click **Refresh** to refresh the page with the most current data from the switch.

## VLAN Configuration

Use this page to enable the MLD snooping querier feature on one or more VLANs and to configure per-VLAN MLD snooping querier settings. Only VLANs that have the MLD snooping querier feature enabled appear in the table.

To access the MLD Snooping Querier VLAN Configuration page, click **Switching > MLD Snooping Querier > VLAN Configuration** in the navigation menu.

**Figure 211.** MLD Snooping Querier VLAN Configuration



Use the buttons to perform the following tasks:

- To enable the MLD snooping querier feature on a VLAN, click **Add** and specify the desired settings.
- To change the MLD snooping querier settings for a VLAN, select the entry to modify and click **Edit**.
- To disable the MLD snooping querier feature on one or more VLANs, select each entry to change and click **Remove**. You must confirm the action before the entry is deleted. Clicking this button does not remove the VLAN from the system.

**Table 202.** MLD Snooping Querier VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN on which the MLD snooping querier is enabled. When enabling the MLD snooping querier on a VLAN, use this menu to select the desired VLAN. Only VLANs that have been configured on the system and are not already enabled for the MLD snooping querier appear in the menu. When modifying MLD snooping querier settings, this field identifies the VLAN that is being configured.

**Table 202.** *MLD Snooping Querier VLAN Configuration Fields (continued)*

Field	Description
Querier Election Participation	The participation mode for the MLD snooping querier election process: <ul style="list-style-type: none"> <li>• <b>Enabled</b> – The MLD snooping querier on this VLAN participates in the querier election process when it discovers the presence of another querier in the VLAN. If the snooping querier finds that the other querier source IPv6 address is lower than its own address, it stops sending periodic queries. If the snooping querier wins the election (because it has the lowest IPv6 address), then it continues sending periodic queries.</li> <li>• <b>Disabled</b> – When the MLD snooping querier on this VLAN sees other queriers of the same version in the VLAN, the snooping querier moves to the non-querier state and stops sending periodic queries.</li> </ul>
Querier VLAN IPv6 Address	The MLD snooping querier unicast link-local IPv6 address the VLAN uses as the source address in periodic MLD queries sent on the VLAN. If this value is not configured, the VLAN uses the global MLD snooping querier IPv6 address.

Click **Refresh** to refresh the page with the most current data from the switch.

## VLAN Status

Use this page to view information about the MLD snooping querier status for all VLANs that have the snooping querier enabled.

To access the MLD Snooping Querier VLAN Status page, click **Switching > MLD Snooping Querier > VLAN Status** in the navigation menu.

**Figure 212.** MLD Snooping Querier VLAN Status



**Table 203.** *MLD Snooping Querier VLAN Configuration Fields*

Field	Description
VLAN ID	The VLAN associated with the rest of the data in the row. The table includes only VLANs that have the snooping querier enabled.

**Table 203.** (continued)MLD Snooping Querier VLAN Configuration Fields (continued)

Field	Description
State	The operational state of the MLD Snooping Querier on a VLAN, which is one of the following: <ul style="list-style-type: none"><li>• <b>Querier</b> – The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode.</li><li>• <b>Non-Querier</b> – The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode.</li><li>• <b>Disabled</b> – The snooping querier is not operational on the VLAN. The snooping querier moves to the disabled mode when MLD snooping is not operational on the VLAN, when the querier address is not configured, or the network management address is not configured.</li></ul>
Version	The operational MLD protocol version of the querier.
Last IPv6 Address	The IPv6 address of the last querier from which a query was snooped on the VLAN.
Last Version	The MLD protocol version of the last querier from which a query was snooped on the VLAN.
Max Response Time (Seconds)	The maximum response time to be used in the queries that are sent by the snooping querier.

Click **Refresh** to refresh the page with the most current data from the switch.

## Creating Port Channels

Port-channels, which are also known as link aggregation groups (LAGs), allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. You assign the port-channel (LAG) VLAN membership after you create a port-channel. The port channel by default becomes a member of the management VLAN.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols. A static port-channel interface does not require a partner system to be able to aggregate its member ports.

**Note:** If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LACPDU.

## Port Channel Summary

Use the Port Channel Summary page to group one or more full duplex Ethernet links to be aggregated together to form a port-channel, which is also known as a link aggregation group (LAG). The switch can treat the port-channel as if it were a single link.

To access the Port Channel Summary page, click **Switching > Port Channel > Summary** in the navigation menu.

**Figure 213.** Port Channel Summary

	Name	Type	Admin Mode	STP Mode	Link State	Link Trap	Local Preference Mode	Members	Active Ports	Load Balance
<input type="checkbox"/>	ch1	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether
<input type="checkbox"/>	ch2	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether
<input type="checkbox"/>	ch3	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether
<input type="checkbox"/>	ch4	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether
<input type="checkbox"/>	ch5	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether
<input type="checkbox"/>	ch6	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether
<input type="checkbox"/>	ch7	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether
<input type="checkbox"/>	ch8	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether
<input type="checkbox"/>	ch9	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether
<input type="checkbox"/>	ch10	Static	Enable	Enable	Down	Disable	Disable			Source/Destination MAC, VLAN, Ether

**Table 204.** Port Channel Summary Fields

Field	Description
Name	Identifies the user-configured text name of the port channel.

**Table 204.** Port Channel Summary Fields (continued)

Field	Description
Type	<p>The type of port channel:</p> <ul style="list-style-type: none"> <li>• <b>Dynamic</b> – Uses Link Aggregation Control Protocol (LACP) Protocol Data Units (PDUs) to exchange information with the link partners to help maintain the link state. To utilize Dynamic link aggregation on this port channel, the link partner must also support LACP.</li> <li>• <b>Static</b> – Does not require a partner system to be able to aggregate its member ports. When a port is added to a port channel as a static member, it neither transmits nor receives LACP PDUs.</li> </ul> <p>When configuring a port channel, use the Static Mode field to set the port channel type. If the Static Mode is disabled, the port channel type is Dynamic.</p>
Admin Mode	Select enable or disable from the pull-down menu. When the Port Channel is disabled no traffic will flow and LACPDUs will be dropped, but the links that form the Port Channel will not be released. The factory default is enable.
STP Mode	Shows whether the Spanning Tree Protocol (STP) Administrative Mode is enabled or disabled on the port channel
Link State	Indicates whether the link is Up or Down.
Link Trap	Shows whether to send traps when link status changes. If the status is Enabled, traps are sent.
Local Preference Mode	This field is only on systems that support stacking. Indicates whether the option is enabled or disabled. When this option is enabled, the LAG-destined unicast traffic egresses only out of members of the LAG interface on the local unit. This feature makes sure that the LAG-destined unicast traffic does not cross the external stack link when the LAG has members on the local unit.
Members	Lists the ports that are members of the Port Channel, in Slot/Port notation (Unit/Slot/Port for stackable systems). There can be a maximum of 8 ports assigned to a Port Channel.
Active Ports	Lists the ports that are actively participating members of this Port Channel, in Slot/Port notation (Unit/Slot/Port for stackable systems).
Load Balance	<p>The algorithm used to distribute traffic load among the physical ports of the port channel while preserving the per-flow packet order. The packet attributes the load-balancing algorithm can use to determine the outgoing physical port include the following:</p> <ul style="list-style-type: none"> <li>• Source MAC, VLAN, EtherType, Incoming Port</li> <li>• Destination MAC, VLAN, EtherType, Incoming Port</li> <li>• Source/Destination MAC, VLAN, EtherType, Incoming Port</li> <li>• Source IP and Source TCP/UDP Port Fields</li> <li>• Destination IP and Destination TCP/UDP Port Fields</li> <li>• Source/Destination IP and TCP/UDP Port Fields</li> <li>• Enhanced Hashing Mode</li> </ul>

## Port Channel Configuration

Use the Port Channel Configuration page to group one or more full duplex Ethernet links to be aggregated together to form a port-channel, which is also known as a link aggregation group (LAG). The switch treats the port-channel as if it were a single link.

To access the Port Channel Configuration page, click **Switching > Port Channel > Summary** in the navigation menu. Select a port and click **Edit**.

**Figure 214.** Port Channel Configuration

The screenshot shows the 'Edit Existing Port Channel' configuration page. The 'Port Channel Name' is set to 'ch1'. The 'Admin Mode', 'STP Mode', and 'Static Mode' are all set to 'Enable'. The 'Link Trap' is set to 'Disable'. The 'Local Preference Mode' is set to 'Disable'. The 'Load Balance' dropdown is set to 'Source/Destination MAC, VLAN, Ethertype, Incoming Port'. Below these settings are two lists: 'Port List' and 'Members'. The 'Port List' contains ports 1/0/1 through 1/0/8. The 'Members' list is currently empty. There are arrows between the lists to add or remove ports. A 'Submit' button is visible at the bottom right.

**Table 205.** Port Channel Configuration Fields

Field	Description
Port Channel Interface	Select the port channel to configure. The port channel follows a Slot/Port (or Unit/Slot/Port for stacking platforms) interface naming convention, where the slot is 3.
Port Channel Name	Enter the name you want assigned to the Port Channel. You may enter any string of up to 15 alphanumeric characters. You must specify a valid name in order to create the Port Channel.
Link Trap	Specify whether you want to have a trap sent when link status changes. The factory default is enable, which will cause the trap to be sent.
Administrative Mode	Select enable or disable from the pull-down menu. When the Port Channel is disabled no traffic will flow and LACPDU's will be dropped, but the links that form the Port Channel will not be released. The factory default is enable.
Link Status	Indicates whether the link is Up or Down.
STP Mode	Select the Spanning Tree Protocol (STP) Administrative Mode associated with the Port Channel: <ul style="list-style-type: none"> <li>• <b>Disable:</b> Spanning tree is disabled for this Port Channel.</li> <li>• <b>Enable:</b> Spanning tree is enabled for this Port Channel.</li> </ul>

**Table 205.** Port Channel Configuration Fields (continued)

Field	Description
Static Mode	Select enable or disable from the pull-down menu. The factory default is Disable. <ul style="list-style-type: none"> <li>• <b>Enable:</b> The port channel is statically maintained, which means it does not transmit or process received LAGPDUs. The member ports do not transmit LAGPDUs and all the LAG-PDUs it may receive are dropped. A static port-channel interface does not require a partner system to be able to aggregate its member ports.</li> <li>• <b>Disable:</b> The port channel is dynamically maintained. The interface transmits and processes LAGPDUs and requires a partner system.</li> </ul>
Local Preference Mode	The local preference mode for the port channel. <ul style="list-style-type: none"> <li>• <b>Enabled:</b> Known unicast traffic that is destined for a LAG egresses only out of members (if it has any) of the LAG interface on the local unit. This ensures that the LAG-destined known unicast traffic does not cross the external stack link when the LAG has members on the local unit. Unknown unicast, broadcast and multicast traffic behavior remains unchanged.</li> <li>• <b>Disabled:</b> Known unicast traffic that is destined for a LAG may egress out of any of the member ports depending upon the traffic pattern and the configured LAG hashing algorithm for the LAG interface. It is possible that this traffic may egress out of a member port on another unit. In this case, the traffic has to cross the external stacking link, which results in unnecessary bandwidth utilization of the external stack link.</li> </ul>
Load Balance	Select the hashing algorithm used to distribute the traffic load among available physical ports in the LAG. The range of possible values may vary with the type of switch. The possible values are: <ul style="list-style-type: none"> <li>• Source MAC, VLAN, EtherType, and source port</li> <li>• Destination MAC, VLAN, EtherType and source port</li> <li>• Source/Destination MAC, VLAN, EtherType, and source port</li> <li>• Source IP and Source TCP/UDP Port</li> <li>• Destination IP and Destination TCP/UDP Port</li> <li>• Source/Destination IP and source/destination TCP/UDP Port</li> <li>• Enhanced hashing mode</li> </ul>
Port Channel Members	After you create one or more port channel, this field lists the members of the Port Channel. If there are no port channels on the system, this field is not present.
Unit/Slot/Port	This column lists the physical ports available on the system.
Participation	Select each port's membership status for the Port Channel you are configuring. There can be a maximum of 8 ports assigned to a Port Channel. <ul style="list-style-type: none"> <li>• <b>Include:</b> The port participates in the port channel.</li> <li>• <b>Exclude:</b> The port does not participate in the port channel, which is the default.</li> </ul>
Membership Conflicts	Shows ports that are already members of other Port Channels. A port may only be a member of one Port Channel at a time. If the entry is blank, the port is not currently a member of any Port Channel.

- If you make any changes to this page, click **Submit** to apply the changes to the system.



- To remove a port channel, select it from the **Port Channel Name** drop-down menu and click delete. All ports that were members of this Port Channel are removed from the Port Channel and included in the default VLAN. This field will not appear when a new Port Channel is being created.

## Port Channel Statistics

This page displays the flap count for each port channel and their member ports. A flap occurs when a port-channel interface or port-channel member port goes down.

To access the Port Channel Statistics page, click **Switching > Port Channel > Statistics** in the navigation menu.

**Figure 215.** Port Channel Statistics

Interface	Channel Name	Type	Flap Count
0/3/1	ch1	Port Channel	0
0/3/2	ch2	Port Channel	0
0/3/3	ch3	Port Channel	0
0/3/4	ch4	Port Channel	0
0/3/5	ch5	Port Channel	0
0/3/6	ch6	Port Channel	0
0/3/7	ch7	Port Channel	0
0/3/8	ch8	Port Channel	0
0/3/9	ch9	Port Channel	0
0/3/10	ch10	Port Channel	0

**Table 206.** Port Channel Statistics Fields

Field	Description
Interface	The port channel or member port (physical port) associated with the rest of the data in the row.
Channel Name	The port channel name associated with the port channel. For a physical port, this field identifies the name of the port channel of which the port is a member.
Type	The interface type, which is either Port Channel (logical link-aggregation group) or Member Port (physical port).
Flap Count	The number of times the interface has gone down. The counter for a member port is incremented when the physical port is either manually shut down by the administrator or when its link state is down. When a port channel is administratively shut down, the flap counter for the port channel is incremented, but the flap counters for its member ports are not affected. When all active member ports for a port channel are inactive (either administratively down or link down), then the port channel flap counter is incremented.
Clear Counters (Button)	Click this button to reset the flap counters for all port channels and member ports to 0.

Click **Refresh** to display the latest information from the router.

## Viewing Multicast Forwarding Database Information

The Layer 2 Multicast Forwarding Database (MFDB) is used by the switch to make forwarding decisions for packets that arrive with a multicast destination MAC address. By limiting multicasts to only certain ports in the switch, traffic is prevented from going to parts of the network where that traffic is unnecessary.

When a packet enters the switch, the destination MAC address is combined with the VLAN ID and a search is performed in the Layer 2 Multicast Forwarding Database. If no match is found, the packet is either flooded to all ports in the VLAN or discarded, depending on the switch configuration. If a match is found, the packet is forwarded only to the ports that are members of that multicast group.

### MFDB Table

Use the MFDB Table page to view the port membership information for all active multicast address entries. The key for an entry consists of a VLAN ID and MAC address pair. Entries may contain data for more than one protocol.

To access the MFDB Table page, click **Switching > Multicast Forwarding Database > Summary** in the navigation menu.

**Figure 216.** MFDB Table

VLAN ID	MAC Address	Component	Type	Description	Interface(s)
Table is Empty					

**Table 207.** MFDB Summary Fields

Field	Description
MAC Address	The VLAN ID (the first two groups of hexadecimal digits) and multicast MAC address (the last six groups of hexadecimal digits) that has been added to the MFDB.
Component	The feature on the device that was responsible for adding the entry to the multicast forwarding database, which is one of the following: <ul style="list-style-type: none"><li>• <b>IGMP Snooping</b> – A layer 2 feature that allows the device to dynamically add or remove ports from IPv4 multicast groups by listening to IGMP join and leave requests.</li><li>• <b>MLD Snooping</b> – A layer 2 feature that allows the device to dynamically add or remove ports from IPv6 multicast groups by listening to MLD join and leave requests.</li><li>• <b>GMRP</b> – Generic Address Resolution Protocol (GARP) Multicast Registration Protocol, which helps help control the flooding of multicast traffic by keeping track of group membership information.</li><li>• <b>Static Filtering</b> – A static MAC filter that was manually added to the address table by an administrator.</li></ul>
Type	The type of entry, which is one of the following: <ul style="list-style-type: none"><li>• <b>Static</b> – The entry has been manually added to the MFDB by an administrator.</li><li>• <b>Dynamic</b> – The entry has been added to the MFDB as a result of a learning process or protocol.</li></ul>
Description	A text description of this multicast table entry.
Interface(s)	The list of interfaces that will forward or filter traffic sent to the multicast MAC address.
Forwarding Interface(s)	The list of forwarding interfaces. This list does not include any interfaces that are listed as static filtering interfaces.

- To search for a MAC address if the list is too long to scan, enter the MAC address in hex format and click **Search**.
- Click **Refresh** to update the information on the screen with the most current data.

## GMRP Table

Use the GMRP Table page to display the entries in the multicast forwarding database (MFDB) that were added by using the GARP Multicast Registration Protocol (GMRP).

To access the MFDB Table page, click **Switching > Multicast Forwarding Database > GMRP** in the navigation menu.

**Figure 217.** GMRP Table



**Table 208.** GMRP Fields

Field	Description
VLAN ID	The VLAN ID associated with the entry in the MFDB.
MAC Address	The multicast MAC address associated with the entry in the MFDB.
Type	The type of entry, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Static</b> – The entry has been manually added to the MFDB by an administrator.</li> <li>• <b>Dynamic</b> – The entry has been added to the MFDB as a result of a learning process or protocol. Entries that appear on this page have been added by using GARP.</li> </ul>
Description	A text description of this multicast table entry.
Interface(s)	The list of interfaces that will forward or filter traffic sent to the multicast MAC address.

- Click **Refresh** to update the information on the screen with the most current data.

## IGMP Snooping Table

This page displays the entries in the multicast forwarding database (MFDB) that were added because they were discovered by the IGMP snooping feature. IGMP snooping allows the device to dynamically add or remove ports from IPv4 multicast groups by listening to IGMP join and leave requests.

To access the MFDB Table page, click **Switching > Multicast Forwarding Database > IGMP Snooping** in the navigation menu.

**Figure 218.** IGMP Snooping Table



**Table 209.** IGMP Snooping Fields

Field	Description
VLAN ID	The VLAN ID associated with the entry in the MFDB.
MAC Address	The multicast MAC address associated with the entry in the MFDB.
Type	The type of entry, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Static</b> – The entry has been manually added to the MFDB by an administrator.</li> <li>• <b>Dynamic</b> – The entry has been added to the MFDB as a result of a learning process or protocol. Entries that appear on this page have been learned by examining IGMP messages.</li> </ul>
Description	A text description of this multicast table entry.
Interface(s)	The list of interfaces that will forward or filter traffic sent to the multicast MAC address.

- Click **Refresh** to update the information on the screen with the most current data.

## Source Specific Multicast

This page displays the entries in the multicast forwarding database (MFDB) for source specific multicast, those were added because they were discovered by the IGMP Snooping or MLD Snooping feature.

To access the MFDB Table page, click **Switching > Multicast Forwarding Database > Source Specific Multicast** in the navigation menu.

**Figure 219.** Source Specific Multicast



**Table 210.** Source Specific Multicast Fields

Field	Description
Type	Type of snooping. The values can be either IGMP Snooping or MLD Snooping.
VLAN ID	VLAN on which the entry is learned.
Group	The multicast group address.
Source	The source address.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Interface(s)	Specifies the list of interfaces on which a incoming packet is forwarded.

Click **Refresh** to update the information on the screen with the most current data.

## Source Specific Multicast Status

This page displays the entries in the multicast forwarding database (MFDB) for source specific multicast, those were added because they were discovered by the IGMP Snooping or MLD Snooping feature.

To access the MFDB Table page, click **Switching > Multicast Forwarding Database > Source Specific Multicast Status** in the navigation menu.

**Figure 220.** Source Specific Multicast Status

IGMP Snooping	
Total Entries	32
Peak Entries	0
Current Entries	0

MLD Snooping	
Total Entries	32
Peak Entries	0
Current Entries	0

**Table 211.** Source Specific Multicast Status Fields

Field	Description
IGMP Snooping	
Total Entries	The total number of entries that can possibly be in IGMP snooping's SSMFDB.
Peak Entries	The largest number of entries that have been present in the IGMP snooping's SSMFDB.
Current Entries	The current number of entries in the IGMP snooping's SSMFDB.
MLD Snooping	
Total Entries	The total number of entries that can possibly be in MLD snooping's SSMFDB.
Peak Entries	The largest number of entries that have been present in the MLD snooping's SSMFDB.
Current Entries	The current number of entries in the MLD snooping's SSMFDB.

Click **Refresh** to update the information on the screen with the most current data.

## MFDB Statistics

Use the multicast forwarding database Stats page to view statistical information about the MFDB table.

To access the Stats page, click **Switching > Multicast Forwarding Database > Statistics** in the navigation menu.

**Figure 221.** Multicast Forwarding Database Statistics

Multicast Forwarding Database Statistics	
MFDB Max Table Entries	1024
MFBD Most Entries Since Last Reset	0
MFDB Current Entries	0

**Table 212.** Multicast Forwarding Database Statistics Fields

Field	Description
MFDB Max Table Entries	The maximum number of entries that the multicast forwarding database can hold.
MFBD Most Entries Since Last Reset	The largest number of entries that have been present in the multicast forwarding database since the device was last reset. This value is also known as the MFDB high-water mark.
MFDB Current Entries	The current number of entries in the multicast forwarding database.

Click **Refresh** to update the information on the screen with the most current data.



## Multicast VLAN Registration

Multicast VLAN Registration (MVR) allows the switch to listen to the Internet Group Management Protocol (IGMP) frames. Both protocols operate independently from each other and can be enabled on the switch interfaces. In such case, MVR listens to the Join and Report messages only for the statically configured groups. All other groups are managed by IGMP snooping. MVR uses the multicast VLAN, a dedicated VLAN used to transfer multicast traffic over the network avoiding duplication of multicast streams for clients in different VLANs.

## MVR Global Configuration

Use this page to view and configure the global settings for MVR. To access the MVR Global Configuration page, click **Switching > MVR > Global**.

**Figure 222.** MVR Global Configuration

Field	Value
Admin Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MVR Mode	<input checked="" type="radio"/> Compatible <input type="radio"/> Dynamic
Multicast VLAN	1 (1 to 4093)
Maximum Multicast Groups	256
Current Multicast Groups	0
Query Response Time (Tenths of Seconds)	5 (1 to 100)

**Table 213.** MVR Global Configuration Fields

Field	Description
Admin Mode	The administrative mode of MVR on the device.
MVR Mode	The MVR learning mode, which can be one of the following: <ul style="list-style-type: none"><li>• <b>Compatible</b> – MVR does not learn source ports membership; instead, all source ports are members of all groups by default. MVR does not forward IGMP Joins and Leaves from the hosts to the router.</li><li>• <b>Dynamic</b> – MVR learns source ports membership from IGMP queries. MVR forwards the IGMP Joins and Leaves from the hosts to the router.</li></ul> The multicast traffic is forwarded only to the receiver ports that joined the group, either by IGMP Joins or MVR static configuration.
Multicast VLAN	A dedicated VLAN used to transfer multicast traffic over the network, avoiding duplication of multicast streams for clients in different VLANs.
Maximum Multicast Groups	The maximum number of membership groups that can be statically configured in the MVR database.
Current Multicast Groups	The current number of membership groups that are statically configured in the MVR database.

**Table 213.** MVR Global Configuration Fields (continued)

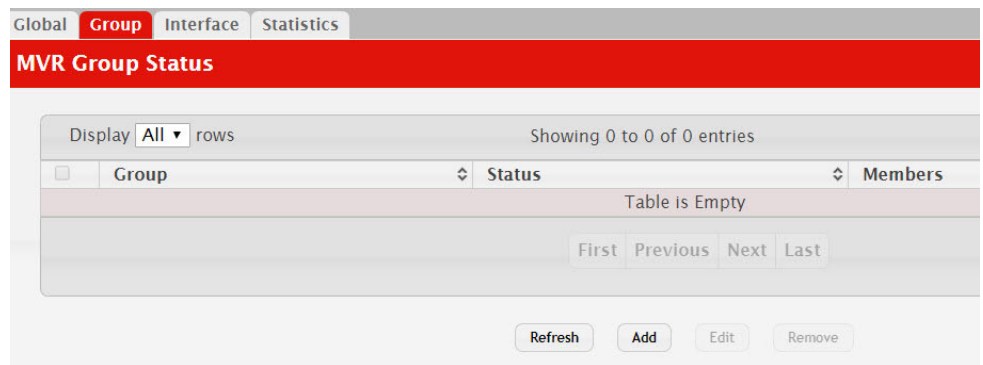
Field	Description
Query Response Time	The maximum time to wait for an IGMP membership report on a receiver port before removing the port from the multicast group. The query time is specified in tenths of a second.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Refresh** to update the information on the screen with the most current data.

## MVR Group Status

Use this page to view or configure MVR groups. MVR maintains two types of group entries in its database, Static and Dynamic. Static entries are configured by the administrator and Dynamic entries are learned by MVR on the source ports. To access the MVR Group Status page, click **Switching > MVR > Group**.

**Figure 223.** MVR Group Status



Use the buttons to perform the following tasks:

- To add a group, click **Add** and specify a group address in the available field.
- To edit a configured group, select the entry to modify and click **Edit**. Then, configure which interfaces should be members of that group.
- To remove one or more configured groups, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 214.** MVR Group Status Fields

Field	Description
Group	The multicast group address.
Status	The status of the group, which can be one of the following: <ul style="list-style-type: none"><li>• <b>Active</b> – Group has one or more MVR ports participating.</li><li>• <b>Inactive</b> – Group has no MVR ports participating.</li></ul>
Members	The list of interfaces which participate in the MVR group. In the compatible mode, all source ports are members of all groups by default.

**Table 214.** MVR Group Status Fields (continued)

Field	Description
Contiguous Group Count	This field is available in the Add Group dialog. Specify the desired number of groups to be created starting with the entered group address. The default contiguous group count is 1.
Available Interfaces	This field is available in the Edit Group Configuration dialog. The interfaces that can be added to the group. To move an interface between the Available Interfaces and Group Interfaces fields, click the interface (or <b>CTRL</b> + click to select multiple interfaces), and then click the appropriate arrow to move the selected interfaces to the desired field.
Group Interfaces	This field is available in the Edit Group Configuration dialog. The interfaces that are members of the MVR group.

Click **Refresh** to update the information on the screen with the most current data.

## MVR Interface Status

Use this page to configure MVR settings on specific interfaces. To configure the settings for one or more interfaces, select each entry to modify and click **Edit**. The same MVR settings are applied to all selected interfaces. To access the MVR Interface Status page, click **Switching > MVR > Interface**.

**Figure 224.** MVR Interface Status

Interface	MVR Interface Mode	Type	Status
1/0/1	Disabled	None	Inactive
1/0/2	Disabled	None	Inactive
1/0/3	Disabled	None	Inactive
1/0/4	Disabled	None	Inactive
1/0/5	Disabled	None	Inactive
1/0/6	Disabled	None	Inactive
1/0/7	Disabled	None	Inactive
1/0/8	Disabled	None	Inactive
1/0/9	Disabled	None	Inactive
1/0/10	Disabled	None	Inactive

**Table 215.** MVR Interface Status Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring MVR settings, this field identifies the interface(s) that are being configured.

**Table 215.** MVR Interface Status Fields (continued)

Field	Description
MVR Interface Mode	The administrative mode of MVR on the interface. MVR must be enabled globally and on an interface in order to listen to the Join and Report messages for the configured groups.
Type	The type of interface, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Source</b> – The port where multicast traffic is flowing to. It must be a member of the multicast VLAN.</li> <li>• <b>Receiver</b> – The port where listening host is connected to the switch. It must not be a member of the multicast VLAN.</li> <li>• <b>None</b> – The port is not an MVR port.</li> </ul>
Status	The active state of the interface, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Active</b> – The port has link up and is in the forwarding state.</li> <li>• <b>Inactive</b> – The port may not have link up, not be in the forwarding state, or both.</li> </ul>
Immediate Leave	The MVR immediate leave mode on the interface. It can only be configured on the receiver ports. MVR handles IGMP Leaves in Normal or Immediate leave mode. When a Leave message is received, in the normal mode a general IGMP query is sent from the switch to the receiver port, whereas in the immediate leave mode the switch is immediately reconfigured not to forward specific multicast stream to the receiver port. The immediate leave mode is used for ports where only one client may be connected.

Click **Refresh** to update the information on the screen with the most current data.

## MVR Statistics

Use this page to view statistical information about IGMP packets intercepted by MVR. To access the MVR Statistics page, click **Switching > MVR > Statistics**.

**Figure 225.** MVR Statistics

Statistics	Transmit	Rec
IGMP Queries	0	0
IGMPv1 Reports	0	0
IGMPv2 Reports	0	0
IGMP Leaves	0	0
Packet Failures	0	0

**Table 216.** MVR Statistics Fields

Field	Description
IGMP Queries	The total number of IGMP Queries successfully transmitted or received by the processor.

**Table 216.** *MVR Statistics Fields (continued)*

<b>Field</b>	<b>Description</b>
IGMPv1 Reports	The total number of IGMPv1 Reports successfully transmitted or received by the processor.
IGMPv2 Reports	The total number of IGMPv2 Reports successfully transmitted or received by the processor.
IGMP Leaves	The total number of IGMP Leaves successfully transmitted or received by the processor.
Packet Failures	The total number of packets which failed to get transmitted or received by the processor.

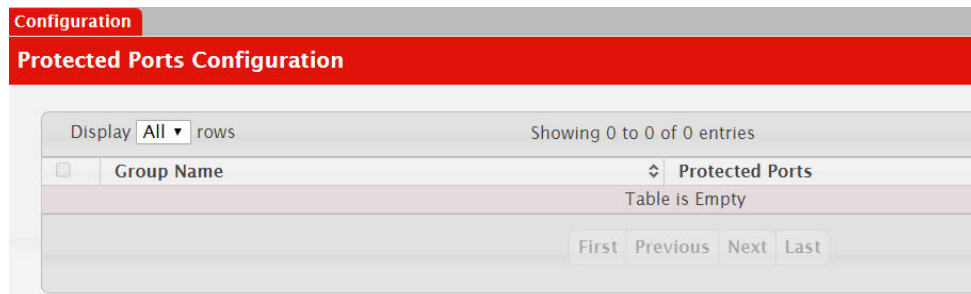
Click **Refresh** to update the information on the screen with the most current data.

## Configuring Protected Ports

Use this page to configure and view protected ports groups. A port that is a member of a protected ports group is a protected port. A port that is not a member of any protected ports group is an unprotected port. Each port can be a member of only one protected ports group. Ports in the same protected ports group cannot forward traffic to other protected ports within the group, even if they are members of the same VLAN. However, a port in a protected ports group can forward traffic to ports that are in a different protected ports group. A protected port can also forward traffic to unprotected ports. Unprotected ports can forward traffic to both protected and unprotected ports.

To access the **Protected Ports Configuration** page, click **Switching > Protected Ports > Configuration** in the navigation menu.

**Figure 226.** Protected Ports Configuration



Use the buttons to perform the following tasks:

- To create a protected ports group and add ports to the group, click **Add** and configure the settings in the available fields.
- To change the name or the port members for an existing group, select the group to update and click **Edit**.
- To remove one or more protected ports groups, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 217.** Protected Ports Configuration Fields

Field	Description
Group Name	This is the configured name of the protected ports group.
Protected Ports	The ports that are members of the protected ports group. When adding a port to a protected ports group, the Available Interfaces field lists the ports that are not already members of a protected ports group. To move an interface between the Available Interfaces and Selected Interfaces fields, click the port (or <b>CTRL</b> + click to select multiple ports), and then click the appropriate arrow to move the port(s) to the desired field.

Click **Refresh** to update the information on the screen with the most current data.

# Configuring Spanning Tree Protocol

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops. Spanning tree versions supported include Common STP, Multiple STP, and Rapid STP.

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information on configuring Common STP, see [“CST Port Configuration” on page 338](#).

Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (chief among the effects, is the rapid transitioning of the port to ‘Forwarding’). The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full duplex connectivity and ports which are connected to end stations, resulting in rapid transitioning of the port to ‘Forwarding’ state and the suppression of Topology Change Notification. These features are represented by the parameters ‘pointtopoint’ and ‘edgeport’. MSTP is compatible to both RSTP and STP. It behaves appropriately to STP and RSTP bridges. A MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge.

**Note:** For two bridges to be in the same region, the force version should be 802.1S and their configuration name, digest key, and revision level should match. For more information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

## Switch Configuration/Status

The Spanning Tree Switch Configuration/Status page contains fields for enabling STP on the switch.

To display the Spanning Tree Switch Configuration/Status page, click **Switching > Spanning Tree > Switch** in the navigation menu.

**Figure 227.** Spanning Tree Switch Configuration

Spanning Tree Switch Configuration	
Spanning Tree Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Force Protocol Version	IEEE 802.1s ▼
Configuration Name	00-13-31-12-21-56 (1 to 32 characters)
Configuration Revision Level	0 (0 to 65535)
Configuration Digest Key	0xAC36177F50283CD4883821D8AB26DE62
Configuration Format Selector	0

Submit Refresh Cancel

**Table 218.** *Spanning Tree Switch Configuration Fields*

Field	Description
Spanning Tree Admin Mode	The administrative mode of STP on the device. When enabled, the device participates in the root bridge election process and exchanges Bridge Protocol Data Units (BPDUs) with other switches in the spanning tree to determine the root path costs and maintain topology information.
Force Protocol Version	The STP version the device uses, which is one of the following: <ul style="list-style-type: none"> <li>• <b>IEEE 802.1d</b> – Classic STP provides a single path between end stations, avoiding and eliminating loops.</li> <li>• <b>IEEE 802.1w</b> – Rapid Spanning Tree Protocol (RSTP) behaves like classic STP but also has the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notifications.</li> <li>• <b>IEEE 802.1s</b> – Multiple Spanning Tree Protocol (MSTP) includes all the advantages of RSTP and also supports multiple spanning tree instances to efficiently channel VLAN traffic over different interfaces. MSTP is compatible with both RSTP and STP.</li> <li>• <b>PVST</b> – Per-VLAN Spanning Tree (PVST) maintains a spanning tree instance for each VLAN configured in the network. This is based on IEEE 802.1d standard with additional features.</li> <li>• <b>RPVST</b> – Rapid Per-VLAN Spanning Tree (RPVST) maintains a spanning tree instance for each VLAN configured in the network. This is based on IEEE 802.1w standard with additional features.</li> </ul>
Configuration Name	The name of the MSTP region. Each switch that participates in the same MSTP region must share the same Configuration Name, Configuration Revision Level, and MST-to-VLAN mappings.
Configuration Revision Level	The revision number of the MSTP region. This number must be the same on all switches that participate in the MSTP region.
Configuration Digest Key	The 16 byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID-to-MST ID mapping).
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Refresh** to update the information on the screen with the most current data.

## CST Configuration

Use the CST Configuration page to configure the Common Spanning Tree (CST) settings. The settings and information on this page define the device within the spanning tree topology that connects all STP/RSTP bridges and MSTP regions.

To display the CST Configuration page, click **Switching > Spanning Tree > CST** in the navigation menu.



**Figure 228.** Spanning Tree CST

Switch MST MST Port **CST** CST Port Statistics PVST Global PVST VLAN PVST Interface PVST Statistics

**Spanning Tree CST Configuration**

Bridge Priority	8000 (0 to F000 hex)
Bridge Max Age	20 (6 to 40)
Bridge Hello Time	2
Bridge Forward Delay	15 (4 to 30)
Spanning Tree Maximum Hops	20 (6 to 40)
BPDU Guard	<input type="checkbox"/>
BPDU Filter	<input type="checkbox"/>
Spanning Tree Tx Hold Count	6 (1 to 10)
Bridge Identifier	80:00:80:96:21:F1:01:00
Time Since Topology Change	3d:10:23:51
Topology Change Count	0
Topology Change	False
Designated Root	80:00:80:96:21:F1:01:00
Root Path Cost	0
Root Port	00:00
Max Age	20
Forward Delay	15
Hold Time	6
CST Regional Root	80:00:80:96:21:F1:01:00
CST Path Cost	0

Submit Refresh Cancel

**Table 219.** Spanning Tree CST Fields

Field	Description
Bridge Priority	The value that helps determine which bridge in the spanning tree is elected as the root bridge during STP convergence. A lower value increases the probability that the bridge becomes the root bridge.
Bridge Max Age	The amount of time a bridge waits before implementing a topological change.
Bridge Hello Time	The amount of time the root bridge waits between sending hello BPDUs.
Bridge Forward Delay	The amount of time a bridge remains in a listening and learning state before forwarding packets.
Spanning Tree Maximum Hops	The maximum number of hops a Bridge Protocol Data Unit (BPDU) is allowed to traverse within the spanning tree region before it is discarded.
BPDU Guard	When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
BPDU Filter	When enabled, this feature filters the BPDU traffic on the edge ports. When spanning tree is disabled on a port, BPDU filtering allows BPDU packets received on that port to be dropped.
Spanning Tree Tx Hold Count	The maximum number of BPDUs that a bridge is allowed to send within a hello time window.

**Table 219.** *Spanning Tree CST Fields (continued)*

Field	Description
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value and the base MAC address of the bridge. When electing the root bridge for the spanning tree, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Time Since Topology Change	The amount of time that has passed since the topology of the spanning tree has changed since the device was last reset.
Topology Change Count	The number of times the topology of the spanning tree has changed.
Topology Change	Indicates whether a topology change is in progress on any port assigned to the CST. If a change is in progress the value is True; otherwise, it is False.
Designated Root	The bridge identifier of the root bridge for the CST. The identifier is made up of the bridge priority and the base MAC address.
Root Path Cost	The path cost to the designated root for the CST. Traffic from a connected device to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Root Port	The port on the bridge with the least-cost path to the designated root for the CST.
Max Age	The amount of time a bridge waits before implementing a topological change.
Forward Delay	The forward delay value for the root port bridge.
Hold Time	The minimum amount of time between transmissions of Configuration BPDUs.
CST Regional Root	The bridge identifier of the CST regional root. The identifier is made up of the priority value and the base MAC address of the regional root bridge.
CST Path Cost	The path cost to the CST tree regional root.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Force** to force the port to send out 802.1w or 802.1D BPDUs.
- Click **Refresh** to update the screen with most recent data.

## CST Port Configuration

Use the CST Port page to view and configure the Common Spanning Tree (CST) settings for each interface on the device. To configure CST settings for an interface and to view additional information about the interface's role in the CST topology, select the interface to view or configure and click **Edit**.

To display the Spanning Tree CST Port Configuration/Status page, click **Switching > Spanning Tree > CST Port** in the navigation menu.

**Figure 229.** Spanning Tree CST Port

Interface	Port Role	Port Forwarding State	Port Priority	Port Pa
1/0/1	Disabled	Disabled	0x0080	0
1/0/2	Disabled	Disabled	0x0080	0
1/0/3	Disabled	Disabled	0x0080	0
1/0/4	Disabled	Disabled	0x0080	0
1/0/5	Disabled	Disabled	0x0080	0
1/0/6	Disabled	Disabled	0x0080	0
1/0/7	Disabled	Disabled	0x0080	0
1/0/8	Disabled	Disabled	0x0080	0
1/0/9	Disabled	Disabled	0x0080	0
1/0/10	Disabled	Disabled	0x0080	0

**Table 220.** Spanning Tree CST Port Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
Port Role	The role of the port within the CST, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Root</b> – A port on the non-root bridge that has the least-cost path to the root bridge.</li> <li>• <b>Designated</b> – A port that has the least-cost path to the root bridge on its segment.</li> <li>• <b>Alternate</b> – A blocked port that has an alternate path to the root bridge.</li> <li>• <b>Backup</b> – A blocked port that has a redundant path to the same network segment as another port on the bridge.</li> <li>• <b>Master</b> – The port on a bridge within an MST instance that links the MST instance to other STP regions.</li> <li>• <b>Disabled</b> – The port is administratively disabled and is not part of the spanning tree.</li> </ul>

**Table 220.** *Spanning Tree CST Port Fields (continued)*

Field	Description
Port Forwarding State	<ul style="list-style-type: none"> <li>• <b>Blocking</b> – The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops.</li> <li>• <b>Listening</b> – The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state.</li> <li>• <b>Learning</b> – The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state.</li> <li>• <b>Forwarding</b> – The port sends and receives user traffic.</li> <li>• <b>Disabled</b> – The port is administratively disabled and is not part of the spanning tree.</li> </ul>
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost from the port to the root bridge.
Description	A user-configured description of the port. After you select an interface and click <b>Edit</b> , a window opens and allows you to edit the CST port settings and view additional CST information for the interface. The following information describes the additional fields available in the Edit CST Port Entry window.
Admin Edge Port	Select this option administratively configure the interface as an edge port. An edge port is an interface that is directly connected to a host and is not at risk of causing a loop.
Auto-calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
Hello Timer	The amount of time the port waits between sending hello BPDUs.
External Port Path Cost	The cost of the path from the port to the CIST root. This value becomes important when the network includes multiple regions.
Auto-calculate External Port Path Cost	Shows whether the path cost from the port to the CIST root is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
BPDU Flood	This option determines the behavior of the interface if STP is disabled on the port and the port receives a BPDU. If BPDU flooding is enabled, the port will flood the received BPDU to all the ports on the switch that are similarly disabled for spanning tree.
BPDU Guard Effect	Shows the status of BPDU Guard Effect on the interface. When enabled, BPDU Guard Effect can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Up Time Since Counters Last Cleared	The amount of time that the port has been up since the counters were cleared.
Port Mode	The administrative mode of spanning tree on the port.
Designated Root	The bridge ID of the root bridge for the CST.

**Table 220.** *Spanning Tree CST Port Fields (continued)*

Field	Description
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.
Topology Change Acknowledge	Indicates whether the next BPDU to be transmitted for this port will have the topology change acknowledgment flag set.
Auto Edge	When enabled, Auto Edge allows the interface to become an edge port if it does not receive any BPDUs within a given amount of time.
Edge Port	Indicates whether the interface is configured as an edge port (Enabled).
Point-to-point MAC	Indicates whether the link type for the interface is a point-to-point link.
Root Guard	When enabled, Root Guard allows the interface to discard any superior information it receives to protect the root of the device from changing. The port gets put into discarding state and does not forward any frames.
Loop Guard	When enabled, Loop Guard prevents an interface from erroneously transitioning from blocking state to forwarding when the interface stops receiving BPDUs. The port is marked as being in loop-inconsistent state. In this state, the interface does not forward frames.
TCN Guard	When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.
CST Regional Root	The bridge ID of the bridge that has been elected as the root bridge of the CST region.
CST Path Cost	The path cost from the interface to the CST regional root.
Loop Inconsistent State	Identifies whether the interface is currently in a loop inconsistent state. An interface transitions to a loop inconsistent state if loop guard is enabled and the port stops receiving BPDUs. In this state, the interface does not transmit frames.
Transitions Into LoopInconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out Of Loop-Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Cancel** to cancel the change.
- Click **Refresh** to update the screen with most recent data.

## MST Configuration

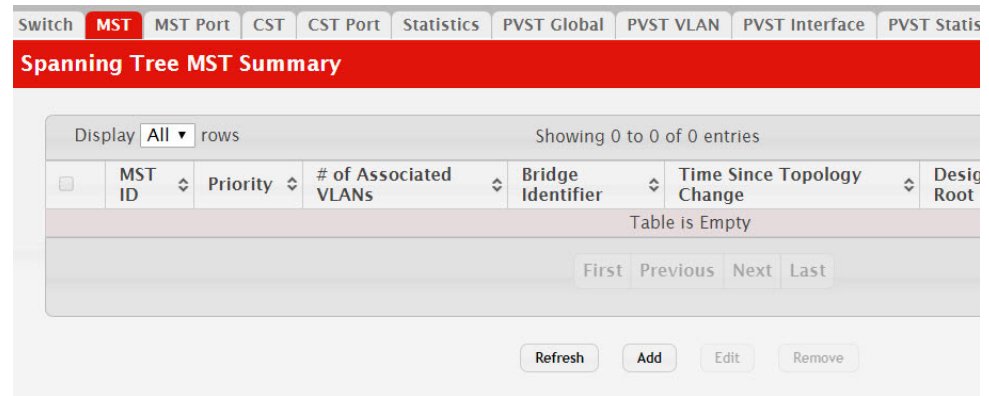
Use the MST Configuration page to view and configure the Multiple Spanning Tree Instances (MSTIs) on the device. Multiple Spanning Tree Protocol (MSTP) allows the creation of MSTIs based upon a VLAN or groups of VLANs. Configuring MSTIs creates an active topology with a better distribution of network traffic and an increase in available bandwidth when compared to classic STP.

- Use the buttons to perform the following tasks:

- To configure a new MSTI, click **Add** and specify the desired settings.
- To change the Priority or the VLAN associations for an existing MSTI, select the entry to modify and click **Edit**.
- To remove one or more MSTIs, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

To display the Spanning Tree MST Summary page, click **Switching > Spanning Tree > MST** in the navigation menu.

**Figure 230.** Spanning Tree MST Summary



**Table 221.** Spanning Tree MST Summary Fields

Field	Description
MST ID	The number that identifies the MST instance.
Priority	The bridge priority for the spanning-tree instance. This value affects the likelihood that the bridge is selected as the root bridge. A lower value increases the probability that the bridge is selected as the root bridge.
# of Associated VLANs	The number of VLANs that are mapped to the MSTI. This number does not contain any information about the VLAN IDs that are mapped to the instance.
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value of the MSTI and the base MAC address of the bridge. When electing the root bridge for an MST instance, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Time Since Topology Change	The amount of time that has passed since the topology of the MSTI has changed.
Designated Root	The bridge identifier of the root bridge for the MST instance. The identifier is made up of the bridge priority and the base MAC address.
Root Path Cost	The path cost to the designated root for this MST instance. Traffic from a connected device to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Root Port	The port on the bridge with the least-cost path to the designated root for the MST instance.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Refresh** to update the screen with most recent data.

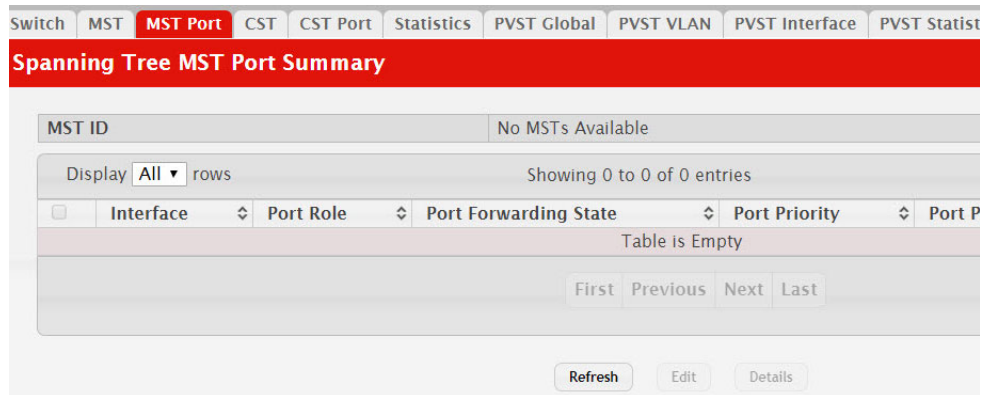
## MST Port Configuration

Use this page to view and configure the Multiple Spanning Tree (MST) settings for each interface on the device. To configure MST settings for an interface and to view additional information about the interface's role in the MST topology, first select the appropriate MST instance from the MST ID menu. Then, select the interface to view or configure and click **Edit**.

To display the Spanning Tree MST Port Summary page, click **Switching > Spanning Tree > MST Port** in the navigation menu.

**Note:** If no MST instances have been configured on the switch, the page displays a *No MSTs Available* message and does not display the fields shown in [Figure 231](#).

**Figure 231.** Spanning Tree MST Port Configuration



**Table 222.** Spanning Tree MST Port Configuration Fields

Field	Description
MST ID	The menu contains the ID of each MST instance that has been created on the device.
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring MST settings for an interface, this field identifies the interface being configured.

**Table 222.** *Spanning Tree MST Port Configuration Fields (continued)*

Field	Description
Port Role	<p>The role of the port within the MST, which is one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Root</b> – A port on the non-root bridge that has the least-cost path to the root bridge.</li> <li>• <b>Designated</b> – A port that has the least-cost path to the root bridge on its segment.</li> <li>• <b>Alternate</b> – A blocked port that has an alternate path to the root bridge.</li> <li>• <b>Backup</b> – A blocked port that has a redundant path to the same network segment as another port on the bridge.</li> <li>• <b>Master</b> – The port on a bridge within an MST instance that links the MST instance to other STP regions.</li> <li>• <b>Disabled</b> – The port is administratively disabled and is not part of the spanning tree.</li> </ul>
Port Forwarding State	<ul style="list-style-type: none"> <li>• <b>Blocking</b> – The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops.</li> <li>• <b>Listening</b> – The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state.</li> <li>• <b>Learning</b> – The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state.</li> <li>• <b>Forwarding</b> – The port sends and receives user traffic.</li> <li>• <b>Disabled</b> – The port is administratively disabled and is not part of the spanning tree.</li> </ul>
Port Priority	The priority for the port within the MSTI. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost from the port to the root bridge.
Description	A user-configured description of the port. After you select an interface and click <b>Edit</b> , a window opens and allows you to edit the MST port settings and view additional MST information for the interface. The following information describes the additional fields available in this window.
Auto-calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Up Time Since Counters Last Cleared	The amount of time that the port has been up since the counters were cleared.
Port Mode	The administrative mode of spanning tree on the port.
Designated Root	The bridge ID of the root bridge for the MST instance.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.



**Table 222.** *Spanning Tree MST Port Configuration Fields (continued)*

Field	Description
Loop Inconsistent State	Identifies whether the interface is currently in a loop inconsistent state. An interface transitions to a loop inconsistent state if loop guard is enabled and the port stops receiving BPDUs. In this state, the interface does not transmit frames.
Transitions Into LoopInconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out Of LoopInconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Refresh** to update the screen with most recent data.

## Spanning Tree Statistics

Use the Spanning Tree Statistics page to view information about the number and type of bridge protocol data units (BPDUs) transmitted and received on each port.

To display the Spanning Tree Statistics page, click **Switching > Spanning Tree > Statistics** in the navigation menu.

**Figure 232.** Spanning Tree Statistics

Interface	STP BPDUs Rx	STP BPDUs Tx	RSTP BPDUs Rx	RSTP BPDUs Tx	MSTP BPDUs Rx	MSTP BPDUs Tx
1/0/1	0	0	0	0	0	0
1/0/2	0	0	0	0	0	0
1/0/3	0	0	0	0	0	0
1/0/4	0	0	0	0	0	0
1/0/5	0	0	0	0	0	0
1/0/6	0	0	0	0	0	0
1/0/7	0	0	0	0	0	0
1/0/8	0	0	0	0	0	0
1/0/9	0	0	0	0	0	0
1/0/10	0	0	0	0	0	0

**Table 223.** *Spanning Tree Statistics Fields*

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row.

**Table 223.** *Spanning Tree Statistics Fields (continued)*

Field	Description
STP BPDUs Rx	The number of classic STP (IEEE 802.1d) BPDUs received by the interface.
STP BPDUs Tx	The number of classic STP BPDUs sent by the interface.
RSTP BPDUs Rx	The number of RSTP (IEEE 802.1w) BPDUs received by the interface.
RSTP BPDUs Tx	The number of RSTP BPDUs sent by the interface.
MSTP BPDUs Rx	The number of MSTP (IEEE 802.1s) BPDUs received by the interface.
MSTP BPDUs Tx	The number of MSTP BPDUs sent by the interface.

- Click **Refresh** to update the screen with most recent data.

## PVST Global

Use this page to view and configure Per VLAN Spanning Tree Protocol (PVSTP)/Per VLAN Rapid Spanning Tree Protocol (PVRSTP) Global settings for the device.

To display the PVST Global page, click **Switching > Spanning Tree > PVST Global** in the navigation menu.

**Figure 233.** PVST Global

**Table 224.** *PVSTP/PVRSTP Global Fields*

Field	Description
Status	PVSTP/PVRSTP configuration operational mode.
Fast Backbone	Configures Fast Backbone mode. When enabled, the switch detects the indirect link failures and accelerates the spanning tree convergence.
Fast Uplink	Configures Fast Uplink mode.
Max Update Rate (pps)	Configures Fast Uplink's Maximum Update Rate.

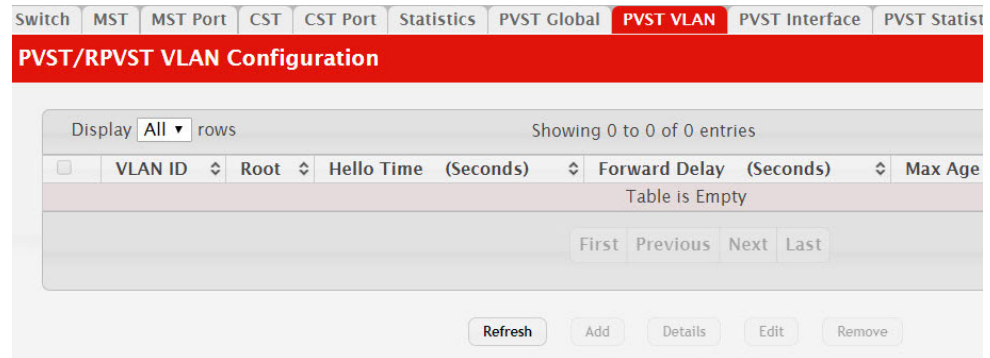
- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Refresh** to update the screen with most recent data.

## PVST VLAN

Use this page to view and configure Per VLAN Spanning Tree Protocol (PVSTP)/Per VLAN Rapid Spanning Tree Protocol (PVRSTP) VLAN settings for the device.

To display the PVST VLAN page, click **Switching > Spanning Tree > PVST VLAN** in the navigation menu.

**Figure 234.** PVST VLAN



**Table 225.** PVSTP/PVRSTP VLAN Details Fields

Field	Description
VLAN ID	The unique VLAN identifier (VID).
Root	Configures the switch to become the root bridge or standby root bridge by modifying the bridge priority to a lower value to ensure the bridge is the root (or standby) bridge.
Hello Time (Seconds)	The interval between sending successive BDPUs. Configures the spanning tree hello time interval for the specified VLAN.
Forward Delay (Seconds)	Configures the spanning tree forward delay time for a specified VLAN. This interval is the time spent in listening and learning states before transitioning a port to the forwarding states.
Max Age (Seconds)	The maximum age time before a bridge port saves its configuration information.
Bridge Priority	Configures the bridge priority of a VLAN. The value will be automatically adjusted (rounded) as needed by the system. If the value configured is not among the specified values, then it will be rounded off to the nearest valid value.
To view details of any VLAN, the entry needs to be selected and Details button need to be pressed.	
Root ID	
Priority	The root ID priority for the specified VLAN.
Address	The root ID MAC address for the specified VLAN.
Cost	The root ID cost for the specified VLAN.
Port	The root ID port for the specified VLAN.
Hello Time (Seconds)	The root ID hello time for the specified VLAN.
Max Age (Seconds)	The maximum age for the specified VLAN.

**Table 225.** PVSTP/PVRSTP VLAN Details Fields (continued)

Field	Description
Forward Delay (Seconds)	The root ID forward delay for the specified VLAN.
Bridge ID	
Priority	The bridge ID priority for the specified VLAN.
Address	The bridge ID MAC address for the specified VLAN.
Hello Time (Seconds)	The bridge ID hello time for the specified VLAN.
Max Age (Seconds)	The bridge ID maximum age for the specified VLAN.
Forward Delay (Seconds)	The bridge ID forward delay for the specified VLAN.
Aging Time (Seconds)	The bridge ID aging time for the specified VLAN.
Interface Details	
Interface	Interface which participates in the specified VLAN.
Role	The role of the interface.
Status	The status of the interface.
Cost	The cost value of the interface.
Prio.Nbr	The priority and neighbor of the interface.

**Table 226.** PVSTP/PVRSTP VLAN Add/Edit Fields

Field	Description
Root	Configures the switch to become the root bridge or standby root bridge by modifying the bridge priority to a lower value to ensure the bridge is the root (or standby) bridge.
Hello Time (Seconds)	The interval between sending successive BDPUs. Configures the spanning tree hello time interval for the specified VLAN.
Forward Delay (Seconds)	Configures the spanning tree forward delay time for a specified VLAN. This interval is the time spent in listening and learning states before transitioning a port to the forwarding states.
Max Age (Seconds)	The maximum age time before a bridge port saves its configuration information.
Bridge Priority	Configures the bridge priority of a VLAN. The value will be automatically adjusted (rounded) as needed by the system. If the value configured is not among the specified values, then it will be rounded off to the nearest valid value.

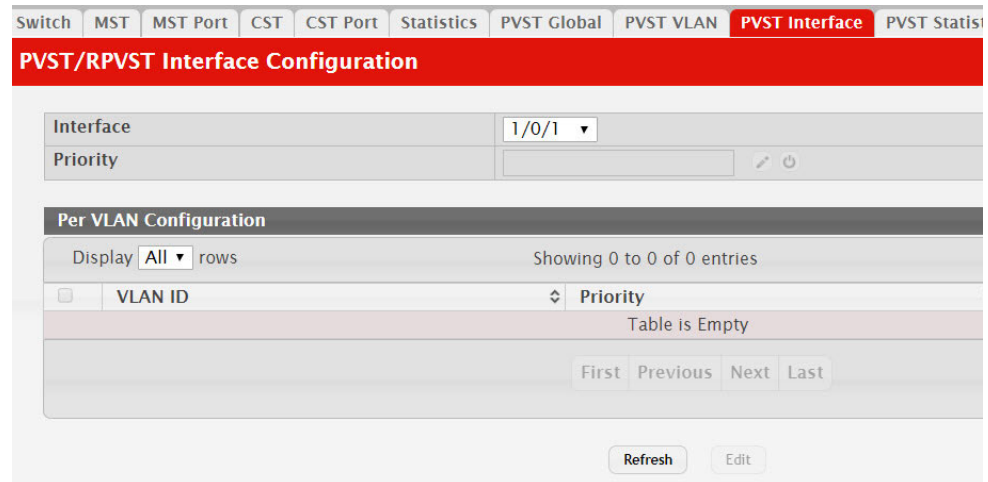
- Click **Refresh** to update the screen with most recent data.
- Click **Add** to add a new row to the VLAN configuration
- Select an entry and then click **Edit** to change the PVST configuration on the VLAN.
- Select an entry and then click **Remove** to remove the PVST row from the VLAN configuration.

## PVST Interface

Use this page to view and configure Per VLAN Spanning Tree Protocol (PVSTP)/Per VLAN Rapid Spanning Tree Protocol (PVRSTP) Interface settings for the device.

To display the PVST Interface page, click **Switching > Spanning Tree > PVST Interface** in the navigation menu.

**Figure 235.** PVST Interface



**Table 227.** PVSTP/PVRSTP Interface Fields

Field	Description
Interface	List of physical interfaces and LAGs.
Priority	The port priority configuration is used to allow the operator to select the relative importance of the port in the selection process for forwarding. Set this value to a lower number to prefer a port for forwarding of frames. This field is available for configuration only when PVSTP/PVRSTP is enabled.
Per VLAN Configuration	Configuration of each VLAN.
VLAN ID	The unique VLAN identifier (VID).
Priority	The per VLAN priority value configuration of the port is the priority used to allow the operator to select the relative importance of the port in the selection process for forwarding. Set this value to a lower number to prefer a port for forwarding of frames. This priority configuration is used when the port is configured as a point-to-point link type.
Cost	The path cost from the port to the root bridge.

**Table 228.** PVSTP/PVRSTP Interface Edit Fields

Field	Description
Interface	List of physical interfaces and LAGs.
Priority	The port priority configuration is used to allow the operator to select the relative importance of the port in the selection process for forwarding. Set this value to a lower number to prefer a port for forwarding of frames. This field is available for configuration only when PVSTP/PVRSTP is enabled.
Cost	The path cost from the port to the root bridge.

- Click **Refresh** to update the screen with most recent data.
- Select an entry and then click **Edit** to change the PVST interface configuration.

## PVST Statistics

Use this page to view and configure Per VLAN Spanning Tree Protocol (PVSTP)/Per VLAN Rapid Spanning Tree Protocol (PVRSTP) Statistics settings for the device.

To display the PVST Statistics page, click **Switching > Spanning Tree > PVST Statistics** in the navigation menu.

**Figure 236.** PVST Statistics

Switch	MST	MST Port	CST	CST Port	Statistics	PVST Global	PVST VLAN	PVST Interface	PVST Statistics
<b>PVST/RPVST Statistics</b>									
<b>Fast Backbone</b>									
Transition via Fast Backbone						0			
Inferior BPDUs Received						0			
RLQ Request PDUs Received						0			
RLQ Response PDUs Received						0			
RLQ Request PDUs Sent						0			
RLQ Response PDUs Sent						0			
<b>Fast Uplink</b>									
Fast Uplink Transitions						0			
Proxy Multicast Addresses Transmitted						0			
<input type="button" value="Refresh"/>									

**Table 229.** PVSTP/PVRSTP Statistics Fields

Field	Description
Fast Backbone	
Transition via Fast Backbone	Number of fast backbone transitions.
Inferior BPDUs Received	Number of the received inferior BPDUs.
RLQ Request PDUs Received	Number of the received RLQ request PDUs.
RLQ Response PDUs Received	Number of the received RLQ response PDUs.

**Table 229.** *PVSTP/PVRSTP Statistics Fields (continued)*

<b>Field</b>	<b>Description</b>
RLQ Request PDUs Sent	Number of the sent RLQ request PDUs.
RLQ Response PDUs Sent	Number of the sent RLQ response PDUs.
Fast Uplink	
Fast Uplink Transitions	Number of the fast uplink transitions.
Proxy Multicast Addresses Transmitted	Number of the transmitted proxy multicast addresses.

- Click **Refresh** to update the screen with most recent data.

## Mapping 802.1p Priority

The IEEE 802.1p feature allows traffic prioritization at the MAC level. The switch can prioritize traffic based on the 802.1p tag attached to the L2 frame. Each port on the switch has multiple queues to give preference to certain packets over others based on the class of service (CoS) criteria you specify. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission.

Use the 802.1p Priority Mapping page in the Class of Service folder to assign 802.1p priority values to various traffic classes on one or more interfaces.

To display the page, click **Switching > Class of Service > 802.1p** in the navigation menu.

**Figure 237.** 802.1p Priority Mapping

Interface	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 7
Global	1	0	0	1	2	2
1/0/1	1	0	0	1	2	2
1/0/2	1	0	0	1	2	2
1/0/3	1	0	0	1	2	2
1/0/4	1	0	0	1	2	2
1/0/5	1	0	0	1	2	2
1/0/6	1	0	0	1	2	2
1/0/7	1	0	0	1	2	2
1/0/8	1	0	0	1	2	2
1/0/9	1	0	0	1	2	2

**Table 230.** 802.1p Priority Mapping

Field	Description
Interface	The interface associated with the rest of the data in the row. The Global entry represents the common settings for all interfaces, unless specifically overridden individually.
Priority	The heading row lists each 802.1p priority value (0–7), and the data in the table shows which traffic class is mapped to the priority value. Incoming frames containing the designated 802.1p priority value are mapped to the corresponding traffic class in the device.
802.1p Priority	The 802.1p priority value to be mapped.



**Table 230.** *802.1p Priority Mapping (continued)*

Field	Description
Traffic Class	The internal traffic class to which the corresponding 802.1p priority value is mapped. The default value for each 802.1p priority level is displayed for reference.

---

## Configuring Port Security

Port Security can be enabled on a per-port basis. When a port is locked, only packets with allowable source MAC addresses can be forwarded. All other packets are discarded. A MAC address can be defined as allowable by one of two methods: dynamically or statically.

**Note:** Both methods are used concurrently when a port is locked.

Dynamic locking implements a *first arrival* mechanism for Port Security. You specify how many addresses can be learned on the locked port. If the limit has not been reached, a packet with an unknown source MAC address is learned and forwarded normally. Once the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. Note that you can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

To see the MAC addresses learned on a specific port, see [“Managing Logs” on page 113](#).

Disabled ports can only be activated from the **Configuring Ports** page.

## Port Security Administration

Use the Port Security Administration page to enable or disable the port security feature on your switch.

To access the Port Security Administration page, click **Switching > Port Security > Global** in the navigation menu.

**Figure 238.** Port Security Administration

Global Interface VLAN Static MAC Dynamic MAC

**Port Security Global Administration**

Port Security Admin Mode  Enable  Disable

Submit Refresh Cancel

Select **Enable** or **Disable** from the **Port Security Mode** list and click **Submit**.

## Port Security Interface Configuration

Use this page to configure the port security feature on a selected interface.

To access the Port Security Interface Configuration page, click **Switching > Port Security > Interface** in the navigation menu.

**Figure 239.** Port Security Interface Configuration

Interface	Port Security Mode	Max Dynamic Addresses Allowed	Max Static Addresses Allowed	Sticky Mode	Violation Trap Mode
<input type="checkbox"/> 1/0/1	Disable	600	40	Disable	Disable
<input type="checkbox"/> 1/0/2	Disable	600	40	Disable	Disable
<input type="checkbox"/> 1/0/3	Disable	600	40	Disable	Disable
<input type="checkbox"/> 1/0/4	Disable	600	40	Disable	Disable
<input type="checkbox"/> 1/0/5	Disable	600	40	Disable	Disable
<input type="checkbox"/> 1/0/6	Disable	600	40	Disable	Disable
<input type="checkbox"/> 1/0/7	Disable	600	40	Disable	Disable
<input type="checkbox"/> 1/0/8	Disable	600	40	Disable	Disable
<input type="checkbox"/> 1/0/9	Disable	600	40	Disable	Disable
<input type="checkbox"/> 1/0/10	Disable	600	40	Disable	Disable

**Table 231.** Port Security Interface Configuration Fields

Field	Description
Interface	Select the physical interface or the LAG on which to configure port security information.
Port Security	Determines whether port security is enabled. The default mode is Disable. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Locks the port so that only packets with allowable source MAC addresses can be forwarded. All other packets are discarded.</li> <li>• <b>Disable:</b> The port is not locked, so no port security restrictions are applied.</li> </ul>
Maximum Number of Dynamically Learned MAC Addresses Allowed	Sets the maximum number of dynamically learned MAC addresses on the selected interface. Once the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.
Maximum Number of Statically Locked MAC Addresses Allowed	Sets the maximum number of statically locked MAC addresses on the selected interface.
Add a Static MAC Address	Adds a MAC address to the list of statically locked MAC addresses for the selected interface. Only packets with an allowable source MAC address can be forwarded.
VLAN ID	Adds a corresponding VLAN ID for the MAC Address being added to the list of statically locked MAC addresses for the selected interface.
Enable Violation Traps	Enables or disables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port. Value is No by default.

**Table 231.** Port Security Interface Configuration Fields (continued)

Field	Description
Convert dynamically learned address to static locked	When you click Move, all the dynamically learned entries on this interface are added to the static MAC address list for this interface. After moving them, you can view them in the Port Security Static page.

If you make any changes to the page, click **Submit** to apply the new settings to the system.

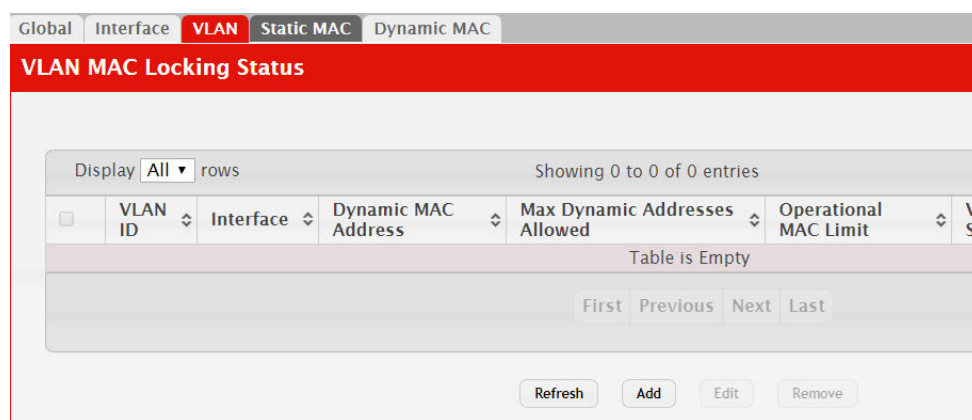
## VLAN MAC Locking

Use this page to configure VLAN MAC Locking. VLAN MAC locking allows you to secure the network by locking down allowable MAC addresses on a given VLAN. Packets with a matching source MAC address can be forwarded normally. All other packets will be discarded. VLAN MAC locking will lock the dynamic MAC entries.

If VLAN and port MAC locking are enabled, VLAN MAC locking will be given precedence over port MAC locking.

To access the VLAN MAC Locking Status page, click **Switching > Port Security > VLAN** in the navigation menu.

**Figure 240.** VLAN MAC Locking Status Configuration



**Table 232.** Port Security Interface Configuration Fields

Field	Description
VLAN ID	The VLAN ID specified in the Ethernet frame received by the interface.
Interface	The interface associated with the rest of the data in the row.
Dynamic MAC Address	The MAC address that was learned on the device. An address is dynamically learned when a frame arrives on the interface and the source MAC address in the frame is added to the MAC address table.

**Table 232.** Port Security Interface Configuration Fields (continued)

Field	Description
Max Dynamic Addresses Allowed	The number of source MAC addresses that can be dynamically learned on an interface. If an interface reaches the configured limit, any other addresses beyond that limit are not learned, and the frames are discarded. Frames with a source MAC address that has already been learned will be forwarded. A dynamically-learned MAC address is removed from the MAC address table if the entry ages out, the link goes down, or the system resets. Note that the behavior of a dynamically-learned address changes if the sticky mode for the interface is enabled or the address is converted to a static MAC address.
Operational MAC Limit	The number of source MAC addresses that are dynamically currently reached to that of Maximum Configured MAC Limit.
Violation Shutdown Mode	After MAC limit has reached, action will shut down the ports participating in the VLAN.
Violation Trap Mode	After MAC limit has reached, a log message will be generated with violation MAC address details.

To configure The VLAN MAC Locking, use the following buttons to perform the tasks:

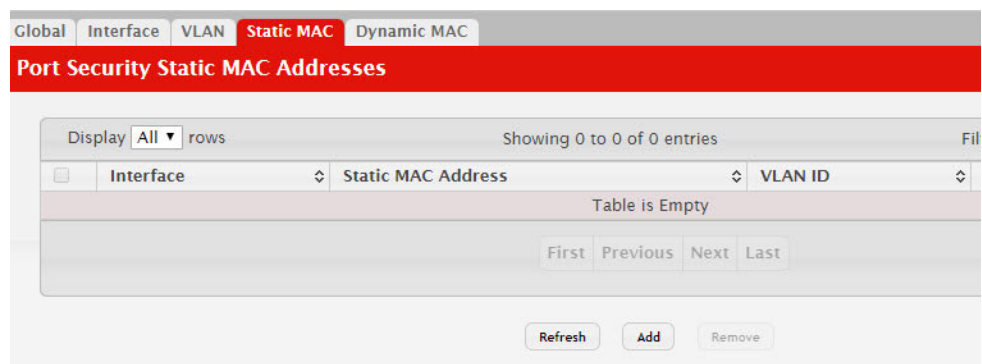
- Use **Submit** to enable or disable VLAN MAC Locking Admin Mode.
- Use **Add** to configure VLAN MAC Locking.
- Use **Edit** to modify configuration parameters of VLAN MAC Locking.
- Use **Remove** to remove configured VLANs.

## Port Security Statically Configured MAC Addresses

Use the Port Security Statically Configured MAC Addresses page to view static MAC addresses configured on an interface. From this page, you can delete statically configured MAC addresses.

To access the Port Security Static page, click **Switching > Port Security > Static MAC** in the navigation menu.

**Figure 241.** Port Security Statically Configured MAC Addresses



**Table 233.** Port Security Statically Configured MAC Address Fields

Field	Description
Interface	The interface associated with the rest of the data on the row. When adding a static MAC address, use the interface menu to select the interface to associate with the permitted MAC address.
Static MAC Address	The MAC address of the host that is allowed to forward packets on the associated interface.
VLAN ID	Displays the ID of the VLAN that includes the host with the specified MAC address.
Sticky Mode	Indicates whether the static MAC address entry is added in sticky mode. When adding a static MAC address entry, the Sticky Mode field can be selected only if it is enabled on the interface. If a static MAC address is added in sticky mode, and sticky mode is disabled on the interface, the MAC address entry is converted to a dynamic entry and will age out and be removed from the running (and saved) configuration if it is not relearned.

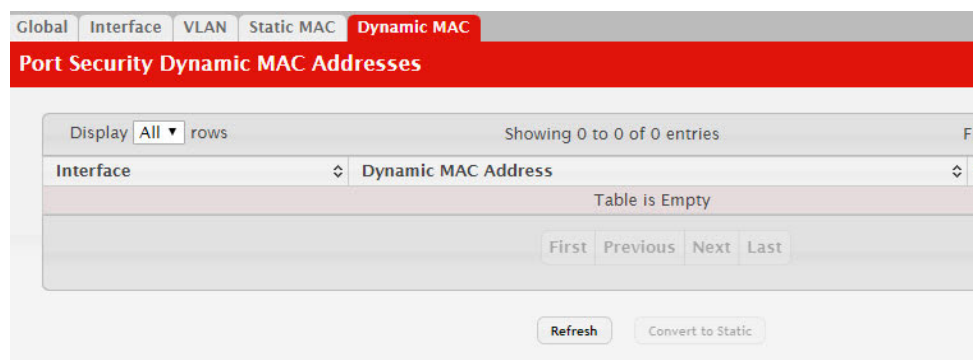
After you enter the MAC address and VLAN ID of the statically configured MAC address to delete, click **Submit** to remove the MAC address from the port and apply the new settings to the system. The screen refreshes, and the MAC address no longer appears in the table on the page.

## Port Security Dynamically Learned MAC Addresses

Use the Port Security Dynamically Learned MAC Addresses page to view a table with the dynamically learned MAC addresses on an interface. With dynamic locking, MAC addresses are learned on a *first arrival* basis. You specify how many addresses can be learned on the locked port.

To access the Port Security Dynamic page, click **Switching > Port Security > Dynamic MAC** in the navigation menu.

**Figure 242.** Port Security Dynamic MAC Address



**Table 234.** Port Security Dynamic Fields

Field	Description
Interface	Select the physical interface or the LAG on which to view the dynamically learned MAC addresses.

**Table 234.** *Port Security Dynamic Fields (continued)*

Field	Description
Dynamic MAC Address	The MAC address that was learned on the device. An address is dynamically learned when a frame arrives on the interface and the source MAC address in the frame is added to the MAC address table. The MAC addresses can be converted to static which allows them to be saved in the startup configuration.
VLAN ID	Displays the VLAN ID corresponding to the dynamically learned MAC address.
Convert to Static (Button)	Converts all MAC addresses learned on an interface to static MAC address entries. After you click the button, a window opens and allows you to select the interface associated with the MAC address entries to convert. A static MAC address entry is written to the running configuration file and does not age out.

## Managing LLDP

The IEEE 802.1AB defined standard, Link Layer Discovery Protocol (LLDP), allows stations residing on an 802 LAN to advertise major capabilities and physical descriptions. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The transmit and receive functions can be enabled/disabled separately per port. By default, both transmit and receive are disabled on all ports. The application is responsible for starting each transmit and receive state machine appropriately, based on the configured status and operational state of the port.

CE0128XB/CE0152XB allows LLDP to have multiple LLDP neighbors per interface. The number of such neighbors is limited by the memory constraints. A product-specific constant defines the maximum number of neighbors supported by the switch. There is no restriction on the number of neighbors supported on a per LLDP port. If all the remote entries on the switch are filled up, the new neighbors are ignored. In case of multiple VOIP devices on a single interface, the 802.1ab component sends the Voice VLAN configuration to all the VoIP devices.

## Global Configuration

Use the LLDP Global Configuration page to specify LLDP parameters that are applied to the switch.

To display the LLDP Global Configuration page, click **Switching > LLDP > Global** in the navigation menu.

**Figure 243.** LLDP Global Configuration

Field	Description
Transmit Interval (Seconds)	30 (5 to 32768)
Transmit Hold Multiplier (Seconds)	4 (2 to 10)
Re-Initialization Delay (Seconds)	2 (1 to 10)
Notification Interval (Seconds)	5 (5 to 3600)

**Table 235.** LLDP Global Configuration Fields

Field	Description
Transmit Interval	Specifies the interval at which LLDP frames are transmitted. The default is 30 seconds, and the valid range is 1-32768 seconds.
Transmit Hold Multiplier	Specifies multiplier on the transmit interval to assign to TTL. The default is 4, and the range is 2-10.



**Table 235.** LLDP Global Configuration Fields (continued)

Field	Description
Re-Initialization Delay	Specifies the delay before a re-initialization. The default is 2 seconds, and the range is 1-10 seconds.
Notification Interval	Limits the transmission of notifications. The default is 5 seconds, and the range is 5-3600 seconds.

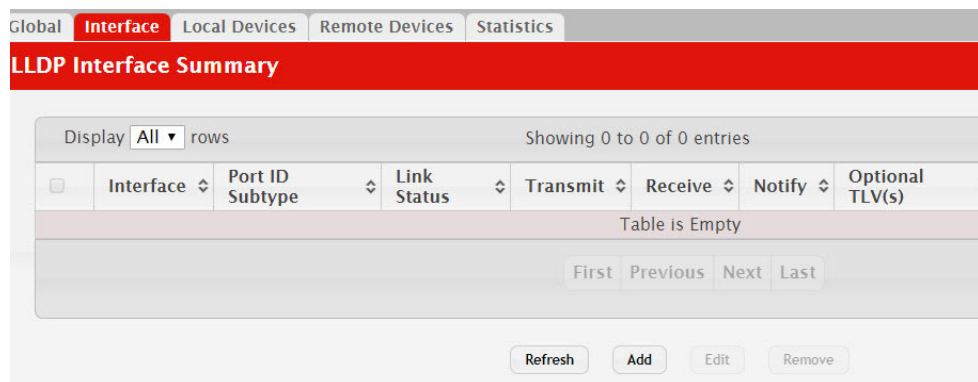
If you make any changes to the page, click **Submit** to apply the new settings to the system.

## LLDP Interface Configuration

Use the LLDP Interface Configuration page to specify LLDP parameters that are applied to a specific interface.

To display the LLDP Interface Configuration page, click **Switching > LLDP > Interface** in the navigation menu.

**Figure 244.** LLDP Interface Summary



**Note:** When adding or editing LLDP settings on an interface, select the appropriate check box to enable a feature, or clear the check box to disable a feature.

**Table 236.** LLDP Interface Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. Only interfaces that have at least one LLDP setting enabled appear in the table. In the Add LLDP Interface window, use this field to select the interface with the LLDP settings to configure. In the Edit LLDP Interface window, this field identifies the interface that is being configured.
Port ID Subtype	The LLDP Port ID subtype of the interface, which is either MAC Address or Interface Name.
Link Status	The link status of the interface, which is either Up or Down. An interface that is down does not forward traffic.
Transmit	The LLDP advertise (transmit) mode on the interface. If the transmit mode is enabled, the interface sends LLDP Data Units (LLDPDUs) that advertise the mandatory TLVs and any optional TLVs that are enabled.

**Table 236.** *LLDP Interface Summary Fields (continued)*

Field	Description
Receive	The LLDP receive mode on the interface. If the receive mode is enabled, the device can receive LLDPDUs from other devices.
Notify	The LLDP remote data change notification status on the interface. If the notify mode is enabled, the interface sends SNMP notifications when a link partner device is added or removed.
Optional TLV(s)	Select each check box next to the type-length value (TLV) information to transmit. Choices include: <ul style="list-style-type: none"> <li>• <b>System Name.</b> To include system name TLV in LLDP frames. To configure the System Name, see <a href="#">“System Description” on page 62</a>.</li> <li>• <b>System Description.</b> To include system description TLV in LLDP frames.</li> <li>• <b>System Capabilities.</b> To include system capability TLV in LLDP frames.</li> <li>• <b>Port Description.</b> To include port description TLV in LLDP frames. To configure the Port Description, see <a href="#">“Port Description” on page 139</a>.</li> </ul>
Transmit Management Information	Select the check box to enable the transmission of management address instance. Clear the check box to disable management information transmission. The default is disabled.

Use the buttons to perform the following tasks:

- To configure LLDP settings on an interface that does not have any LLDP settings enabled, click **Add**.
- To change the LLDP settings for an interface in the table, select the entry to update and click **Edit**. If you clear (disable) all LLDP settings, the entry is removed from the table.
- To clear (disable) all LLDP settings from one or more interfaces, select each entry to clear and click **Remove**.

After you click **Add** or **Edit**, a window opens and allows you to configure the LLDP settings for an interface. The following information describes the additional fields that appear in the windows used for adding or editing per-interface LLDP settings.

**Figure 245.** LLDP Interface Add

In addition to some of the fields that [Table 236, “LLDP Interface Summary Fields,”](#) on [page 361](#) describes, [Table 237](#) shows the additional fields available on the Add LLDP Interface window.

**Table 237.** LLDP Interface Add Fields

Field	Description
System Name	Select this option to include the user-configured system name in the LLDPDU the interface transmits. The system name is configured on the System Description page and is the SNMP server name for the device.
System Description	Select this option to include a description of the device in the LLDPDU the interface transmits. The description includes information about the product model and platform.
System Capabilities	Select this option to advertise the primary function(s) of the device in the LLDPDU the interface transmits.
Port Description	Select this option to include the user-configured port description in the LLDPDU the interface transmits.

If you make any changes to the page, click **Submit** to apply the new settings to the system.

## Local Devices

Use the LLDP Local Device page to view information about all interfaces on the device that are enabled to transmit LLDP information.

To display the LLDP Local Device Summary page, click **Switching > LLDP > Local Devices** in the navigation menu.

**Figure 246.** LLDP Local Devices



**Table 238.** LLDP Local Devices Columns

Field	Description
Interface	The interface associated with the rest of the LLDP - 802.1AB data in the row. When viewing the details for an interface, this field identifies the interface that is being viewed.
Port ID	The port identifier, which is the physical address associated with the interface.
Port Description	A description of the port. An administrator can configure this information on the Port Description page.

Click **Refresh** to update the information on the screen with the most current data.

After you click **Details**, a window opens and displays additional information about the data the interface transmits in its LLDPDUs. The following information describes the additional fields that appear in the LLDP Local Device Information window.

**Table 239.** LLDP Local Devices Details

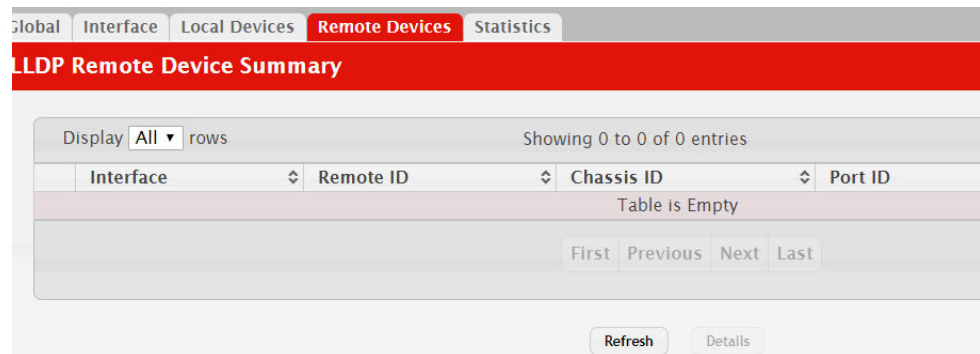
Field	Description
Chassis ID Subtype	The type of information used to identify the device in the Chassis ID field.
Chassis ID	The hardware platform identifier for the device.
Port ID Subtype	The type of information used to identify the interface in the Port ID field.
System Name	The user-configured system name for the device. The system name is configured on the System Description page and is the SNMP server name for the device.
System Description	The device description, which includes information about the product model and platform.
System Capabilities Supported	The primary function(s) the device supports.
System Capabilities Enabled	The primary function(s) the device supports that are enabled.
Management Address	The physical address associated with the management interface of the device.
Management Address Type	The protocol type or standard associated with the management address.

## Remote Devices

Use the LLDP Remote Device Summary page to view information about all interfaces on the device that are enabled to transmit LLDP information.

To display the LLDP Remote Device Summary page, click **Switching > LLDP > Remote Devices** in the navigation menu.

**Figure 247.** LLDP Remote Device Summary



**Table 240.** LLDP Remote Device Summary Columns

Field	Description
Interface	The local interface that is enabled to receive LLDPDUs from remote devices.
Remote ID	The client identifier assigned to the remote system that sent the LLDPDU.
Chassis ID	The information the remote device sent as the Chassis ID TVL. This identifies the hardware platform for the remote system.
Port ID	The port on the remote system that transmitted the LLDP data.
System Name	The system name configured on the remote device.

Click **Refresh** to update the information on the screen with the most current data.

After you click **Details**, a window opens and displays additional information. If the interface has received LLDP data from a remote device, the window displays detailed information about the device. If the interface has not received any LLDPDUs from remote devices, the window displays a message indicating that no LLDP data has been received. The following information describes the additional fields that appear in the LLDP Remote Device Information window when LLDP data has been received on the selected interface.

**Table 241.** LLDP Remote Device Summary Columns

Field	Description
Chassis ID Subtype	The type of information used to identify the device in the Chassis ID field.
Port ID Subtype	The type of information used to identify the interface in the Port ID field.
System Description	The device description, which includes information about the product model and platform.

**Table 241.** *LLDP Remote Device Summary Columns*

Field	Description
Port Description	The description of the port on the remote device that transmitted the LLDP data.
System Capabilities Supported	The primary function(s) the remote system supports. The possible capabilities include Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and Station.
System Capabilities Enabled	The primary function(s) of the remote system that are both supported and enabled. The possible capabilities include Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and Station.
Time To Live	The number of seconds the local device should consider the LLDP data it received from the remote system to be valid.

## Statistics

Use the LLDP Statistics page to view the global and interface LLDP statistics.

To display the LLDP Statistics page, click **Switching > LLDP > Statistics** in the navigation menu.

**Figure 248.** LLDP Statistics

Global	Interface	Local Devices	Remote Devices	Statistics			
<b>LLDP Statistics</b>							
Last Update	0d:00:00:00						
Total Inserts	0						
Total Deletes	0						
Total Drops	0						
Total Ageouts	0						
Display <b>All</b> rows Showing 0 to 0 of 0 entries							
Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV Unkno
Table is Empty							
<input type="button" value="First"/> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Last"/>							
<input type="button" value="Refresh"/> <input type="button" value="Clear"/>							

**Table 242.** *LLDP Statistics Fields*

Field	Description
System-wide Statistics	
Last Update	Displays the time when an entry was created, modified, or deleted in the tables associated with the remote systems.
Total Inserts	Displays the number of times a complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into the tables associated with the remote systems.
Total Deletes	Displays the number of times a complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from the tables associated with the remote systems.

**Table 242.** *LLDP Statistics Fields (continued)*

Field	Description
Total Drops	Displays the number of times a complete set of information advertised by a particular MAC Service Access Point (MSAP) could not be entered into tables associated with the remote systems because of insufficient resources.
Total Ageouts	Displays the number of times a complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with the remote systems because the information timelines interval has expired.
Port Statistics	
Interface	Identifies the interfaces.
Transmit Total	Displays the total number of LLDP frames transmitted by the LLDP agent on the corresponding port.
Receive Total	Displays the total number of valid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Discards	Displays the number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.
Errors	Displays the number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Ageouts	Displays the number of age-outs that occurred on a given port. An age-out is the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with remote entries because the information timeliness interval had expired.
TLV Discards	Displays the number of LLDP TLVs (Type, Length, Value sets) discarded for any reason by the LLDP agent on the corresponding port.
TLV Unknowns	Displays the number of LLDP TLVs received on the local ports which were not recognized by the LLDP agent on the corresponding port.
TLV MED	Displays the total number of LLDP-MED TLVs received on the local ports.
TLV 802.1	Displays the total number of LLDP TLVs received on the local ports which are of type 802.1.
TLV 802.3	Displays the total number of LLDP TLVs received on the local ports which are of type 802.3.

- Click **Refresh** to update the page with the most current information.
- Click **Clear** to clear the LLDP statistics of all the interfaces.

## LLDP-MED

The Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP that features:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and DiffServ settings), enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet endpoints.

- Inventory management, enabling network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial/asset number).

## LLDP-MED Global Configuration

Use this page to set global parameters for LLDP-MED operation. To display this page, click **Switching > LLDP-MED > Global** in the navigation menu.

**Figure 249.** LLDP-MED Global Configuration

**Table 243.** LLDP Global Configuration Fields

Field	Description
Fast Start Repeat Count	Specifies the number of LLDP PDUs that will be transmitted when the protocol is enabled. The range is from (1 to 10). The default value is 3.
Device Class	Specifies local device's MED Classification. The following three represent the actual endpoints: <ul style="list-style-type: none"> <li>• Class I Generic [IP Communication Controller etc.]</li> <li>• Class II Media [Conference Bridge etc.]</li> <li>• Class III Communication [IP Telephone etc.]</li> </ul> The fourth device is Network Connectivity Device, which is typically a LAN switch/router, IEEE 802.1 bridge, IEEE 802.11 wireless access point, etc.

Click **Submit** to update the switch. The changes take effect but will not be retained across a power cycle unless a save is performed.

## LLDP-MED Interface Configuration

Use this page to enable LLDP-MED mode on an interface and to configure its properties. To configure the settings for one or more interfaces, select each entry to modify and click **Edit**. The same LLDP-MED settings are applied to all selected interfaces.

To display this page, click **Switching > LLDP-MED > Interface** in the navigation menu.



**Figure 250.** LLDP-MED Interface Summary

Interface	Link Status	MED Status	Notification Status	Operational
1/0/1	Down	Disable	Disable	Disable
1/0/2	Down	Disable	Disable	Disable
1/0/3	Down	Disable	Disable	Disable
1/0/4	Down	Disable	Disable	Disable
1/0/5	Down	Disable	Disable	Disable
1/0/6	Down	Disable	Disable	Disable
1/0/7	Down	Disable	Disable	Disable
1/0/8	Down	Disable	Disable	Disable
1/0/9	Down	Disable	Disable	Disable
1/0/10	Down	Disable	Disable	Disable

**Table 244.** LLDP-MED Interface Configuration Fields

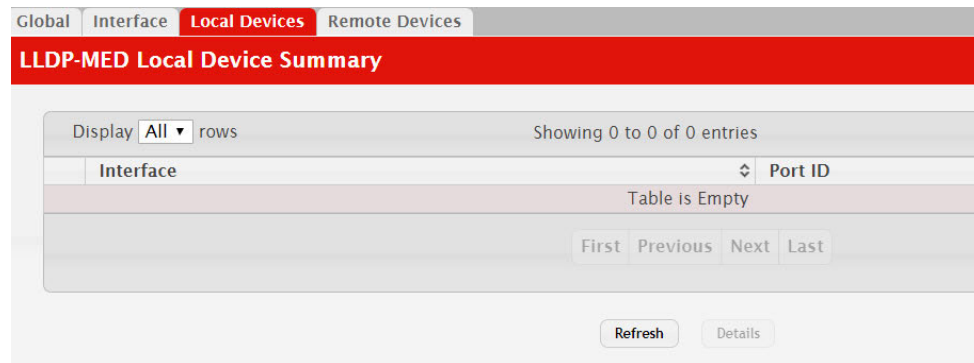
Field	Description
Interface	Selects the port that you want to configure LLDP-MED–802.1AB on. You can select <b>All</b> to configure all interfaces on the DUT with the same properties. The Interface Configuration page will not be able to display the summary of ‘All’ interfaces. The summary of individual interfaces is visible from the Interface Configuration page. The Interface Configuration page for the ‘All’ option will always display the LLDP-MED mode and notification mode as ‘disabled’ and check boxes for ‘Transmit TLVs’ will always be unchecked.
Link Status	The link status of the interface, which is either Up or Down. An interface that is down does not forward traffic.
MED Status/LLDP-MED Mode	The administrative status of LLDP-MED on the interface. When LLDP-MED is enabled, the transmit and receive function of LLDP is effectively enabled on the interface.
Notification Status/Configuration Notification Mode	Indicates whether LLDP-MED topology change notifications are enabled or disabled on the interface.
Operational Status	Indicates whether the interface will transmit TLVs.
Transmit TLVs	The LLDP-MED TLV(s) that the interface transmits: <ul style="list-style-type: none"> <li>• MED Capabilities: 0</li> <li>• Network Policy: 1</li> </ul>

Click **Submit** to send the updated configuration to the switch. These changes take effect immediately but will not be retained across a power cycle unless a save is performed.

## LLDP Local Device Information

This page displays information on LLDP-MED information advertised on the selected local interface. To display this page, click **Switching > LLDP-MED > Local Devices** in the navigation menu.

**Figure 251.** LLDP-MED Local Device Summary



**Table 245.** LLDP-MED Local Device Information Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing LLDP-MED details for an interface, this field identifies the interface that is being viewed.
Port ID	The MAC address of the interface. This is the MAC address that is advertised in LLDP-MED PDUs. After you click <b>Details</b> , a window opens and shows detailed information about the LLDP-MED information the selected interface transmits. The following information describes the additional fields that appear in the LLDP-MED Local Device Information window.
Network Policy Information The information in this table identifies the data transmitted in the Network Policy TLVs.	
Media Application Type	The media application type transmitted in the TLV. The application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, vidoesignalling. Each application type that is transmitted has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port may transmit one or many such application types. This information is displayed only when a network policy TLV has been transmitted.
VLAN ID	The VLAN ID associated with a particular policy type.
Priority	The user priority associated with a particular policy type.
DSCP	The DSCP value associated with a particular policy type.
Unknown Bit Status	The unknown bit associated with a particular policy type.
Tagged Bit Status	Identifies whether the network policy is defined for tagged or untagged VLANs.
Location Information	

**Table 245.** *LLPD-MED Local Device Information Fields (continued)*

Field	Description
Sub Type	The type of location information: <ul style="list-style-type: none"> <li>• <b>Coordinate Based</b> – The location map coordinates (latitude, longitude and altitude) of the device.</li> <li>• <b>Civic Address</b> – The civic or street address location of the device.</li> <li>• <b>ELIN</b> – The Emergency Call Service (ECS) Emergency Location Identification Number (ELIN) of the device.</li> </ul>
Information	This column displays the information related to the coordinates, civic address, and ELIN for the device.

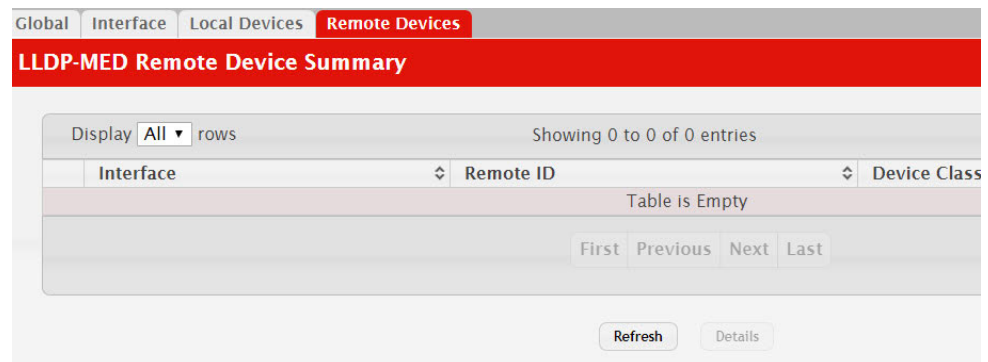
Click **Refresh** to update the page with the latest information from the router.

## LLDP-MED Remote Device Information

This page displays information about the remote devices the local system has learned about through the LLDP-MED data units received on its interfaces. Information is available about remote devices only if an interface receives an LLDP-MED data unit from a device. To view additional information about a remote device, select the interface that received the LLDP-MED data and click **Details**. The information below is organized according to the order in which the fields appear in the LLDP-MED Remote Device Information window.

To display this page, click **Switching > LLDP-MED > Remote Devices** in the navigation menu.

**Figure 252.** LLDP Remote Device Summary



**Table 246.** *LLPD-MED Remote Device Information Fields*

Field	Description
Interface	The local interface that has received LLDP-MED data units from remote devices.
Remote ID	The client identifier assigned to the remote system that sent the LLDP-MED data unit.
Capability Information	
Supported Capabilities	The supported capabilities that were received in the MED TLV on this interface.

**Table 246.** LLDP-MED Remote Device Information Fields (continued)

Field	Description
Enabled Capabilities	The supported capabilities on the remote device that are also enabled.
Device Class	The MED Classification advertised by the TLV from the remote device. The following three classifications represent the actual endpoints: <ul style="list-style-type: none"> <li>• Class I Generic (for example, IP Communication Controller)</li> <li>• Class II Media (for example, Conference Bridge)</li> <li>• Class III Communication (for example, IP Telephone)</li> </ul> The fourth device is Network Connectivity Device, which is typically a device such as a LAN switch or router, IEEE 802.1 bridge, or IEEE 802.11 wireless access point.
Network Policy Information This section describes the information in the network policy TLVs received in the LLDP-MED frames on this interface.	
Media Application Type	The media application type received in the TLV from the remote device. The application types are unknown, voicesignaling, guest-voice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, vidoesignalling. Each application type that is transmitted has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. The port on the remote device may transmit one or many such application types. This information is displayed only when a network policy TLV has been received.
VLAN ID	The VLAN ID associated with a particular policy type.
Priority	The user priority associated with a particular policy type.
DSCP	The DSCP value associated with a particular policy type.
Unknown Bit Status	The unknown bit associated with a particular policy type.
Tagged Bit Status	Identifies whether the network policy is defined for tagged or untagged VLANs.
Inventory Information This section describes the information in the inventory TLVs received in the LLDP-MED frames on this interface.	
Hardware Revision	The hardware version advertised by the remote device.
Firmware Revision	The firmware version advertised by the remote device.
Software Revision	The software version advertised by the remote device.
Serial Number	The serial number advertised by the remote device.
Manufacturer Name	The name of the system manufacturer advertised by the remote device.
Model Name	The name of the system model advertised by the remote device.
Asset ID	The system asset ID advertised by the remote device.
Location Information This section describes the information in the location TLVs received in the LLDP-MED frames on this interface.	
Sub Type	The type of location information advertised by the remote device.
Information	The text description of the location information included in the sub-type.
Extended PoE	Indicates whether the remote device is advertised as a PoE device.
Device Type	If the remote device is a PoE device, this field identifies the PoE device type of the remote device connected to this port.

Click **Refresh** to update the page with the latest information from the router.

---

## Loop Protection

L2 Loop Protection feature allows loop detection in downstream switches that do not run spanning tree. It can optionally disable the associated port on loop detection.

The Loop Protection feature is not intended for ports that serve as uplinks between spanning tree aware switches. Loop Protection feature is designed for unmanaged switches which drop spanning Tree BPDUs. This feature detects physical and logical loops between Ethernet ports on a device. The feature needs to be enabled globally before enabling it at the interface level for the system policy filter to be installed.

## Loop Protection Configuration

Use this page to configure the Loop Protection feature. Loops on a network consume resources and can impact network performance. When loop protection is enabled on the switch and on one or more interfaces (ports and trunks), the interfaces send loop protection protocol data units (PDUs) to the multicast destination address 01:80:C2:00:00:08. When an interface receives a loop protection PDU, it compares the source MAC address with its own. If the MAC addresses match, a loop is detected and a configured action is taken, which may include shutting down the port for a specified period. An interface can also be configured to receive and take action in response to loop protection PDUs, but not to send out the PDUs itself.

To display this page, click **Switching > Loop Protection > Configuration** in the navigation menu.

**Figure 253.** Loop Protection Configuration

**Configuration**

**Loop Protection Configuration**

Loop Protection	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Transmission Time (Seconds)	5 (1 to 10)
Maximum PDU Received	1 (1 to 10)

Display 10 rows Showing 1 to 10 of 92 entries Filter

<input type="checkbox"/>	Interface	Loop Protection	Action	Status	Loop	Loop Count
<input type="checkbox"/>	1/0/1	Disabled	Shutdown Port	Link Down		0
<input type="checkbox"/>	1/0/2	Disabled	Shutdown Port	Link Down		0
<input type="checkbox"/>	1/0/3	Disabled	Shutdown Port	Link Down		0
<input type="checkbox"/>	1/0/4	Disabled	Shutdown Port	Link Down		0
<input type="checkbox"/>	1/0/5	Disabled	Shutdown Port	Link Down		0
<input type="checkbox"/>	1/0/6	Disabled	Shutdown Port	Link Down		0
<input type="checkbox"/>	1/0/7	Disabled	Shutdown Port	Link Down		0
<input type="checkbox"/>	1/0/8	Disabled	Shutdown Port	Link Down		0
<input type="checkbox"/>	1/0/9	Disabled	Shutdown Port	Link Down		0
<input type="checkbox"/>	1/0/10	Disabled	Shutdown Port	Link Down		0

First Previous 1 2 3 4 5 Next Last

Submit Refresh Edit Edit All

**Table 247.** Loop Protection Configuration Fields

Field	Description
Loop Protection	Enables or disables the loop protection feature globally on the switch. <b>Note:</b> The loop protection feature is not supported on dynamic trunks. The loop protection feature will be automatically disabled if it was previously enabled on a static trunk that is now configured as dynamic.
Transmission Time (Seconds)	The interval at which the switch sends loop protection PDUs on interfaces that are enabled to send them.
Maximum PDU Received	This configures the count of loop protection packets received by the switch after which the interface will be err-disabled.
Interface	The port or trunk ID.
Action	The action to be taken when a loop is detected on the port: <ul style="list-style-type: none"> <li>• <b>Shutdown Port:</b> Shut down the port for the configured <b>Transmission Time</b>.</li> <li>• <b>Shutdown Port and Log:</b> Shut down the port for the configured <b>Transmission Time</b> and send a message to the system log.</li> <li>• <b>Log Only:</b> Send a message to the system log but do not shut down the port.</li> </ul>
Status	The current status of the interface. Link Up indicates the interface is operating normally. Link Down indicates that the port has been shut down due to the detection of a loop.
Loop	Indicates whether a loop is currently detected on the interface. If blank, then no loop is detected.
Loop Count	The number of times a loop has occurred on the interface.

**Table 247.** Loop Protection Configuration Fields

Field	Description
Time of Last Loop	The date and time the most recent loop was detected.

## Edit Loop Protection Port Configuration

Select an interface to and click **Edit** to edit the Loop Protection Port Configuration. Click **Edit All** to apply the same configuration to all interfaces.

**Figure 254.** Edit Loop Protection Port Configuration

The screenshot shows a web form titled "Edit Loop Protection Port Configuration". The form contains three rows of configuration options:

Interface	1/0/1
Loop Protection	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Action	Shutdown Port ▼

A "Submit" button is located at the bottom right of the form.

Click **Submit** to updated the switch. The changes take effect but will not be retained across a power cycle unless a save is performed.

---

## Chapter 6. Configuring Routing

CE0128XB/CE0152XB supports IP routing. Use the links in the Routing navigation menu folder to manage routing on the system.

When a packet enters the switch, the destination MAC address is checked to see if it matches any of the configured routing interfaces. If it does, then the silicon searches the host table for a matching destination IP address. If an entry is found, then the packet is routed to the host. If there is not a matching entry, then the switch performs a longest prefix match on the destination IP address. If an entry is found, then the packet is routed to the next hop. If there is no match, then the packet is routed to the next hop specified in the default route. If there is no default route configured, then the packet is passed to the 6200 series software to be handled appropriately.

The routing table can have entries added either statically by the administrator or dynamically via a routing protocol. The host table can have entries added either statically by the administrator or dynamically via ARP.



---

## Configuring ARP

The ARP protocol associates a layer 2 MAC address with a layer 3 IPv4 address. CE0128XB/CE0152XB software features both dynamic and manual ARP configuration. With manual ARP configuration, you can statically add entries into the ARP table.

ARP is a necessary part of the Internet protocol (IP) and is used to translate an IP address to a media (MAC) address, defined by a local area network (LAN) such as Ethernet. A station needing to send an IP packet must learn the MAC address of the IP destination, or of the next hop router, if the destination is not on the same subnet. This is achieved by broadcasting an ARP request packet, to which the intended recipient responds by unicasting an ARP reply containing its MAC address. Once learned, the MAC address is used in the destination address field of the layer 2 header prepended to the IP packet.

The ARP cache is a table maintained locally in each station on a network. ARP cache entries are learned by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), every recipient has the opportunity to store the sender's IP and MAC address in their respective ARP cache. The ARP response, being unicast, is normally seen only by the requester, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The number of supported ARP entries is platform-dependent.

Devices can be moved in a network, which means the IP address that was at one time associated with a certain MAC address is now found using a different MAC, or may have disappeared from the network altogether (i.e., it has been reconfigured, disconnected, or powered off). This leads to stale information in the ARP cache unless entries are updated in reaction to new information seen on the network, periodically refreshed to determine if an address still exists, or removed from the cache if the entry has not been identified as a sender of an ARP packet during the course of an ageout interval, usually specified via configuration.

### ARP Create

Use the ARP Create page to add an entry to the Address Resolution Protocol table.

To display the page, click **Routing > ARP Table > Summary** in the navigation menu.

**Figure 255.** ARP Table



The ARP Table displays at the bottom of the page, and contains the following fields:

Use the buttons to perform the following tasks:

- To add a static ARP entry, click **Add**. The Add Static ARP Entry dialog box opens. Specify the new entry information in the available fields.
- To delete one or more ARP entries, select each entry to delete and click **Remove**. Note that ARP entries designated as Local cannot be removed.

**Table 248.** ARP Create Fields

Field	Description
IP Address	The IP address of a network host on a subnet attached to one of the device's routing interfaces. When adding a static ARP entry, specify the IP address for the entry after you click <b>Add</b> .
MAC Address	The unicast MAC address (hardware address) associated with the network host. When adding a static ARP entry, specify the MAC address to associate with the IP address in the entry.
Interface	The routing interface associated with the ARP entry. The network host is associated with the device through this interface.
Type	The ARP entry type: <ul style="list-style-type: none"><li>• <b>Dynamic</b> – An ARP entry that has been learned by the router</li><li>• <b>Gateway</b> – A dynamic ARP entry that has the IP address of a routing interface</li><li>• <b>Local</b> – An ARP entry associated with the MAC address of a routing interface on the device</li><li>• <b>Static</b> – An ARP entry configured by the user</li></ul>
Age	The age of the entry since it was last learned or refreshed. This value is specified for Dynamic or Gateway entries only (it is left blank for all other entry types).

After you enter an IP address and the associated MAC address, click **Submit** to apply the changes to the system and create the entry in the ARP table.

## ARP Table Configuration

Use this page to change the configuration parameters for the Address Resolution Protocol Table. You can also use this screen to display the contents of the table.

To display the page, click **Routing > ARP Table > Configuration** in the navigation menu.

**Figure 256.** ARP Table Configuration

Field	Value	Range
Age Time (Seconds)	1200	(15 to 21600)
Response Time (Seconds)	1	(1 to 10)
Retries	4	(0 to 10)
Cache Size	512	(1216 to 512)
Dynamic Renew	<input type="checkbox"/>	

**Table 249.** ARP Table Configuration Fields

Field	Description
Age Time	The amount of time, in seconds, that a dynamic ARP entry remains in the ARP table before aging out.
Response Time	The amount of time, in seconds, that the device waits for an ARP response to an ARP request that it sends.
Retries	The maximum number of times an ARP request will be retried after an ARP response is not received. The number includes the initial ARP request.
Cache Size	The maximum number of entries allowed in the ARP table. This number includes all static and dynamic ARP entries.
Dynamic Renew	When selected, this option allows the ARP component to automatically attempt to renew dynamic ARP entries when they age out.

If you make any changes to the page, click **Submit** to apply the changes to the system.

# Configuring Global IP Settings

The **Routing > IP** folder contains links to web pages that configure and display IP routing data.

## Configuration

Use the Configuration page to configure global routing settings on the device. Routing provides a means of transmitting IP packets between subnets on the network. Routing configuration is necessary only if the device is used as a Layer 3 device that routes packets between subnets. If the device is used as a Layer 2 device that handles switching only, it typically connects to an external Layer 3 device that handles the routing functions; therefore, routing configuration is not required on the Layer 2 device.

To display the page, click **Routing > IP > Configuration** in the navigation menu.

**Figure 257.** Configuration

Field	Value	Range
Routing Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
ICMP Echo Replies	<input checked="" type="checkbox"/>	
ICMP Redirects	<input checked="" type="checkbox"/>	
ICMP Rate Limit Interval	1000	(0 to 2147483647)
ICMP Rate Limit Burst Size	100	(1 to 200)
Static Route Preference	1	(1 to 255)
Local Route Preference	0	
Maximum Next Hops	1	
Maximum Routes	512	
Global Default Gateway	<input type="text"/>	

**Table 250.** Configuration Fields

Field	Description
Routing Mode	The administrative mode of routing on the device. The options are as follows: <b>Enable</b> – The device can act as a Layer 3 device by routing packets between interfaces configured for IP routing. <b>Disable</b> – The device acts as a Layer 2 bridge and switches traffic between interfaces. The device does not perform any internet-network routing.
ICMP Echo Replies	Select <b>Enable</b> or <b>Disable</b> from the drop-down menu. If you select <b>Enable</b> , then only the router can send ECHO replies. By default, ICMP Echo Replies are sent for echo requests.
ICMP Redirects	Select this option to allow the device to send ICMP Redirect messages to hosts. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.

**Table 250.** Configuration Fields (continued)

Field	Description
ICMP Rate Limit Interval	To control the ICMP error packets, you can specify the number of ICMP error packets that are allowed per burst interval. By default, the rate limit is 100 packets per second, i.e. the burst interval is 1000 milliseconds. To disable ICMP rate limiting, set this field to zero. The valid rate interval range is 0 to 2147483647 milliseconds.
ICMP Rate Limit Burst Size	To control the ICMP error packets, you can specify the number of ICMP error packets that are allowed per burst interval. By default, the burst size is 100 packets. When the burst interval is zero, then configuring this field is not a valid option. The valid burst size range is 1 to 200.
Static Route Preference	The default distance (preference) for static routes. Lower route-distance values are preferred when determining the best route. The value configured for Static Route Preference is used when using the CLI to configure a static route and no preference is specified. Changing the Static Route Preference does not update the preference of existing static routes.
Local Route Preference	The default distance (preference) for local routes.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a read-only value.
Maximum Routes	The maximum number of routes (routing table size) supported by the switch.
Global Default Gateway	The IP address of the default gateway for the device. If the destination IP address in a packet does not match any routes in the routing table, the packet is sent to the default gateway. The gateway specified in this field is more preferred than a default gateway learned from a DHCP server. Use the icons associated with this field to perform the following tasks: <ul style="list-style-type: none"><li>• To configure the default gateway, click the Edit icon and specify the IP address of the default gateway in the available field.</li><li>• To reset the IP address of the default gateway to the factory default value, click the Reset icon associated with this field.</li></ul>

If you make any changes to the page, click **Submit** to apply the changes to the system.

## Interface Summary

This page shows summary information about the routing configuration for all interfaces. To view additional routing configuration information for an interface, select the interface with the settings to view and click **Details**.

To display the page, click **Routing > IP > Interface Summary** in the navigation menu.

**Figure 258.** Interface Summary

Interface	Status	IP Address	Subnet Mask	Admin Mode	State	MAC Address
1/0/1	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...
1/0/2	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...
1/0/3	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...
1/0/4	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...
1/0/5	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...
1/0/6	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...
1/0/7	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...
1/0/8	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...
1/0/9	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...
1/0/10	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	80:96:21:...

**Table 251.** Interface Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing details about the routing settings for an interface, this field identifies the interface being viewed.
Status	Indicates whether the interface is capable of routing IP packets (Up) or cannot route packets (Down). For the status to be Up, the routing mode and administrative mode for the interface must be enabled. Additionally, the interface must have an IP address and be physically up (active link).
IP Address	The IP address of the interface.
Subnet Mask	The IP subnet mask for the interface (also known as the network mask or netmask). It defines the portion of the interface's IP address that is used to identify the attached network.
Admin Mode	The administrative mode of the interface, which is either Enabled or Disabled.
State	The state of the interface, which is either Active or Inactive. An interface is considered active if the link is up, and the interface is in a forwarding state.
MAC Address	The burned-in physical address of the interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
Proxy ARP	Indicates whether proxy ARP is enabled or disabled on the interface. When proxy ARP is enabled, the interface can respond to an ARP request for a host other than itself. An interface can act as an ARP proxy if it is aware of the destination and can route packets to the intended host, which is on a different subnet than the host that sent the ARP request.

**Table 251.** *Interface Summary Fields (continued)*

Field	Description
IP MTU	The largest IP packet size the interface can transmit, in bytes. The IP Maximum Transmission Unit (MTU) is the maximum frame size minus the length of the Layer 2 header.

After you click **Details**, the **Details** window opens and displays detailed routing information for the selected interface. The following information describes the fields in this window that are not displayed on the summary page.

**Table 252.** *Interface Summary Details Fields*

Field	Description
Routing Mode	Indicates whether routing is administratively enabled or disabled on the interface.
Link Speed Data Rate	The physical link data rate of the interface.
IP Address Configuration Method	The source of the IP address, which is one of the following: <ul style="list-style-type: none"><li>• <b>None</b> – The interface does not have an IP address.</li><li>• <b>Manual</b> – The IP address has been statically configured by an administrator.</li><li>• <b>DHCP</b> – The IP address has been learned dynamically through DHCP. If the method is DHCP but the interface does not have an IP address, the interface is unable to acquire an address from a network DHCP server.</li></ul>
Bandwidth	The configured bandwidth on this interface. This setting communicates the speed of the interface to higher-level protocols.
Encapsulation Type	The link layer encapsulation type for packets transmitted from the interface, which can be either Ethernet or SNAP.
Forward Net Directed Broadcasts	Indicates how the interface handles network-directed broadcast packets. A network-directed broadcast is a broadcast directed to a specific subnet. The possible values are as follows: <ul style="list-style-type: none"><li>• <b>Enabled</b> – Network directed broadcasts are forwarded.</li><li>• <b>Disabled</b> – Network directed broadcasts are dropped.</li></ul>
Local Proxy ARP	Indicates whether local proxy ARP is enabled or disabled on the interface. When local proxy ARP is enabled, the interface can respond to an ARP request for a host other than itself. Unlike proxy ARP, local proxy ARP allows the interface to respond to ARP requests for a host that is on the same subnet as the host that sent the ARP request. This feature is useful when a host is not permitted to reply to an ARP request from another host in the same subnet, for example when using the protected ports feature.
Destination Unreachables	Indicates whether the interface is allowed to send ICMP Destination Unreachable message to a host if the intended destination cannot be reached for some reason. If the status of this field is Disabled, this interface will not send ICMP Destination Unreachable messages to inform the host about the error in reaching the intended destination.
ICMP Redirects	Indicates whether the interface is allowed to send ICMP Redirect messages. The device sends an ICMP Redirect message on an interface only if ICMP Redirects are enabled both globally and on the interface. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.

## Interface Configuration

Use the Interface Configuration page to configure the IP routing settings for each interface.

To display the page, click **Routing > IP > Interface Configuration** in the navigation menu.

**Figure 259.** Interface Configuration

**Table 253.** Interface Configuration Fields

Field	Description
Interface	The menu contains all interfaces that can be configured for routing. To configure routing settings for an interface, select it from the menu and then configure the rest of the settings on the page.
Status	Indicates whether the interface is currently capable of routing IP packets (Up) or cannot route packets (Down). For the status to be Up, the routing mode and administrative mode for the interface must be enabled. Additionally, the interface must have an IP address and be physically up (active link).
Routing Mode	The administrative mode of IP routing on the interface.



**Table 253.** *Interface Configuration Fields (continued)*

Field	Description
Admin Mode	The administrative mode of the interface. If an interface is administratively disabled, it cannot forward traffic.
State	The state of the interface, which is either Active or Inactive. An interface is considered active if the link is up, and the interface is in a forwarding state.
Link Speed Data Rate	The physical link data rate of the interface.
IP Address Configuration Method	The method to use for configuring an IP address on the interface, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>None</b> – No address is to be configured.</li> <li>• <b>Manual</b> – The address is to be statically configured. When this option is selected you can specify the IP address and subnet mask in the available fields.</li> <li>• <b>DHCP</b> – The interface will attempt to acquire an IP address from a network DHCP server.</li> </ul>
IP Address	The IP address of the interface. This field can be configured only when the selected IP Address Configuration Method is Manual. If the method is DHCP, the interface attempts to lease an IP address from a DHCP server on the network, and the IP address appears in this field (read-only) after it is acquired. If this field is blank, the IP Address Configuration Method might be None, or the method might be DHCP and the interface is unable to lease an address.
Subnet Mask	The IP subnet mask for the interface (also known as the network mask or netmask). This field can be configured only when the selected IP Address Configuration Method is Manual.
MAC Address	The burned-in physical address of the interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
IP MTU	The largest IP packet size the interface can transmit, in bytes. The IP Maximum Transmission Unit (MTU) is the maximum frame size minus the length of the Layer 2 header.
Bandwidth	The configured bandwidth on this interface. This setting communicates the speed of the interface to higher-level protocols.
Encapsulation Type	The link layer encapsulation type for packets transmitted from the interface, which can be either Ethernet or SNAP.
Forward Net Directed Broadcasts	Determines how the interface handles network-directed broadcast packets. A network-directed broadcast is a broadcast directed to a specific subnet. If this option is selected, network directed broadcasts are forwarded. If this option is clear, network directed broadcasts are dropped.
Proxy ARP	When this option is selected, proxy ARP is enabled, and the interface can respond to an ARP request for a host other than itself. An interface can act as an ARP proxy if it is aware of the destination and can route packets to the intended host, which is on a different subnet than the host that sent the ARP request.
Local Proxy ARP	When this option is selected, local proxy ARP is enabled, and the interface can respond to an ARP request for a host other than itself. Unlike proxy ARP, local proxy ARP allows the interface to respond to ARP requests for a host that is on the same subnet as the host that sent the ARP request. This feature is useful when a host is not permitted to reply to an ARP request from another host in the same subnet, for example when using the protected ports feature.

**Table 253.** *Interface Configuration Fields (continued)*

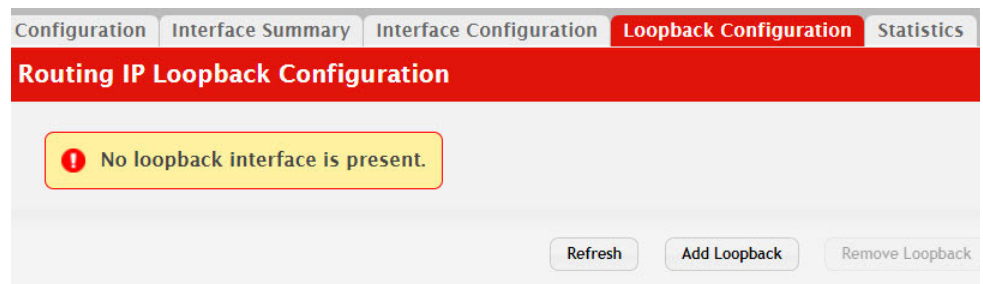
Field	Description
Destination Unreachables	When this option is selected, the interface is allowed to send ICMP Destination Unreachable message to a host if the intended destination cannot be reached for some reason. If this option is clear, the interface will not send ICMP Destination Unreachable messages to inform the host about the error in reaching the intended destination.
ICMP Redirects	When this option is selected, the interface is allowed to send ICMP Redirect messages. The device sends an ICMP Redirect message on an interface only if ICMP Redirects are enabled both globally and on the interface. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.
Secondary IP Address	To add a secondary IP address on the interface, click the + (plus) symbol in the header row and enter the address in the appropriate field in the Secondary IP Address Configuration window. You can add one or more secondary IP addresses to an interface only if the interface already has a primary IP address. To remove a configured secondary IP address, click the – (minus) symbol associated with the entry to remove. To remove all configured secondary IP addresses, click the – (minus) symbol in the header row.
Secondary Subnet Mask	The subnet mask associated with the secondary IP address. You configure this field in the Secondary IP Address Configuration window.

## IP Loopback Configuration

Use this page to configure the IP routing settings for each loopback interface.

To display the IP Loopback Configuration page, click **Routing > IP > Loopback Configuration** in the navigation menu.

**Figure 260.** IP Loopback Configuration



**Table 254.** *IP Loopback Configuration Fields*

Field	Description
Interface	The menu contains all loopback interfaces that can be configured for routing. To configure routing settings for an interface, select it from the menu and then configure the rest of the settings on the page.
IP Address	The IP address of the loopback interface.

**Table 254.** IP Loopback Configuration Fields (continued)

Field	Description
Subnet Mask	The IP subnet mask for the interface (also known as the network mask or netmask).
Secondary IP Address	To add a secondary IP address on the interface, click the + (plus) symbol in the header row and enter the address in the appropriate field in the Secondary IP Address Configuration window. You can add one or more secondary IP addresses to an interface only if the interface already has a primary IP address. To remove a configured secondary IP address, click the – (minus) symbol associated with the entry to remove. To remove all configured secondary IP addresses, click the – (minus) symbol in the header row.
Secondary Subnet Mask	The subnet mask associated with the secondary IP address. You configure this field in the Secondary IP Address Configuration window.

Click **Refresh** to update the information on the screen.

## IP Statistics

The statistics reported on the IP Statistics page are as specified in RFC 1213.

To display the page, click **Routing > IP > Statistics** in the navigation menu. A partial page is shown.

**Note:** Figure 261 does not show all of the fields on the page.

**Figure 261.** IP Statistics

The screenshot shows a navigation bar with tabs for Configuration, Interface Summary, Interface Configuration, Loopback Configuration, and Statistics (which is selected). Below the navigation bar is a red header for "Routing IP Statistics". The main content is a table with the following data:

Field	Value
IpInReceives	218613
IpInHdrErrors	0
IpAddrErrors	0
IpFwdDatagrams	71
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	153598
IpOutRequests	137204
IpOutDiscards	0
IpOutNoRoutes	0

**Table 255.** IP Statistics Fields

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

**Table 255.** *IP Statistics Fields (continued)*

Field	Description
IpInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter includes only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this 'no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully re-assembled.
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.

**Table 255.** *IP Statistics Fields (continued)*

Field	Description
IpFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
IcmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
IcmpInErrors	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
IcmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
IcmpInTimeExcds	The number of ICMP Time Exceeded messages received.
IcmpInParmProbs	The number of ICMP Parameter Problem messages received.
IcmpInSrcQuenchs	The number of ICMP Source Quench messages received.
IcmpInRedirects	The number of ICMP Redirect messages received.
IcmpInEchos	The number of ICMP Echo (request) messages received.
IcmpInEchoReps	The number of ICMP Echo Reply messages received.
IcmpInTimestamps	The number of ICMP Timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object is always zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
IcmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

# Router

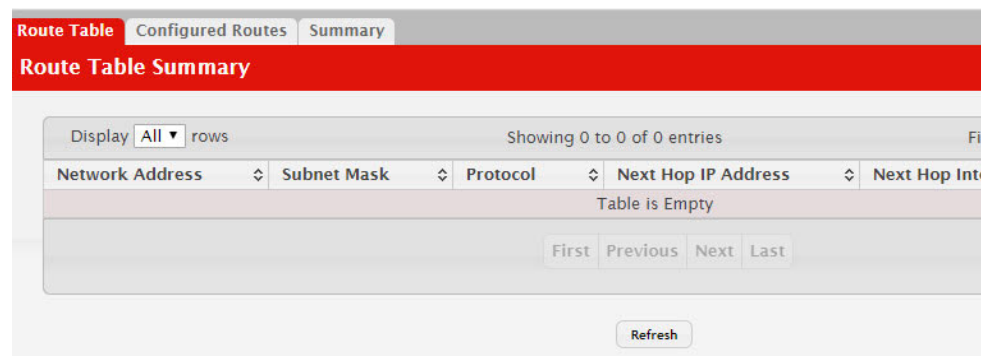
The **Routing > Router** menu contains links to web pages that configure and display route tables.

## Route Table

The route table manager collects routes from multiple sources: static routes, RIP routes, OSPF routes, local routes. The route table manager may learn multiple routes to the same destination from multiple sources. The route table lists all routes. The best routes table displays only the most preferred route to each destination.

To display the page, click **Routing > Router > Route Table** in the navigation menu.

**Figure 262.** Route Table



**Table 256.** Route Table Fields

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are one of the following: <ul style="list-style-type: none"><li>• <b>Local</b></li><li>• <b>Static</b></li><li>• <b>Default</b></li><li>• OSPF Intra</li><li>• OSPF Inter</li><li>• OSPF Type-1</li><li>• OSPF Type-2</li><li>• RIP</li></ul>
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly-attached network.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null.

**Table 256.** *Route Table Fields (continued)*

Field	Description
Best Route	Indicates whether the route is the preferred route to the network. If the field is blank, a better route to the same network exists in the routing table.

Click **Refresh** to update the information on the screen.

## Configured Routes

Use the Configured Routes page to create and display static routes.

To display the page, click **Routing > Router > Configured Routes** in the navigation menu.

**Figure 263.** Configured Routes



Use the buttons to perform the following tasks:

- To configure a route, click **Add** and specify the desired settings in the available fields.
- To remove a configured route, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 257.** *Configured Routes Fields*

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Next Hop IP	The next hop router address to use when forwarding traffic to the destination.
Next Hop Unit/Slot Port	The outgoing interface to use when forwarding traffic to the destination. For static reject routes it would be Null0.
Preference	The preferences configured for the added routes.

## Adding a Static Route

1. Open the Configured Routes page.
2. Click **Add**.

The **Router Route Entry Configuration** page displays:

3. Next to **Route Type**, select **Default** route, **Static** or **Static Reject** from the menu.

**Default:** Enter the default gateway address in the **Next Hop IP Address** field.

**Static:** Enter values for **Network Address**, **Subnet Mask**, **Next Hop IP Address**, and **Preference**.

**Static Reject:** Packets to these destinations will be dropped.

**Note:** The route type you select determines the fields available on the page. Some of the fields that [Table 258](#) describes are not available when configuring certain types of routes.

**Table 258.** *Route Entry Create Fields*

Field	Description
Network Address	Specify the IP route prefix for the destination from the drop-down menu. In order to create a route, a valid routing interface must exist and the next hop IP Address must be on the same network as the routing interface. Routing interfaces are created on the <b>IP Interface Configuration</b> page. Valid next hop IP Addresses can be viewed on the <b>Route Table</b> page.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. Possible values are: <ul style="list-style-type: none"> <li>• <b>Local</b></li> <li>• <b>Static</b></li> <li>• <b>Default</b></li> <li>• OSPF Intra</li> <li>• OSPF Inter</li> <li>• OSPF Type-1</li> <li>• OSPF Type-2</li> <li>• RIP</li> </ul>
Next Hop Slot/Port	The outgoing router interface to use when forwarding traffic to the destination.



**Table 258.** *Route Entry Create Fields (continued)*

Field	Description
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network. When creating a route, the next hop IP must be on the same network as the routing interface. Valid next hop IP Addresses can be seen on the 'Route Table' page.
Metric	Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 to 255. This field is present only when creating a static route.
Preference	Specifies a preference value for the configured next hop.
Route Type	Specifies whether the route is to be a Default route or a Static route.

4. Click **Submit**. The new route is added, and you are returned to the Configured Routes page.

## *Deleting a Route*

Click **Delete** to remove a configured route.

## **Summary**

The Summary page displays summary information about the entries in the IP routing table.

To display the page, click **Routing > Router > Summary** in the navigation menu.

**Figure 264.** Summary

Route Table		Configured Routes	Summary
<b>IP Route Summary</b>			
<b>Route Types</b>			
Connected Routes			0
Static Routes			0
RIP Routes			0
OSPF Routes			0
Intra Area Routes			0
Inter Area Routes			0
External Type-1 Routes			0
External Type-2 Routes			0
Reject Routes			0
<b>Total Routes</b>			<b>0</b>
<b>Route Table Counters</b>			
Best Routes (High)			0 (0)
Alternate Routes			0
Route Adds			0
Route Modifies			0
Route Deletes			0
Unresolved Route Adds			0
Invalid Route Adds			0
Failed Route Adds			0
Reserved Locals			0
Unique Next Hops (High)			0 (0)
<input type="button" value="Refresh"/> <input type="button" value="Clear Counters"/>			

**Table 259.** Summary Fields

Field	Description
Connected Routes	The total number of connected routes in the IP routing table.
Static Routes	The total number of static routes in the IP routing table.
RIP Routes	The total number of routes installed by the RIP protocol.
OSPF Routes	The total number of routes installed by the OSPF protocol.
Intra Area Routes	The total number of intra-area routes installed by the OSPF protocol.
Inter Area Routes	The total number of inter-area routes installed by the OSPF protocol.
External Type-1 Routes	The total number of external type-1 routes installed by the OSPF protocol.
External Type-2 Routes	The total number of external type-2 routes installed by the OSPF protocol.
Reject Routes	The total number of reject routes installed by all protocols.
Total Routes	The total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination.

**Table 259.** *Summary Fields (continued)*

Field	Description
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes.
Clear Counters	This button resets to zero IPv4 routing table counters reported in this page. This only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Click **Refresh** to update the information on the screen.

# Configuring IPv6 Settings

The **Routing > IPv6** folder contains links to web pages that configure and display IP routing data.

## IPv6 Global Configuration

Use this page to configure global IPv6 routing settings on the device. IPv6 routing provides a means of transmitting IPv6 packets between subnets on the network. IPv6 routing configuration is necessary only if the device is used as a Layer 3 device that routes IPv6 packets between subnets. IPv6 is the next generation of the Internet Protocol. With 128-bit addresses, versus 32-bit addresses for IPv4, IPv6 solves the address depletion issues seen with IPv4 and removes the requirement for Network Address Translation (NAT), which is used in IPv4 networks to reduce the number of globally unique IP addresses required for a given network.

To display the IPv6 Global Configuration page, click **Routing > IPv6 > Configuration** in the navigation menu.

**Figure 265.** Configuration

Field	Value	Range
IPv6 Unicast Routing Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
IPv6 Neighbors Dynamic Renew	<input type="checkbox"/>	
IPv6 Hop Limit	64	(1 to 255)
IPv6 Unresolved Packets Rate Limit (pps)	1024	(5 to 1024)
NUD Maximum Unicast Solicits	3	(3 to 10)
NUD Maximum Multicast Solicits	3	(3 to 255)
NUD Back-off Multiple	1	(1 to 5)
ICMPv6 Rate Limit Error Interval (Msecs)	1000	(0 to 2147483647)
ICMPv6 Rate Limit Burst Size	100	(1 to 200)
Static Route Preference	1	(1 to 255)
Local Route Preference	0	

**Table 260.** Configuration Fields

Field	Description
IPv6 Unicast Routing Mode	The administrative mode of IPv6 routing on the device. The options are as follows: <ul style="list-style-type: none"> <li>• Enable – The device can act as a Layer 3 device by routing IPv6 packets between interfaces configured for IPv6 routing.</li> <li>• Disable – The device does not support IPv6 routing.</li> </ul>
IPv6 Neighbors Dynamic Renew	Select this option to enable dynamic renewal mode for the periodic Neighbor Unreachability Detection (NUD) run on the existing IPv6 neighbor entries in the IPv6 neighbor cache. If NUD attempts to communicate with IPv6 neighbors and no response is received after the maximum number of solicits is reached, its entry is removed from the cache.

**Table 260.** Configuration Fields (continued)

Field	Description
IPv6 Hop Limit	The unicast hop count used in IPv6 packets originated by the device. This value is also included in router advertisements.
IPv6 Unresolved Packets Rate Limit	The rate in packets-per-second for the number of IPv6 data packets trapped to the CPU when the packet fails to be forwarded in the hardware due to the unresolved hardware address of the destined IPv6 node.
NUD Maximum Unicast Solicits	The maximum number of unicast neighbor solicitations sent during NUD before switching to multicast neighbor solicitations.
NUD Maximum Multicast Solicits	The maximum number of multicast neighbor solicitations sent during NUD when a neighbor is in the UNREACHABLE state.
NUD Back-off Multiple	The exponential backoff multiplier to be used in the calculation of the next timeout value for neighbor solicitation transmission during NUD following the exponential backoff algorithm.
ICMPv6 Rate Limit Error Interval	The maximum burst interval for ICMPv6 error messages transmitted by the device. The rate limit for ICMPv6 error messages is configured as a token bucket. The ICMPv6 Rate Limit Error Interval specifies how often the token bucket is initialized with tokens of the size configured in the ICMPv6 Rate Limit Burst Size field.
ICMPv6 Rate Limit Burst Size	The number of ICMPv6 error messages that can be sent during the burst interval configured in the ICMPv6 Rate Limit Error Interval field.
Static Route Preference	The default distance (preference) for static IPv6 routes. Lower route-distance values are preferred when determining the best route. The value configured for Static Route Preference is used when using the CLI to configure a static route and no preference is specified. Changing the Static Route Preference does not update the preference of existing static routes.
Local Route Preference	The default distance (preference) for local IPv6 routes.

If you make any changes to the page, click **Submit** to apply the changes to the system.

## IPv6 Interface Summary

This page shows summary information about the IPv6 routing configuration for all interfaces.

To display the IPv6 Interface Summary page, click **Routing > IPv6 > Interface Summary** in the navigation menu.

**Figure 266.** IPv6 Interface Summary

Interface	Operational Status	IPv6 Mode	Routing Mode	Admin Mode	IPv6 Pr
<input type="checkbox"/> 1/0/1	Disabled	Disabled	Disabled	Enabled	
<input type="checkbox"/> 1/0/2	Disabled	Disabled	Disabled	Enabled	
<input type="checkbox"/> 1/0/3	Disabled	Disabled	Disabled	Enabled	
<input type="checkbox"/> 1/0/4	Disabled	Disabled	Disabled	Enabled	
<input type="checkbox"/> 1/0/5	Disabled	Disabled	Disabled	Enabled	
<input type="checkbox"/> 1/0/6	Disabled	Disabled	Disabled	Enabled	
<input type="checkbox"/> 1/0/7	Disabled	Disabled	Disabled	Enabled	
<input type="checkbox"/> 1/0/8	Disabled	Disabled	Disabled	Enabled	
<input type="checkbox"/> 1/0/9	Disabled	Disabled	Disabled	Enabled	
<input type="checkbox"/> 1/0/10	Disabled	Disabled	Disabled	Enabled	

Use the buttons to perform the following tasks:

- To edit any interface, select the interface and click **Edit**. You are redirected to the IPv6 Interface Configuration or IPv6 Loopback Configuration page for the selected interface.
- To view additional routing configuration information for an interface, select the interface with the settings to view and click **Details**.
- To add the next available loopback interface, click **Add Loopback**. You are redirected to the IPv6 Loopback Configuration page.

**Table 261.** IPv6 Interface Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing details about the routing settings for an interface, this field identifies the interface being viewed.
Operational Status	The IPv6 routing operational mode on the interface. The operational mode is enabled under the conditions in the following list; otherwise, the mode is disabled: <ul style="list-style-type: none"> <li>• The IPv6 mode is enabled on the interface.</li> <li>• The routing mode is enabled on the interface.</li> <li>• The administrative mode is enabled on the interface.</li> <li>• The link is up.</li> </ul>
IPv6 Mode	The IPv6 mode on the interface. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used.
Routing Mode	The IPv6 mode on the interface. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used.
Admin Mode	The administrative mode on the interface.

**Table 261.** IPv6 Interface Summary Fields (continued)

Field	Description
IPv6 Prefix	The IPv6 routing prefix dynamically or manually configured on the interface.
Prefix Length	The number of bits used for the IPv6 prefix.
State	The state of the IPv6 address. The state is TENT if routing is disabled or Duplicate Address Detection (DAD) fails. The state is Active if the interface is active and DAD is successful. Otherwise, the state is Inactive.
After you click <b>Details</b> , the Details window opens and displays detailed IPv6 routing information for the selected interface. The following information describes the fields in this window that are not displayed on the summary page.	
Link Local Prefix	The autoconfigured link-local address which is: <ul style="list-style-type: none"> <li>Allocated from part of the IPv6 unicast address space</li> <li>Not visible off the local link</li> <li>Not globally unique</li> </ul>
Link Local Prefix Length	The number of bits used for the prefix of the link-local IPv6 address.
Link Local Status	The status of the IPv6 link local address. The status is TENT if routing is disabled or Duplicate Address Detection (DAD) fails. The state is Active if the interface is active and DAD is successful. Otherwise, the state is Inactive.
DHCPv6 Client Mode	The administrative mode of the DHCPv6 client on the interface. An interface can acquire an IPv6 address by communicating with a network DHCPv6 server (stateful configuration). An interface can also obtain an IPv6 address through stateless address auto-configuration or static configuration.
Stateless Address Auto-Config	The administrative mode of stateless address autoconfiguration on the interface. When enabled, the interface can configure itself by using the Neighbor Discovery Protocol.
Interface Maximum Transmit Unit	The largest IPv6 packet size the interface can transmit, in bytes. To change the MTU value, click the <b>Edit</b> icon to the right of the field. To reset the MTU to the default value, click the <b>Reset</b> icon.
Router Duplicate Address Detection Transmits	The number of duplicate address detection probes the interface transmits while doing neighbor discovery.
Router Advertisement NS Interval	The interval between router advertisements for advertised neighbor solicitations. To change the interval, click the <b>Edit</b> icon to the right of the field. To reset the interval to the default value, click the <b>Reset</b> icon.
Router Lifetime Interval	The value that is placed in the Router Lifetime field of the router advertisements sent from the interface.
Router Advertisement Reachable Time	The value that is placed in the Reachable Time field of the router advertisements. The amount of time to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	The transmission interval between router advertisements messages sent by the interface.
Router Advertisement Managed Config	The mode of the Managed Address Configuration flag in router advertisements sent from the interface. When enabled, the Managed Address Configuration flag is set in router advertisements, indicating that the interface should use stateful autoconfiguration (DHCPv6) to obtain addresses.

**Table 261.** IPv6 Interface Summary Fields (continued)

Field	Description
Router Advertisement Other Config	The mode of the Other Stateful Configuration flag in router advertisements sent from the interface. When enabled, the Other Stateful Configuration flag is set in router advertisements, indicating that the interface should use stateful autoconfiguration for information other than addresses.
Router Advertisement Suppress	The mode of router advertisement transmission suppression on an interface. When enabled, the interface does not transmit router advertisements.
IPv6 Destination Unreachable Messages	The mode for ICMPv6 Destination Unreachable messages. When enabled, the interface can send ICMPv6 Destination Unreachable messages back to the source device if a datagram is undeliverable.
IPv6 Hop Limit Unspecified	The mode that controls whether the interface transmits the hop limit value as 0 in Router Advertisements (Enabled) or transmits the global hop limit value (Disabled).

Click **Refresh** to update the information on the screen.

## IPv6 Interface Configuration

Use this page to configure the IPv6 routing settings for each non-loopback interface.

To display the IPv6 Interface Configuration page, click **Routing > IPv6 > Interface Configuration** in the navigation menu.



**Figure 267.** IPv6 Interface Configuration

Field	Value	Range/Options
Type	<input checked="" type="radio"/> VLAN <input type="radio"/> Interface	
VLAN	VLAN 1	
Interface	1/0/1	
Operational Status	Disabled	
Link Local Prefix		
Link Local Prefix Length		
Link Local Status		
Routing Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
IPv6 Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
DHCPv6 Client Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Stateless Address AutoConfig	<input type="checkbox"/>	
Interface Maximum Transmit Unit	1500	(1280 to 9216)
Router Duplicate Address Detection Transmits	1	(0 to 600)
Router Advertisement NS Interval		(1000 to 429496729)
Router Lifetime Interval	1800	(0 to 9000)
Router Advertisement Reachable Time	0	(0 to 3600000)
Router Advertisement Interval	600	(4 to 1800)
Router Advertisement Managed Config	<input type="checkbox"/>	
Router Advertisement Other Config	<input type="checkbox"/>	
Router Advertisement Suppress	<input type="checkbox"/>	
IPv6 Destination Unreachable Messages	<input type="checkbox"/>	
ICMPv6 Redirects	<input type="checkbox"/>	
IPv6 Hop Limit Unspecified	<input type="checkbox"/>	

**Table 262.** IPv6 Interface Configuration Fields

Field	Description
Type	The type of interface that can be configured for IPv6 routing: <ul style="list-style-type: none"> <li>Interface - Enables a list of all non-loopback interfaces that can be configured for IPv6 routing.</li> <li>VLAN - Enables a list of all VLANs that can be configured for IPv6 routing.</li> </ul>
VLAN	The menu contains all VLANs that can be configured for IPv6 routing. To configure routing settings for a VLAN, select it from the menu and then configure the rest of the settings on the page.
Interface	The menu contains all non-loopback interfaces that can be configured for IPv6 routing. To configure routing settings for an interface, select it from the menu and then configure the rest of the settings on the page.
Operational Status	The IPv6 routing operational mode on the interface. The operational mode is enabled under the conditions in the following list; otherwise, the mode is disabled: <ul style="list-style-type: none"> <li>The IPv6 mode is enabled on the interface.</li> <li>The routing mode is enabled on the interface.</li> <li>The administrative mode is enabled on the interface.</li> <li>The link is up.</li> </ul>

**Table 262.** IPv6 Interface Configuration Fields (continued)

Field	Description
Link Local Prefix	The autoconfigured link-local address which is: <ul style="list-style-type: none"> <li>Allocated from part of the IPv6 unicast address space</li> <li>Not visible off the local link</li> <li>Not globally unique</li> </ul>
Link Local Prefix Length	The number of bits used for the prefix of the link-local IPv6 address.
Link Local Status	The status of the IPV6 link local address. The status is TENT if routing is disabled or Duplicate Address Detection (DAD) fails. The state is Active if the interface is active and DAD is successful. Otherwise, the state is Inactive.
Routing Mode	The administrative mode for Layer 3 routing on the interface.
IPv6 Mode	The administrative mode for IPv6 on the interface. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used.
Admin Mode	The administrative mode of the interface. If an interface is administratively disabled, it will not forward traffic.
DHCPv6 Client Mode	The administrative mode of the DHCPv6 client on the interface. An interface can acquire an IPv6 address by communicating with a network DHCPv6 server (stateful configuration). An interface can also obtain an IPv6 address through stateless address auto-configuration or static configuration.
Stateless Address Auto-Config	When this option is selected, the interface can generate its own IPv6 address by using local interface information and prefix information advertised by routers.
Interface Maximum Transmit Unit	The largest IPv6 packet size the interface can transmit, in bytes. To change the MTU value, click the <b>Edit</b> icon to the right of the field. To reset the MTU to the default value, click the Reset icon.
Router Duplicate Address Detection Transmits	The number of duplicate address detection probes the interface transmits while doing neighbor discovery.
Router Advertisement NS Interval	The interval between router advertisements for advertised neighbor solicitations. To change the interval, click the <b>Edit</b> icon to the right of the field. To reset the interval to the default value, click the Reset icon.
Router Lifetime Interval	The value that is placed in the Router Lifetime field of the router advertisements sent from the interface.
Router Advertisement Reachable Time	The value that is placed in the Reachable Time field of the router advertisements. The amount of time to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	The transmission interval between router advertisements messages sent by the interface.
Router Advertisement Managed Config	When this option is selected, the Managed Address Configuration flag is set in router advertisements, indicating that the interface should use stateful autoconfiguration (DHCPv6) to obtain addresses.
Router Advertisement Other Config	When this option is selected, the Other Stateful Configuration flag is set in router advertisements, indicating that the interface should use stateful autoconfiguration for information other than addresses.
Router Advertisement Suppress	When this option is selected, the interface does not transmit router advertisements.

**Table 262.** IPv6 Interface Configuration Fields (continued)

Field	Description
IPv6 Destination Unreachable Messages	When this option is selected, the interface can send ICMPv6 Destination Unreachable messages back to the source device if a datagram is undeliverable.
ICMPv6 Redirects	When this option is selected, the interface is allowed to send ICMPv6 Redirect messages. An ICMPv6 Redirect message notifies a host when a better route to a particular destination is available on the network segment.
IPv6 Hop Limit Unspecified	When this option is selected, the device can send Router Advertisements on this interface with an unspecified (0) current hop limit value. This will tell the hosts on the link to ignore the hop limit from this device.

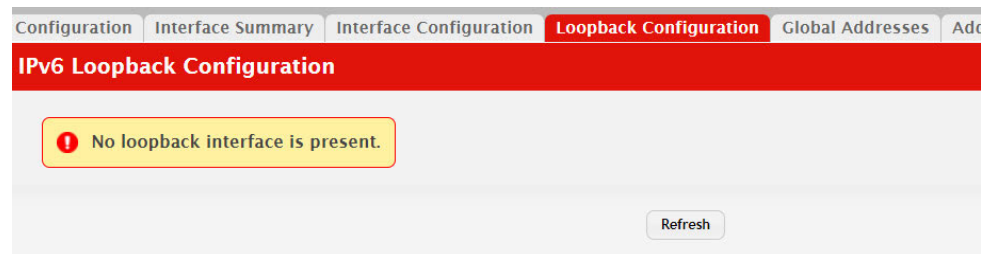
Click **Refresh** to update the information on the screen.

## IPv6 Loopback Configuration

Use this page to configure the IPv6 routing settings for each loopback interface. A loopback interface is a logical interface that is always up (as long as it is administratively enabled) and, because it cannot go down, allows the device to have a stable IPv6 address that other network nodes and protocols can use to reach the device. The loopback can provide the source address for sent packets. The loopback interface does not behave like a network switching port. Specifically, there are no neighbors on a loopback interface; it is a pseudo device for assigning local addresses so that the other Layer 3 hosts can communicate with the device by using the loopback IPv6 address.

To display the IPv6 Loopback Configuration page, click **Routing > IPv6 > Loopback Configuration** in the navigation menu.

**Figure 268.** IPv6 Loopback Configuration



**Table 263.** IPv6 Loopback Configuration Fields

Field	Description
Interface	The menu contains all loopback interfaces that can be configured for IPv6 routing. To configure routing settings for an interface, select it from the menu and then configure the rest of the settings on the page. To add a new loopback interface, use the IPv6 Global Configuration page.
Operational Status	The operational status of the loopback interface. To be operational, both the IPv6 mode and administrative mode must be enabled.

**Table 263.** IPv6 Loopback Configuration Fields (continued)

Field	Description
Link Local Prefix	The autoconfigured link-local address which is: <ul style="list-style-type: none"><li>• Allocated from part of the IPv6 unicast address space</li><li>• Not visible off the local link</li><li>• Not globally unique</li></ul>
Link Local Prefix Length	The number of bits used for the prefix of the link-local IPv6 address.
IPv6 Mode	The IPv6 mode on the loopback interface. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used.
Admin Mode	The administrative mode of the loopback interface.

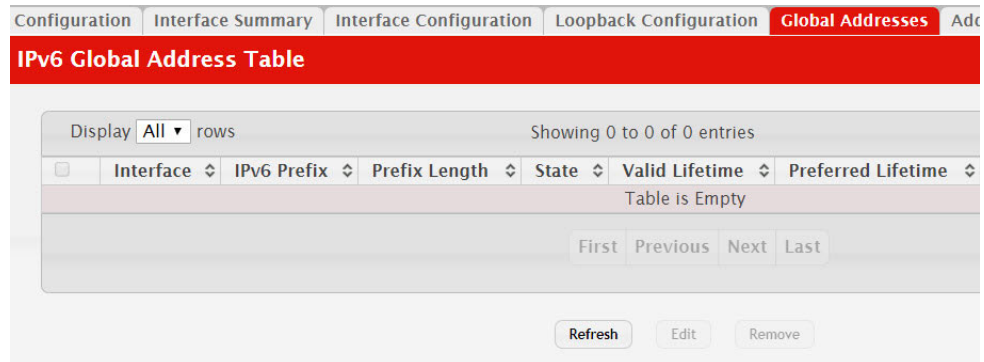
Click **Refresh** to update the information on the screen.

## IPv6 Global Address Table

This page shows information about all global IPv6 addresses configured on all interfaces on the device. From this page, you can also remove a configured IPv6 address from an interface.

To display the IPv6 Global Address Table page, click **Routing > IPv6 > Global Addresses** in the navigation menu.

**Figure 269.** IPv6 Global Address Table



Use the buttons to perform the following tasks:

- To edit any interface, select the interface and click **Edit**. You are redirected to the IPv6 Global Address Configuration page for the selected interface.
- To delete the IPv6 address configuration from one or more interfaces, select each entry to remove and click **Remove**. You must confirm the action.

**Table 264.** IPv6 Global Address Table Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
IPv6 Prefix	The IPv6 routing prefix dynamically or manually configured on the interface. This page does not show information about link-local addresses.

**Table 264.** IPv6 Global Address Table Fields (continued)

Field	Description
Prefix Length	The number of bits used for the IPv6 prefix.
State	The link state, which is either Active or Inactive.
Valid Lifetime	The value, in seconds, to be placed in the Valid Lifetime field of the Prefix Information option in a router advertisement. The prefix is valid for on-link determination for this length of time. Hosts that generate an address from this prefix using stateless address auto-configuration can use those addresses for this length of time. An auto-configured address older than the preferred lifetime but younger than the valid lifetime are considered deprecated addresses. As defined by RFC 2462, a deprecated address is "An address assigned to an interface whose use is discouraged, but not forbidden. A deprecated address should no longer be used as a source address in new communications, but packets sent from or to deprecated addresses are delivered as expected. A deprecated address may continue to be used as a source address in communications where switching to a preferred address causes hardship to a specific upper-layer activity (e.g., an existing TCP connection)." If you specify the maximum value, an autoconfigured address may remain preferred indefinitely.
Preferred Lifetime	The value, in seconds, to be placed in the Preferred Lifetime in the Prefix Information option in a router advertisement. Addresses generated from a prefix using stateless address auto-configuration remain preferred for this length of time. As defined by RFC 2462, a preferred address is "an address assigned to an interface whose use by upper layer protocols is unrestricted. Preferred addresses may be used as the source (or destination) address of packets sent from (or to) the interface." If you specify the maximum value, an autoconfigured address may remain preferred indefinitely.
Onlink Flag	The state of the on-link flag in the IPv6 prefix. When enabled, the prefix can be used for on-link determination by other hosts with IPv6 addresses within this prefix.
Autonomous Flag	The state of the autonomous flag in the IPv6 prefix. When enabled, the prefix can be used for autonomous address configuration by other hosts (in combination with an interface identifier on the other hosts).

Click **Refresh** to update the information on the screen.

## IPv6 Global Address Configuration

This page shows information about all global IPv6 addresses configured on all interfaces on the device. From this page, you can also remove a configured IPv6 address from an interface.

To display the IPv6 Global Address Configuration page, click **Routing > IPv6 > Address Configuration** in the navigation menu.

**Figure 270.** IPv6 Global Address Configuration

To configure an IPv6 address on an interface that already has an IPv6 address, click **Add**.

**Table 265.** IPv6 Global Address Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
IPv6 Prefix	The IPv6 routing prefix dynamically or manually configured on the interface. This page does not show information about link-local addresses.
Prefix Length	The number of bits used for the IPv6 prefix.
Valid Lifetime	The value, in seconds, to be placed in the Valid Lifetime field of the Prefix Information option in a router advertisement. The prefix is valid for on-link determination for this length of time. Hosts that generate an address from this prefix using stateless address auto-configuration can use those addresses for this length of time. An auto-configured address older than the preferred lifetime but younger than the valid lifetime are considered deprecated addresses. As defined by RFC 2462, a deprecated address is “An address assigned to an interface whose use is discouraged, but not forbidden. A deprecated address should no longer be used as a source address in new communications, but packets sent from or to deprecated addresses are delivered as expected. A deprecated address may continue to be used as a source address in communications where switching to a preferred address causes hardship to a specific upper-layer activity (e.g., an existing TCP connection).” If you specify the maximum value, an autoconfigured address may remain preferred indefinitely.
Preferred Lifetime	The value, in seconds, to be placed in the Preferred Lifetime in the Prefix Information option in a router advertisement. Addresses generated from a prefix using stateless address auto-configuration remain preferred for this length of time. As defined by RFC 2462, a preferred address is “an address assigned to an interface whose use by upper layer protocols is unrestricted. Preferred addresses may be used as the source (or destination) address of packets sent from (or to) the interface.” If you specify the maximum value, an autoconfigured address may remain preferred indefinitely.
Onlink Flag	The state of the on-link flag in the IPv6 prefix. When enabled, the prefix can be used for on-link determination by other hosts with IPv6 addresses within this prefix.

**Table 265.** IPv6 Global Address Configuration Fields (continued)

Field	Description
Autonomous Flag	The state of the autonomous flag in the IPv6 prefix. When enabled, the prefix can be used for autonomous address configuration by other hosts (in combination with an interface identifier on the other hosts).

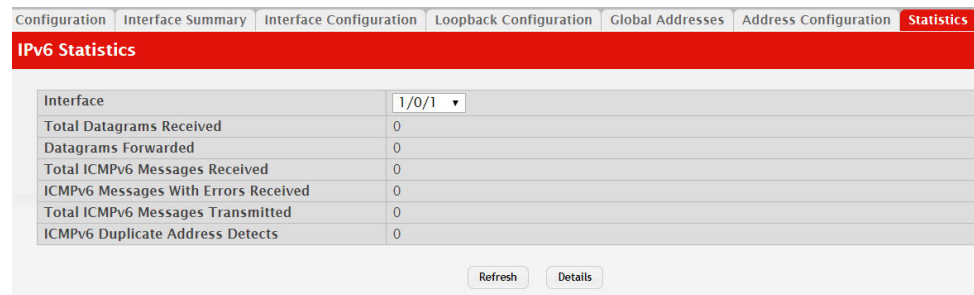
Click **Refresh** to update the information on the screen.

## IPv6 Statistics

This page displays summary statistics about the IPv6 datagrams each interface sends and receives, successfully or unsuccessfully. It also displays summary statistics about the ICMPv6 messages each interface sends and receives. To view more information about the types of datagrams and IPv6 messages an interface has sent and received, select the interface with the information to view and click **Details**. You are redirected to the IPv6 Detailed Statistics page for the selected interface.

To display the IPv6 Statistics page, click **Routing > IPv6 > Statistics** in the navigation menu.

**Figure 271.** IPv6 Statistics



To configure an IPv6 address on an interface that already has an IPv6 address, click **Add**.

**Table 266.** IPv6 Statistics

Field	Description
Interface	The menu contains all physical interfaces that exist on the system. Select an interface to view its IPv6 statistics.
Total Datagrams Received	The total number of input datagrams received by the interface, including those received in error.
Datagrams Forwarded	The number of output datagrams that this entity received and forwarded toward their final destinations. In entities that do not act as IPv6 routers, this counter will include only those packets which were source-routed via this entity, and the source-route processing was successful. Note that for a successfully forwarded datagram, the counter of the outgoing interface is incremented.

**Table 266.** IPv6 Statistics (continued)

Field	Description
Total ICMPv6 Messages Received	The total number of ICMPv6 messages received by the interface, which includes all those counted by ipv6IcmpInErrors. Note that this interface is the interface to which the ICMPv6 messages were addressed, which may not be necessarily the input interface for the messages.
ICMPv6 Messages With Errors Received	The total number of ICMPv6 messages received by the interface, which includes all those counted by ipv6IcmpInErrors. Note that this interface is the interface to which the ICMPv6 messages were addressed, which may not be necessarily the input interface for the messages.
Total ICMPv6 Messages Transmitted	The total number of ICMPv6 messages that this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
ICMPv6 Duplicate Address Detects	The number of duplicate IPv6 addresses detected by the interface.

Click **Refresh** to update the information on the screen.

## IPv6 Detailed Statistics

This page displays detailed statistics about the IPv6 datagrams each interface sends and receives, successfully or unsuccessfully. It also displays detailed statistics about the ICMPv6 messages each interface sends and receives.

To display the IPv6 Detailed Statistics page, click **Routing > IPv6 > Statistics** in the navigation menu.

**Figure 272.** IPv6 Detailed Statistics

Configuration	Interface Summary	Interface Configuration	Loopback Configuration	Global Addresses	Address Configuration	Statistics
<b>IPv6 Statistics</b>						
Interface		1/0/1				
Total Datagrams Received		0				
Datagrams Forwarded		0				
Total ICMPv6 Messages Received		0				
ICMPv6 Messages With Errors Received		0				
Total ICMPv6 Messages Transmitted		0				
ICMPv6 Duplicate Address Detects		0				
		Refresh Details				

To configure an IPv6 address on an interface that already has an IPv6 address, click **Add**.

**Table 267.** IPv6 Detailed Statistics

Field	Description
Interface	The menu contains all physical interfaces that exist on the system. Select an interface to view its IPv6 statistics.
Total Datagrams Received	The total number of input datagrams received by the interface, including those received in error.



**Table 267.** IPv6 Detailed Statistics (continued)

Field	Description
Received Datagrams Locally Delivered	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Header Errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.
Received Datagrams Discarded Due To MTU	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	The number of input datagrams discarded because no route could be found to transmit them to their destination.
Received Datagrams With Unknown Protocol	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses, e.g., ::0, and unsupported addresses, e.g., addresses with unallocated prefixes. For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received Datagrams Discarded Due To Truncated Data	The number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Received Datagrams Reassembly Required	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Datagrams Successfully Reassembled	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
Datagrams Failed To Reassemble	The number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.

**Table 267.** IPv6 Detailed Statistics (continued)

Field	Description
Datagrams Forwarded	The number of output datagrams that this entity received and forwarded toward their final destinations. In entities that do not act as IPv6 routers, this counter will include only those packets which were source-routed via this entity, and the source-route processing was successful. Note that for a successfully forwarded datagram, the counter of the outgoing interface is incremented.
Datagrams Locally Transmitted	The number of datagrams which this entity has successfully transmitted from this output interface.
Datagrams Transmit Failed	The number of datagrams which this entity failed to transmit successfully.
Datagrams Fragments Created	The number of IPv6 datagrams that have been successfully fragmented at this output interface.
Datagrams Failed To Fragment	The number of output datagrams that could not be fragmented at this interface.
Datagrams Successfully Fragmented	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Multicast Datagrams Received	The number of multicast packets received by the interface.
Multicast Datagrams Transmitted	The number of multicast packets transmitted by the interface.
Total ICMPv6 Messages Received	The total number of ICMPv6 messages received by the interface, which includes all those counted by ipv6IfcMplnErrors. Note that this interface is the interface to which the ICMPv6 messages were addressed, which may not be necessarily the input interface for the messages.
ICMPv6 Messages With Errors Received	The number of ICMPv6 messages that the interface received but were determined to have ICMPv6-specific errors (bad ICMPv6 checksums, bad length, etc.)
ICMPv6 Destination Unreachable Messages Received	The number of ICMPv6 Destination Unreachable messages received by the interface.
ICMPv6 Messages Prohibited Administratively Received	The number of ICMPv6 destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages Received	The number of ICMPv6 Time Exceeded messages received by the interface.
ICMPv6 Parameter Problem Messages Received	The number of ICMPv6 Parameter Problem messages received by the interface.
ICMPv6 Packet Too Big Messages Received	The number of ICMPv6 Packet Too Big messages received by the interface.
ICMPv6 Echo Request Messages Received	The number of ICMPv6 Echo (request) messages received by the interface.
ICMPv6 Echo Reply Messages Received	The number of ICMPv6 Echo Reply messages received by the interface.
ICMPv6 Router Solicit Messages Received	The number of ICMPv6 Neighbor Solicitation messages received by the interface.
ICMPv6 Router Advertisement Messages Received	The number of ICMPv6 Router Advertisement messages received by the interface.
ICMPv6 Neighbor Solicit Messages Received	The number of ICMPv6 Neighbor Solicitation messages received by the interface.

**Table 267.** IPv6 Detailed Statistics (continued)

Field	Description
ICMPv6 Neighbor Advertisement Messages Received	The number of ICMPv6 Neighbor Advertisement messages received by the interface.
ICMPv6 Redirect Messages Received	The number of Redirect messages received.
ICMPv6 Group Membership Query Messages Received	The number of ICMPv6 Group Membership Query messages received.
ICMPv6 Group Membership Response Messages Received	The number of ICMPv6 Group Membership Response messages received.
ICMPv6 Group Membership Reduction Messages Received	The number of ICMPv6 Group Membership Reduction messages received.
Total ICMPv6 Messages Transmitted	The total number of ICMPv6 messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
ICMPv6 Messages Not Transmitted Due To Error	The number of ICMPv6 messages which this interface did not send due to problems discovered within ICMPv6 such as a lack of buffers. This value should not include errors discovered outside the ICMPv6 layer such as the inability of IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
ICMPv6 Destination Unreachable Messages Transmitted	The number of ICMPv6 Destination Unreachable Messages sent by the interface.
ICMPv6 Messages Prohibited Administratively Transmitted	The number of ICMPv6 destination unreachable/communication administratively prohibited messages sent.
ICMPv6 Time Exceeded Messages Transmitted	The number of ICMPv6 Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	The number of ICMPv6 Parameter Problem messages sent by the interface.
ICMPv6 Packet Too Big Messages Transmitted	The number of ICMPv6 Packet Too Big messages sent by the interface.
ICMPv6 Echo Request Messages Transmitted	The number of ICMPv6 Echo (request) messages sent by the interface.
ICMPv6 Router Solicit Messages Transmitted	The number of ICMPv6 Router Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	The number of ICMPv6 Router Advertisement messages sent by the interface.
ICMPv6 Neighbor Solicit Messages Transmitted	The number of ICMPv6 Neighbor Solicitation messages sent by the interface.
ICMPv6 Neighbor Advertisement Messages Transmitted	The number of ICMPv6 Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Transmitted	The number of Redirect messages sent.
ICMPv6 Group Membership Query Messages Transmitted	The number of ICMPv6 Group Membership Query messages sent.

**Table 267.** IPv6 Detailed Statistics (continued)

Field	Description
ICMPv6 Group Membership Response Messages Transmitted	The number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Transmitted	The number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	The number of duplicate IPv6 addresses detected by the interface.

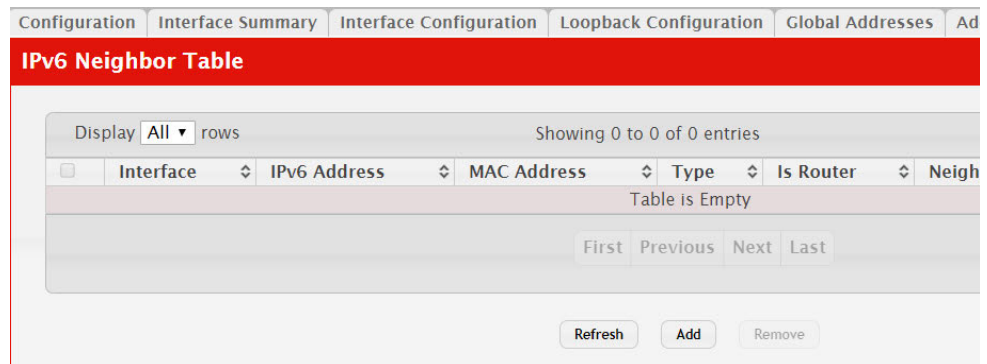
Click **Refresh** to update the information on the screen.

## IPv6 Neighbor Table

This page displays the IPv6 neighbor entries in the local IPv6 neighbor cache. Neighbors are discovered by using the Neighbor Discovery Protocol via ICMPv6 messages on active IPv6 interfaces.

To display the IPv6 Neighbor Table page, click **Routing > IPv6 > Neighbor Table** in the navigation menu.

**Figure 273.** IPv6 Neighbor Table



**Table 268.** IPv6 Neighbor Table

Field	Description
Interface	The local interface on which the neighbor was discovered.
IPv6 Address	The IPv6 prefix and prefix length of the neighbor interface.
MAC Address	The MAC address associated with the neighbor interface. If the MAC address is all zeros, the entry is a Negative NDP entry. A Negative NDP entry is added to the table when the device sends a Neighbor Solicitation Request, but it has not yet been resolved. If the request is resolved and the neighbor is reachable, its valid MAC address replaces the null address. If the request times out, the entry is removed.
Is Router	Indicates whether the neighbor is a router. If the neighbor is a router, the value is TRUE. If the neighbor is not a router, the value is FALSE.

**Table 268.** IPv6 Neighbor Table (continued)

Field	Description
Neighbor State	<p>Specifies the state of the neighbor cache entry. Dynamic entries in the IPv6 neighbor discovery cache can be one of the following:</p> <ul style="list-style-type: none"><li>• <b>Incmp</b> - Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.</li><li>• <b>Reach</b> - Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.</li><li>• <b>Stale</b> - More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.</li><li>• <b>Delay</b> - More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.</li><li>• <b>Probe</b> - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.</li></ul>
Last Updated	<p>The amount of time that has passed since the address was confirmed to be reachable.</p>
Clear (Button)	<p>Click this button to clear all entries from the table. The table is repopulated with IPv6 neighbor entries as the neighbors are discovered.</p>

Click **Refresh** to update the information on the screen.

## Configuring IPv6 Routes

The **Routing > IPv6 Routes** folder contains links to web pages that configure and display IP routing data.

### IPv6 Route Table

This page displays the entries in the IPv6 routing table, including all dynamically learned and statically configured entries. The device uses the routing table to determine how to forward IPv6 packets. A statically-configured route does not appear in the table until it is reachable.

To display the IPv6 Global Configuration page, click **Routing > IPv6 Routes > IPv6 Route Table** in the navigation menu.

**Figure 274.** IPv6 Route Table



**Table 269.** IPv6 Route Table Fields

Field	Description
IPv6 Prefix/Length	The IPv6 address, including the prefix and prefix length, for the destination network.
Protocol	Identifies which protocol created the route. A route can be created one of the following ways: <ul style="list-style-type: none"><li>• Dynamically learned through a supported routing protocol</li><li>• Dynamically learned by being a directly-attached local route</li><li>• Statically configured by an administrator</li></ul>
Next Hop IPv6 Address	The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IPv6 address of the local interface for a directly-attached network.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null.
Best Route	Indicates whether the route is the preferred route to the network. If the field is blank, a better route to the same network exists in the IPv6 routing table.

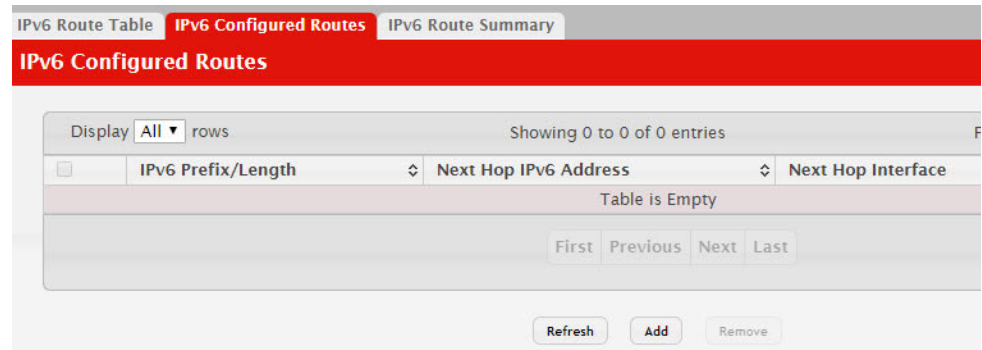
Click **Refresh** to update the information on the screen.

## IPv6 Configured Routes

Use this page to configure static IPv6 global, link local, and static reject routes in the routing table. The page shows the routes that have been manually added to the routing table. To configure a new IPv6 route, click **Add**.

To display the IPv6 Configured Routes page, click **Routing > IPv6 Routes > IPv6 Configured Routes** in the navigation menu.

**Figure 275.** IPv6 Configured Routes



**Table 270.** IPv6 Configured Routes Fields

Field	Description
IPv6 Prefix/Length	The IPv6 address, including the prefix and prefix length, for the destination network.
Next Hop IP Address	The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IPv6 address of the local interface for a directly-attached network.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null. The next hop is Unresolved until the device is able to reach the interface.
Preference	The preference of the route. A lower preference value indicates a more preferred route. When the routing table has more than one route to the same network, the device selects the route with the best (lowest) route preference.
After you click <b>Add</b> , a window opens and displays the configuration options for the new route. The following information describes the additional field in the Add Route window.	
Route Type	The type of route to configure, which is one of the following: <ul style="list-style-type: none"> <li>• Global – A route with an address that is globally routable and is recognized outside of the local network.</li> <li>• Link Local – A route with an address that is allocated from part of the IPv6 unicast address space. It is not visible off the local link and is not globally unique.</li> <li>• Static Reject – A route where packets that match the route are discarded instead of forwarded. The device might send an ICMPv6 Destination Unreachable message.</li> </ul>

If you make any changes to the page, click **Submit** to apply the changes to the system.

Click **Refresh** to update the information on the screen.

## IPv6 Route Summary

This page displays summary information about the entries in the IPv6 routing table.

To display the IPv6 Route Summary page, click **Routing > IPv6 Routes > IPv6 Route Summary** in the navigation menu.

**Figure 276.** IPv6 Route Summary

Route Types	
Connected Routes	0
Static Routes	0
6To4 Routes	0
OSPF Routes	0
Intra Area Routes	0
Inter Area Routes	0
External Type-1 Routes	0
External Type-2 Routes	0
Total Routes	0

Route Table Counters	
Best Routes (High)	0 (0)
Alternate Routes	0
Route Adds	0
Route Deletes	0
Unresolved Route Adds	0
Invalid Route Adds	0
Failed Route Adds	0
Reserved Locals	0
Unique Next Hops (High)	0 (0)
Number of Prefixes	

**Table 271.** IPv6 Route Summary Fields

Field	Description
Connected Routes	The total number of connected routes in the IPv6 routing table.
Static Routes	The total number of static routes in the IPv6 routing table.
6To4 Routes	The total number of 6to4 routes in the IPv6 routing table. A 6to4 route allows IPv6 sites to communicate with each other over an IPv4 network by treating the wide-area IPv4 network as a unicast point-to-point link layer.
OSPF Routes	The total number of routes installed by the OSPFv3 protocol.



**Table 271.** IPv6 Route Summary Fields (continued)

Field	Description
Intra Area Routes	The total number of intra-area routes installed by the OSPFv3 protocol.
Inter Area Routes	The total number of inter-area routes installed by the OSPFv3 protocol.
External Type-1 Routes	The total number of external type-1 routes installed by the OSPFv3 protocol.
External Type-2 Routes	The total number of external type-2 routes installed by the OSPFv3 protocol.
Reject Routes	The total number of reject routes installed by all protocols.
Total Routes	The total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number counts only the best route to each destination.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes.
Number of Prefixes	The unique IPv6 prefixes in the IPv6 routing table.
Clear Counters (Button)	This button resets all IPv6 routing table event counters on this page to zero. Not that only event counters are reset; counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Click **Refresh** to update the information on the screen.

## Configuring DHCPv6

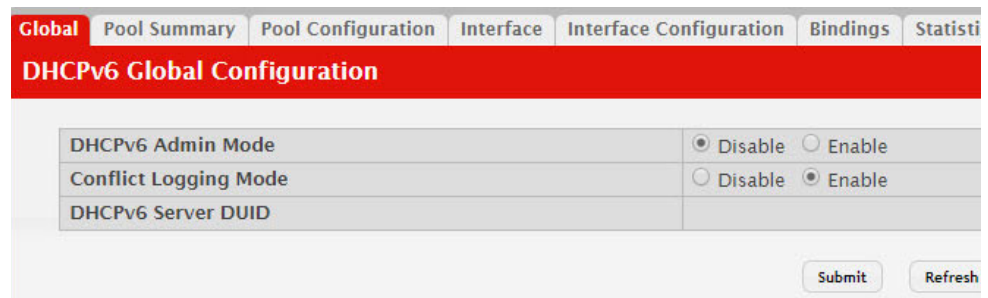
The **Routing > DHCPv6** folder contains links to web pages that configure and display IP routing data.

### DHCPv6 Global Configuration

Use this page to configure the global Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server settings on the device. The device can act as a DHCPv6 server or DHCPv6 relay agent to help assign network configuration information to IPv6 clients.

To display the DHCPv6 Global Configuration page, click **Routing > DHCPv6 > Global** in the navigation menu.

**Figure 277.** DHCPv6 Global Configuration



**Table 272.** DHCPv6 Global Configuration Fields

Field	Description
DHCPv6 Admin Mode	The administrative mode of the DHCPv6 server.
Conflict Logging Mode	The conflict logging mode of the bindings reported to be conflicting by the DHCPv6 Clients via the DECLINE messages
DHCPv6 Server DUID	The DHCP Unique Identifier (DUID) of the DHCPv6 server.

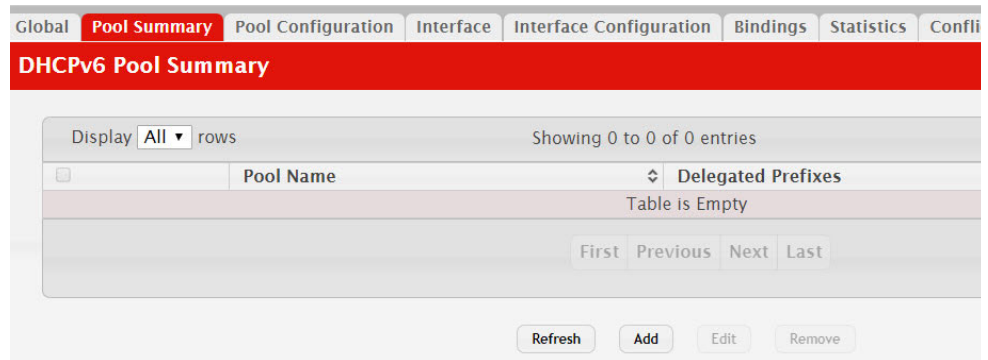
Click **Refresh** to update the information on the screen.

### DHCPv6 Pool Summary

Use this page to view the currently configured DHCPv6 server pools and to add and remove pools. A DHCPv6 server pool is a set of network configuration information available to DHCPv6 clients that request the information.

To display the DHCPv6 Pool Summary page, click **Routing > DHCPv6 > Pool Summary** in the navigation menu.

**Figure 278.** DHCPv6 Pool Summary



Use the buttons to perform the following tasks:

- To add a pool, click **Add** and configure the pool information in the available fields.
- To remove a pool, select each entry to delete and click **Remove**. You must confirm the action before the pool is deleted.
- To change the settings for a pool, select the entry to update and click **Edit**. You are redirected to the DHCPv6 Pool Configuration page for the selected pool. From this page, you can configure additional bindings within the pool.

**Table 273.** DHCPv6 Pool Summary Fields

Field	Description
Pool Name	The name that identifies the DHCPv6 server pool.
Delegated Prefixes	The general prefix in the pool for use in allocating and assigning addresses to hosts that may be utilizing IPv6 auto-address configuration or acting as DHCPv6 clients.
After you click <b>Add</b> , the DHCPv6 Pool Configuration window opens. The following information describes the additional field available in the window.	
DHCPv6 Client DUID	The DHCP Unique Identifier (DUID) of the client. The DUID is a combination of the client's hardware address and client identifier.

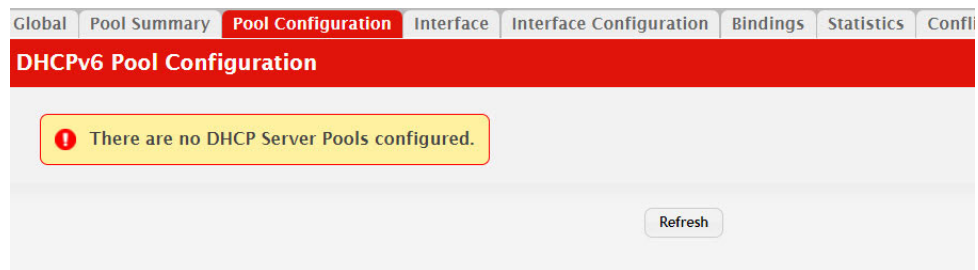
Click **Refresh** to update the information on the screen.

## DHCPv6 Pool Configuration

Use this page to edit pool settings or to configure additional settings for existing DHCPv6 pools.

To display the DHCPv6 Pool Configuration page, click **Routing > DHCPv6 > Pool Configuration** in the navigation menu.

**Figure 279.** DHCPv6 Pool Configuration



To add, remove, or update binding entries within a pool or update other pool configuration information, you must first select the DHCPv6 pool from the Pool Name menu. After you select the pool to configure, use the icons on the page to perform the following tasks:

- To add a new binding to the selected DHCPv6 pool, click the + (plus) icon in the header row above the binding entries.
- To remove all bindings from the selected pool, click the – (minus) icon in the header row above the binding entries.
- To update the information for a binding, click the **Edit** icon associated with the binding.
- To remove a binding from the selected pool, click the – (minus) icon associated with the binding.
- To add DNS server or domain name information to a pool, click the + (plus) icon in the header row of the DNS Server or Domain Name field.
- To remove all configured DNS server or domain name entries from the selected pool, click the – (minus) icon in the header row of the DNS Server or Domain Name field.
- To remove a single DNS or domain name entry, click the – (minus) icon associated with the entry to remove.

**Table 274.** DHCPv6 Pool Configuration Fields

Field	Description
Pool Name	The menu includes all DHCPv6 server pools that have been configured on the device.
Delegated Prefixes	The IPv6 prefix and prefix length to assign the requesting client.
DUID	The DHCP Unique Identifier (DUID) of the client. The DUID is a combination of the client's hardware address and client identifier.
Client Name	The optional system name associated with the client.
Valid Lifetime	The maximum amount of time the requesting client is allowed to use the prefix.
Prefer Lifetime	The preferred amount of time the requesting client is allowed to use the prefix. The value of the Prefer Lifetime must be less than the value of the Valid Lifetime.
DNS Server	The IPv6 prefix of each DNS server each client in the pool can contact to perform address resolution.
Domain Name	The domain name configured for each client in the pool.

Click **Refresh** to update the information on the screen.

## DHCPv6 Interface Summary

Use this page to view the per-interface settings for DHCPv6. To configure the settings, select the interface to configure and click **Edit**. You are redirected to the DHCPv6 Interface Configuration page for the selected interface.

To display the DHCPv6 Interface Summary page, click **Routing > DHCPv6 > Interface** in the navigation menu.

**Figure 280.** DHCPv6 Interface Summary

Interface	Interface Mode	Pool Name	Relay Interface	Destination IP
1/0/1	None	N/A	N/A	N/A
1/0/2	None	N/A	N/A	N/A
1/0/3	None	N/A	N/A	N/A
1/0/4	None	N/A	N/A	N/A
1/0/5	None	N/A	N/A	N/A
1/0/6	None	N/A	N/A	N/A
1/0/7	None	N/A	N/A	N/A
1/0/8	None	N/A	N/A	N/A
1/0/9	None	N/A	N/A	N/A
1/0/10	None	N/A	N/A	N/A

**Table 275.** DHCPv6 Interface Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
Interface Mode	The DHCPv6 function configured on the interface, which is one of the following: <ul style="list-style-type: none"> <li>None – The interface is not configured as a DHCPv6 server or DHCPv6 relay agent.</li> <li>Server – The interface responds to requests from DHCPv6 clients.</li> <li>Relay – The interface acts as an intermediary to deliver DHCPv6 messages between clients and servers. The interface is on the same link as the client.</li> </ul>
Pool Name	(DHCPv6 server interface only) The name of the DHCPv6 pool the server uses to assign client information.
Relay Interface	(DHCPv6 relay agent interface only) The interface on the device through which a DHCPv6 server is reached.
Destination IP Address	(DHCPv6 relay agent interface only) The destination IPv6 address of the DHCPv6 server to which client packets are forwarded.

**Table 275.** DHCPv6 Interface Summary Fields (continued)

Field	Description
Remote ID	(DHCPv6 relay agent interface only) The relay agent information option remote-ID sub-option to be added to relayed messages. This value is derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

Click **Refresh** to update the information on the screen.

## DHCPv6 Interface Configuration

Use this page to configure the per-interface settings for DHCPv6. The DHCPv6 interface modes are mutually exclusive. The fields that can be configured on this page depend on the selected mode for the interface.

To display the Interface Configuration page, click **Routing > DHCPv6 > Interface Configuration** in the navigation menu.

**Figure 281.** DHCPv6 Interface Configuration

**Table 276.** Interface Configuration Fields

Field	Description
Interface	Select the interface with the information to view or configure.

**Table 276.** *Interface Configuration Fields (continued)*

Field	Description
Interface Mode	The DHCPv6 function configured on the interface, which is one of the following: <ul style="list-style-type: none"><li>• <b>None</b> – The interface is not configured as a DHCPv6 server or DHCPv6 relay agent.</li><li>• <b>Server</b> – The interface responds to requests from DHCPv6 clients.</li><li>• <b>Client</b> – The interface initiates requests on a link to obtain configuration parameters from one or more DHCPv6 servers.</li><li>• <b>Relay</b> – The interface acts as an intermediary to deliver DHCPv6 messages between clients and servers. The interface is on the same link as the client.</li></ul>
Server Options	(DHCPv6 server interface only) The name of the DHCPv6 pool the server uses to assign client information.
Pool Name	The name of the DHCPv6 pool the server can use to assign client information.
Rapid Commit	When enabled, this option allows the DHCPv6 client to obtain configuration information by exchanging two messages with the DHCPv6 server instead of the standard four messages.
Preference	The preference value to include in DHCPv6 Advertise messages. If a DHCPv6 client receives Advertise messages from multiple DHCPv6 servers, it responds to the server with the highest preference value.
Relay Options	The information in this section can be configured only if the selected Interface Mode is Relay.
Relay Interface	The interface on the device through which a DHCPv6 server is reached.
Destination IP Address	The destination IPv6 address of the DHCPv6 server to which client packets are forwarded.
Remote ID	The relay agent information option remote-ID sub-option to be added to relayed messages. This value is derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

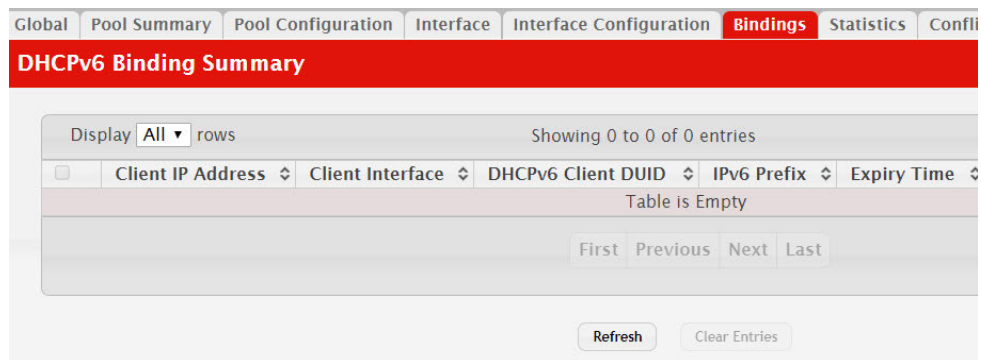
Click **Refresh** to update the information on the screen.

## DHCPv6 Binding Summary

Use this page to view entries in the DHCP Bindings table. After a client acquires IPv6 configuration information from the DHCPv6 server, the server adds an entry to its database. The entry is called a binding.

To display the Binding Summary page, click **Routing > DHCPv6 > Bindings** in the navigation menu.

**Figure 282.** DHCPv6 Binding Summary



**Table 277.** Binding Summary Fields

Field	Description
Client IP Address	The IPv6 address associated with the client.
Client Interface	The interface number where the client binding occurred.
DHCPv6 Client DUID	The DHCP Unique Identifier (DUID) of the client. The DUID is a combination of the client's hardware address and client identifier.
IPv6 Prefix	The type of prefix associated with this binding.
Expiry Time	The number of seconds until the prefix associated with a binding expires.
Valid Lifetime	The maximum amount of time the client is allowed to use the prefix.
Prefer Lifetime	The preferred amount of time the client is allowed to use the prefix.

Click **Refresh** to update the information on the screen.

## DHCPv6 Statistics

This page displays the DHCPv6 server statistics for the device, including information about the DHCPv6 messages sent, received, and discarded globally and on each interface. The values on this page indicate the various counts that have accumulated since they were last cleared.

To display the DHCPv6 Statistics page, click **Routing > DHCPv6 > Statistics** in the navigation menu.



**Figure 283.** DHCPv6 Statistics

Interface	Total DHCPv6 Packets Received	DHCPv6 Request Packets Received	Received DHCPv6 Packets Discarded	Total DHCPv6 Packets Sent
All	0	0	0	0
1/0/1	0	0	0	0
1/0/2	0	0	0	0
1/0/3	0	0	0	0
1/0/4	0	0	0	0
1/0/5	0	0	0	0
1/0/6	0	0	0	0
1/0/7	0	0	0	0
1/0/8	0	0	0	0
1/0/9	0	0	0	0

Use the buttons to perform the following tasks:

- To view detailed DHCPv6 statistics for an interface, select the entry with the information to view and click **Details**.
- To reset the DHCPv6 counters for one or more interfaces, select each interface with the statistics to reset and click **Clear**.

**Table 278.** DHCPv6 Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. The row at the top of the table (All) contains cumulative statistics for all interfaces.
Total DHCPv6 Packets Received	The number of DHCPv6 messages received on the interface. The DHCPv6 messages sent from a DHCPv6 client to a DHCPv6 server include Solicit, Request, Confirm, Renew, Rebind, Release, Decline, and Information-Request messages. Additionally, a DHCPv6 relay agent can forward Relay-Forward messages to a DHCPv6 server.
DHCPv6 Request Packets Received	The number of DHCPv6 Request messages received on the interface. DHCPv6 Request messages are sent by a client to request IPv6 configuration information from the server.
Received DHCPv6 Packets Discarded	The number of DHCPv6 messages received on the interface that were discarded due to errors or because they were invalid.
Total DHCPv6 Packets Sent	The number of DHCPv6 messages sent by the interface. The DHCPv6 messages sent from a DHCPv6 server to a DHCPv6 client include Advertise, Reply, Reconfigure, and Relay-Reply messages.
DHCPv6 Reply Packets Transmitted	The number of DHCPv6 Reply messages sent from the interface to a DHCPv6 client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.

**Table 278.** *DHCPv6 Statistics Fields (continued)*

Field	Description
	After you click Details, a window opens and shows detailed DHCPv6 statistics for the selected interface. The following information describes the additional fields that appear in the Details window.
DHCPv6 Solicit Packets Received	The number of DHCPv6 Solicit messages received on the interface. This type of message is sent by a client to locate DHCPv6 servers.
DHCPv6 Confirm Packets Received	The number of DHCPv6 Confirm messages received on the interface. This type of message is sent by a client to all DHCPv6 servers to determine whether its configuration is valid for the connected link.
DHCPv6 Renew Packets Received	The number of DHCPv6 Renew messages received on the interface. This type of message is sent by a client to extend and update the configuration information provided by the DHCPv6 server.
DHCPv6 Rebind Packets Received	The number of DHCPv6 Rebind messages received on the interface. This type of message is sent by a client to any DHCPv6 server when it does not receive a response to a Renew message.
DHCPv6 Release Packets Received	The number of DHCPv6 Release messages received on the interface. This type of message is sent by a client to indicate that it no longer needs the assigned address.
DHCPv6 Decline Packets Received	The number of DHCPv6 Decline messages received on the interface. This type of message is sent by a client to the DHCPv6 server to indicate that an assigned address is already in use on the link.
DHCPv6 Inform Packets Received	The number of DHCPv6 Information-Request messages received on the interface. This type of message is sent by a client to request configuration information other than IP address assignment.
DHCPv6 Relay-forward Packets Received	The number of DHCPv6 Relay-Forward messages received on the interface. This type of message is sent by a relay agent to forward messages to servers.
DHCPv6 Relay-reply Packets Received	The number of DHCPv6 Relay-Reply messages received on the interface. This type of message is sent by a server to a DHCPv6 relay agent and contains the message for the relay agent to deliver to the client.
DHCPv6 Malformed Packets Received	The number of DHCPv6 messages that were received on the interface but were dropped because they were malformed.
DHCPv6 Advertisement Packets Transmitted	The number of DHCPv6 Advertise messages sent by the interface. This type of message is sent by a server to a DHCPv6 client in response to a Solicit message and indicates that it is available for service.
DHCPv6 Reconfig Packets Transmitted	The number of DHCPv6 Reconfigure messages sent by the interface. This type of message is sent by a server to a DHCPv6 client to inform the client that the server has new or updated information. The client then typically initiates a Renew/Reply or Information-request/Reply transaction with the server to receive the updated information.
DHCPv6 Relay-forward Packets Transmitted	The number of DHCPv6 Relay-Forward messages sent by the interface. This type of message is sent by a relay agent to forward messages to servers.
DHCPv6 Relay-reply Packets Transmitted	The number of DHCPv6 Relay-Reply messages sent by the interface. This type of message is sent by a server to a DHCPv6 relay agent and contains the message for the relay agent to deliver to the client.

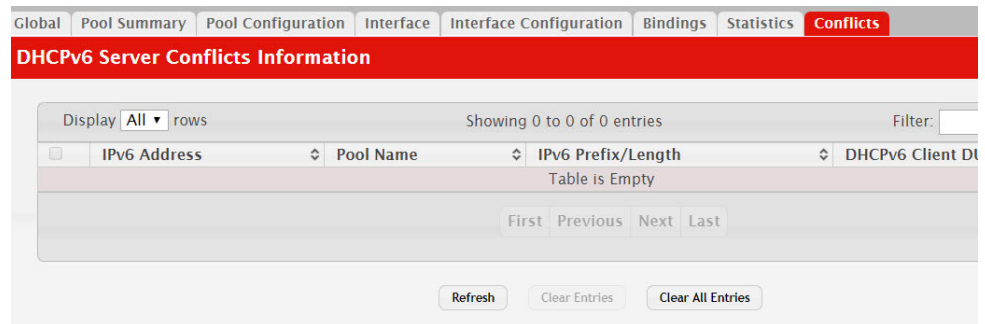
Click **Refresh** to update the information on the screen.

## DHCPv6 Server Conflicts Information

This page displays information about IPv6 address conflicts detected during the DHCPv6 message exchange process between the server and client. An address conflict is created when a leased binding is declined by the DHCPv6 client.

To display the DHCPv6 Server Conflicts Information page, click **Routing > DHCPv6 > Conflicts** in the navigation menu.

**Figure 284.** DHCPv6 Server Conflicts Information



**Table 279.** DHCPv6 Server Conflicts Information Fields

Field	Description
IPv6 Address	The conflicting IPv6 address.
Pool Name	The name of the DHCPv6 pool the server uses to assign client information.
IPv6 Prefix/Length	The IPv6 address, including the prefix and prefix length, as a general prefix in the pool for use in allocating and assigning addresses to DHCPv6 clients.
DHCPv6 Client DUID	The DHCP Unique Identifier (DUID) of the client. The DUID is a combination of the client's hardware address and client identifier.

Use the buttons to perform the following tasks:

- To remove an entry from the table, select each entry to delete and click **Clear Entries**. You must confirm the action before the binding is deleted.
- To remove all entries from the table, click **Clear All Entries**. You must confirm the action before all bindings are deleted.
- To update the information on the screen, click **Refresh**.

---

## Configuring Policy Based Routing

Policy based routing (PBR) enhances/modifies existing features in CE0128XB/CE0152XB. These features are route maps and access-control lists. Route maps are part of routing (see “Router” on page 390) and access control lists are part of QOS (see “Configuring Access Control Lists” on page 464). As policy based routing feature utilizes services of both features mentioned above, the CE0128XB/CE0152XB software with a combination of Routing and QOS packages is required to have PBR functional.

Normally, routers take forwarding decision based on routing tables in order to forward packets to destination addresses. Policy Based Routing is a feature that enables network administrator to define forwarding behavior based on packet contents. In brief, Policy Based Routing overrides traditional destination-based routing behavior.

The CE0128XB/CE0152XB policy-based routing feature match the following packet entities and overrides traditional forwarding behavior accomplished through destination-based routing:

- The size of the packet
- Protocol of the payload
- Source MAC address
- Destination MAC address
- Source IP address
- Destination IP address
- VLAN tag
- Priority

## Chapter 7. Managing Device Security

Use the features in the Security folder on the navigation menu to set management security parameters for port, user, and server security.

### Port Access Control

In port-based authentication mode, when 802.1x is enabled globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

The 802.1X network has three components:

- **Authenticators:** Specifies the port that is authenticated before permitting system access.
- **Supplicants:** Specifies host connected to the authenticated port requesting access to the system services.

**Authentication Server:** Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

The Port Access Control folder contains links to the following pages that allow you to view and configure 802.1X features on the system.

### Global Port Access Control Configuration

Use the Port Based Access Control Configuration page to enable or disable port access control on the system.

To display the Port Based Authentication page, click **Security > Port Access Control > Configuration** in the navigation menu.

**Figure 285.** Port Access Control—Port Configuration

Field	Description
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
EAPOL Flood Mode	Disabled
Campus NOS Version	0

**Table 280.** Port Access Control—Port Configuration Fields

Field	Description
Administrative Mode	The administrative mode of port-based authentication on the switch. Select <b>Enable</b> or <b>Disable</b> 802.1x mode on the switch. The default is Disable.

**Table 280.** Port Access Control—Port Configuration Fields (continued)

Field	Description
EAPOL Flood Mode	The administrative mode of the Extensible Authentication Protocol (EAP) over LAN (EAPOL) flood support on the device. EAPOL Flood Mode can be enabled when Admin Mode and Monitor Mode are disabled.
Campus NOS Version	The version of 802.1x software running on the switch. It is not the 802.1x protocol version, but the software implementation version. The software version field consists of four decimal numbers separated by periods as follows: Major release number, minor release number, support release number, build number. For example, Version 8.4.3.1 indicates major release 8, minor release 4, support release 3, build number 1. The software version is set when the Admin Mode is enabled.

If you change the mode, click **Submit** to apply the new settings to the system.

## Port Access Control Port Summary

Use this page to view summary information about the port-based authentication settings for each port.

To display the Port Access Control Port Summary page, click **Security > Port Access Control > Port Summary** in the navigation menu.

**Figure 286.** Port Access Control—Port Summary

Interface	Interface Status
1/0/1	N/A
1/0/2	N/A
1/0/3	N/A
1/0/4	N/A
1/0/5	N/A
1/0/6	N/A
1/0/7	N/A
1/0/8	N/A
1/0/9	N/A
1/0/10	N/A

Use the buttons to perform the following tasks:

- To change the port-based access control settings for a port, select the port to configure and click **Edit**. You are automatically redirected to the Port Access Control Port Configuration page for the selected port. See “Port Configuration” on page 431.

- To view additional information about the port-based access control settings for a port, select the port with the information to view and click **Details**. You are automatically redirected to the Port Access Control Port Details page for the selected port. See “Port Details” on page 433.

**Table 281.** Port Access Control—Port Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
Interface Status	The authorization status of the port, which is one of the following: <ul style="list-style-type: none"> <li>• Unauthorized</li> <li>• Authorized</li> <li>• N/A</li> </ul>

Use the **Refresh** button to refresh the page with the most current data from the switch.

## Port Configuration

Use the Port Access Control Port Configuration page to enable and configure port access control on one or more ports.

To access the Port Based Access Control Port Configuration page, click **Security > Port Access Control > Port Configuration** in the navigation menu.

**Figure 287.** Port Access Control Port Configuration

The screenshot shows the 'Port Access Control Port Configuration' page. At the top, there are navigation tabs: Configuration, Port Summary, Port Configuration (highlighted), Port Details, Statistics, and Privileges Summary. Below the tabs is a red header with the text 'Port Access Control Port Configuration'. The main content area is divided into several sections:

- Interface:** 1/0/1 (dropdown)
- Protocol Version:** 2
- PAE Capabilities:** Authenticator (with an edit icon)
- Authenticator Options:**
  - Quiet Period (Seconds): 60 (range: 0 to 65535)
  - Transmit Period (Seconds): 30 (range: 1 to 65535)
  - Supplicant Timeout (Seconds): 30 (range: 1 to 65535)
  - Server Timeout (Seconds): 30 (range: 1 to 65535)
  - Maximum Requests: 2 (range: 1 to 20)
  - Maximum Request Identity: 2 (range: 1 to 20)
  - Key Transmission: Disabled
- Supplicant Options:**
  - Control Mode:  Force Unauthorized  Force Authorized  Auto
  - Supplicant PACP State: Initialize
  - User Name: None (dropdown)
  - Authentication Period (Seconds): 90 (range: 1 to 65535)
  - Start Period (Seconds): 30 (range: 1 to 65535)
  - Held Period (Seconds): 60 (range: 1 to 65535)
  - Maximum Start Messages: 3 (range: 1 to 10)

At the bottom of the form, there are three buttons: Submit, Refresh, and Cancel.

**Table 282.** Port Access Control Port Configuration Fields

Field	Description
Interface	The interface with the settings to view or configure. If you have been redirected to this page, this field is read-only and displays the interface that was selected on the Port Access Control Port Summary page.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the Dot1x specification.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Authenticator</b> – The port enforces authentication and passes authentication information from a remote supplicant (client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access.</li> <li>• <b>Supplicant</b> – The port is connected to an authenticator port and must be granted permission by the authentication server before it can send and receive traffic through the remote port.</li> </ul> To change the PAE capabilities of a port, click the <b>Edit</b> icon associated with the field and select the desired setting from the menu in the Set PAE Capabilities window.
Authenticator Options	The fields in this section can be changed only when the selected port is configured as an authenticator port (that is, the PAE Capabilities field is set to Authenticator).
Quiet Period	The number of seconds that the port remains in the quiet state following a failed authentication exchange.
Transmit Period	The value, in seconds, of the timer used by the authenticator state machine on the port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant.
Supplicant Timeout	The amount of time that the port waits for a response before retransmitting an EAP request frame to the client.
Server Timeout	The amount of time the port waits for a response from the authentication server.
Maximum Requests	The maximum number of times that the port sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
Maximum Request Identity	The maximum number of times the port will transmit an EAP Request-Identity frame before timing out the supplicant.
Key Transmission	Indicates if the key is transmitted to the supplicant for the specified port.
Supplicant Options	The fields in this section can be changed only when the selected port is configured as a supplicant port (that is, the PAE Capabilities field is set to Supplicant).
Control Mode	The port-based access control mode on the port, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Auto</b> – The port is unauthorized until a successful authentication exchange has taken place.</li> <li>• <b>Force Unauthorized</b> – The port ignores supplicant authentication attempts and does not provide authentication services to the client.</li> <li>• <b>Force Authorized</b> – The port sends and receives normal traffic without client <b>port-based authentication</b>.</li> </ul>



**Table 282.** *Port Access Control Port Configuration Fields (continued)*

Field	Description
Supplicant PACP State	Current state of the supplicant PACP state machine, which is one of the following: <ul style="list-style-type: none"><li>• Initialize</li><li>• Logoff</li><li>• Held</li><li>• Unauthenticated</li><li>• Authenticating</li><li>• Authenticated</li></ul>
Authentication Period	The amount of time the supplicant port waits to receive a challenge from the authentication server. If the configured Authentication Period expires, the supplicant retransmits the authentication request until it is authenticated or has sent the number of messages configured in the Maximum Start Messages field.
Start Period	The amount of time the supplicant port waits for a response from the authenticator port after sending a Start packet. If no response is received, the supplicant retransmits the Start packet.
Held Period	The amount of time the supplicant port waits before contacting the authenticator port after an active 802.1X session fails.
Maximum Start Messages	The maximum number of Start packets the supplicant port sends to the authenticator port without receiving a response before it considers the authenticator to be 802.1X-unaware.

### Command Buttons

- Click **Refresh** to update the information on the screen with the most current information from the device.
- If you make changes to the page, click **Submit** to apply the changes to the system.

## Port Details

Use this page to view 802.1X information for a specific port.

To access the Port Access Control Port Details page, click **Security > Port Access Control > Port Details** in the navigation menu.

**Figure 288.** Port Access Control Port Details

Port Access Control Port Details	
Interface	1/0/1 ▼
PAE Capabilities	Authenticator
Authenticator Options	
Quiet Period (Seconds)	60
Transmit Period (Seconds)	30
Supplicant Timeout (Seconds)	30
Server Timeout (Seconds)	30
Maximum Requests	2
Maximum Request Identity	2
Key Transmission	Disabled

[Refresh](#)

**Table 283.** Port Access Control Port Details Fields

Field	Description
Interface	The interface associated with the rest of the data on the page.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Authenticator</b> – The port enforces authentication and passes authentication information from a remote supplicant (client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access.</li> <li>• <b>Supplicant</b> – The port is connected to an authenticator port and must be granted permission by the authentication server before it can send and receive traffic through the remote port.</li> </ul>
Authenticator Options	The fields in this section are displayed only when the selected port is configured as an 802.1X authenticator (that is, the PAE Capabilities field is set to <b>Authenticator</b> .)
Quiet Period	The number of seconds that the port remains in the quiet state following a failed authentication exchange.
Transmit Period	The value, in seconds, of the timer used by the authenticator state machine on the port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant.
Supplicant Timeout	The amount of time that the port waits for a response before retransmitting an EAP request frame to the client.
Server Timeout	The amount of time the port waits for a response from the authentication server.
Maximum Requests	The maximum number of times that the port sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
Maximum Requests Identity	The maximum number of times the port will retransmit an EAP Request-Identity frame before timing out the supplicant.
Key Transmission	Indicates if the key is transmitted to the supplicant for the specified port.
Supplicant Options	The fields in this section are displayed only when the selected port is configured as an 802.1X supplicant port (that is, the PAE Capabilities field is set to Supplicant.)

**Table 283.** *Port Access Control Port Details Fields (continued)*

Field	Description
Control Mode	The port-based access control mode on the port, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Auto</b> – The port is unauthorized until a successful authentication exchange has taken place.</li> <li>• <b>Force Unauthorized</b> – The port ignores supplicant authentication attempts and does not provide authentication services to the client.</li> <li>• <b>Force Authorized</b> – The port sends and receives normal traffic without client port-based authentication.</li> </ul>
Supplicant PACP State	Current state of the supplicant PACP state machine, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Initialize</b></li> <li>• <b>Logoff</b></li> <li>• <b>Held</b></li> <li>• <b>Unauthenticated</b></li> <li>• <b>Authenticating</b></li> <li>• <b>Authenticated</b></li> </ul>
Authentication Period	The amount of time the supplicant port waits to receive a challenge from the authentication server. If the configured Authentication Period expires, the supplicant retransmits the authentication request until it is authenticated or has sent the number of messages configured in the Maximum Start Messages field.
Start Period	The amount of time the supplicant port waits for a response from the authenticator port after sending a Start packet. If no response is received, the supplicant retransmits the Start packet.
Held Period	The amount of time the supplicant port waits before contacting the authenticator port after an active 802.1X session fails.
Maximum Start Messages	The maximum number of Start packets the supplicant port sends to the authenticator port without receiving a response before it considers the authenticator to be 802.1X-unaware.

### Command Buttons

- Click **Refresh** to update the information on the screen.

## Statistics

Use this page to view information about the Extensible Authentication Protocol over LAN (EAPOL) frames and EAP messages sent and received by the local interfaces. To view additional per-interface EAPOL and EAP message statistics, select the interface with the information to view and click **Details**.

To access the Port Access Control Statistics page, click **Security > Port Access Control > Statistics** in the navigation menu.

**Figure 289.** Port Access Control Statistics

Interface	PAE Capabilities	EAPOL Frames Received	EAPOL Frames Transmitted	Last EAPOL Frame Version
1/0/1	Authenticator	0	0	0
1/0/2	Authenticator	0	0	0
1/0/3	Authenticator	0	0	0
1/0/4	Authenticator	0	0	0
1/0/5	Authenticator	0	0	0
1/0/6	Authenticator	0	0	0
1/0/7	Authenticator	0	0	0
1/0/8	Authenticator	0	0	0
1/0/9	Authenticator	0	0	0
1/0/10	Authenticator	0	0	0

**Table 284.** Port Access Control Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing detailed information for an interface, this field identifies the interface being viewed.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: <ul style="list-style-type: none"> <li><b>Authenticator</b> – The port enforces authentication and passes authentication information from a remote supplicant (similar to a client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access.</li> <li><b>Supplicant</b> – The port must be granted permission by the authentication server before it can access the remote authenticator port.</li> </ul>
EAPOL Frames Received	The total number of valid EAPOL frames received on the interface.
Last EAPOL Frame Version	The total number of EAPOL frames sent by the interface.
Last EAPOL Frame Source	The source MAC address attached to the most recently received EAPOL frame.
After you click <b>Details</b> , a window opens and displays additional information about the EAPOL and EAP messages the interface sends and receives. The following information describes the additional fields that appear in the Details window. The fields this window displays depend on whether the interface is configured as an authenticator or supplicant, as noted in the applicable field descriptions.	
EAPOL Start Frames Received	The total number of EAPOL-Start frames received on the interface. EAPOL-Start frames are sent by a supplicant to initiate the 802.1X authentication process when it connects to the interface. This field is displayed only if the interface is configured as an authenticator.

**Table 284.** *Port Access Control Statistics Fields (continued)*

Field	Description
EAPOL Logoff Frames Received	The total number of EAPOL-Logoff frames received on the interface. EAPOL-Logoff frames are sent by a supplicant to indicate that it is disconnecting from the network, and the interface can return to the unauthorized state. This field is displayed only if the interface is configured as an authenticator.
EAP Response/ID Frames Received	The total number of EAP-Response Identity frames the interface has received. EAP-Response Identity frames are sent by a supplicant to provide user information that is used to for authentication. This field is displayed only if the interface is configured as an authenticator.
EAP Response Frames Received	The total number of EAP-Response frames the interface has received. EAP-Response frames are sent from a supplicant to an authentication server during the authentication process. This field is displayed only if the interface is configured as an authenticator.
EAP Request/ID Frames Transmitted	The total number of EAP-Request Identity frames the interface has sent. EAP-Request Identity frames are sent from an authenticator to a supplicant to request user information that is used to for authentication. This field is displayed only if the interface is configured as an authenticator.
EAPOL Start Frames Transmitted	The total number of EAPOL-Start frames the interface has sent to a remote authenticator. EAPOL-Start frames are sent by a supplicant to initiate the 802.1X authentication process when it connects to the interface. This field is displayed only if the interface is configured as a supplicant.
EAPOL Logoff Frames Transmitted	The total number of EAPOL-Logoff frames the interface has sent to a remote authenticator. EAPOL-Logoff frames are sent by a supplicant to indicate that it is disconnecting from the network, and the interface can return to the unauthorized state. This field is displayed only if the interface is configured as a supplicant.
EAP Response/ID Frames Transmitted	The total number of EAP-Response Identity frames the interface has sent. EAP-Response Identity frames are sent by a supplicant to provide user information that is used to for authentication. This field is displayed only if the interface is configured as a supplicant.
EAP Request/ID Frames Received	The total number of EAP-Request Identity frames the interface has received. EAP-Request Identity frames are sent from an authenticator to a supplicant to request user information that is used to for authentication. This field is displayed only if the interface is configured as a supplicant.
EAP Request Frames Received	The total number of EAP-Request frames the interface has received. EAP-Request frames are sent from the authentication server to the supplicant during the authentication process. This field is displayed only if the interface is configured as a supplicant.
Invalid EAPOL Frames Received	The number of unrecognized EAPOL frames received on the interface.
EAPOL Length Error Frames Received	The number of EAPOL frames with an invalid packet body length received on the interface.
Clear (Button)	Resets all statistics counters to 0 for the selected interface or interfaces.

### Command Buttons

- Click **Refresh** to update the information on the screen.

## Privileges Summary

Use this page to grant or deny port access to users configured on the system. To change the access control privileges for one or more ports, select each interface to configure and click **Edit**. The same settings are applied to all selected interfaces.

To access the Port Access Control Privileges Summary page, click **Security > Port Access Control > Privileges Summary** in the navigation menu.

**Figure 290.** Port Access Control Privileges Summary

Interface	Users
1/0/1	admin, guest
1/0/2	admin, guest
1/0/3	admin, guest
1/0/4	admin, guest
1/0/5	admin, guest
1/0/6	admin, guest
1/0/7	admin, guest
1/0/8	admin, guest
1/0/9	admin, guest
1/0/10	admin, guest

**Table 285.** Port Access Control Privileges Summary Fields

Field	Description
Interface	The local interface associated with the rest of the data in the row. When configuring access information for one or more interfaces, this field identifies each interface being configured.
Users	The users that are allowed access to the system through the associated port. When configuring user access for a port, the Available Users field lists the users configured on the system that are denied access to the port. The users in the Selected Users field are allowed access. To move a user from one field to the other, click the user to move (or CTL + click to select multiple users) and click the appropriate arrow.

### Command Buttons

- Click **Refresh** to update the information on the screen.

# RADIUS Settings

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. The RADIUS server maintains a user database, which contains per-user authentication information. RADIUS servers provide a centralized authentication method for:

- Telnet Access
- Web Access
- Console to Switch Access
- Port Access Control (802.1X)

The RADIUS folder contains links to pages that help you view and configure system RADIUS settings.

## RADIUS Configuration

Use the RADIUS Configuration page to view and configure various settings for the RADIUS servers configured on the system.

To access the RADIUS **Configuration** page, click **Security > RADIUS > Configuration** in the navigation menu.

**Figure 291.** RADIUS Configuration

RADIUS Attributes	
NAS-IP-ADDRESS (Attribute 4)	Mode: Disable, Value: 0.0.0.0
CALLED-STATION-ID (Attribute 30)	MAC Format: Legacy Lowercase
CALLING-STATION-ID (Attribute 31)	MAC Format: Legacy Lowercase
NAS-IDENTIFIER (Attribute 32 MAC Format)	MAC Format: Legacy Lowercase
NAS-IDENTIFIER (Attribute 32 Include in Access/Accounting Request)	Include in Access/Accounting Request: Disable, Format: %m
ACCT-SESSION-ID (Attribute 44)	Include in Access/Accounting Request: Disable
NAS-IPV6-ADDRESS (Attribute 95)	Mode: Disable, Value: ::

**Table 286.** RADIUS Configuration Fields

Field	Description
Max Number of Retransmits	The maximum number of times the RADIUS client on the device will retransmit a request packet to a configured RADIUS server after a response is not received. If multiple RADIUS servers are configured, the max retransmit value will be exhausted on the first server before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS server equals the sum of (retransmit × timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.
Timeout Duration	The number of seconds the RADIUS client waits for a response from the RADIUS server. Consideration to maximum delay time should be given when configuring RADIUS timeout and RADIUS max retransmit values.
Accounting Mode	Specifies whether the RADIUS accounting mode on the device is enabled or disabled.
MAB Attribute	<p>The RADIUS attribute 1 (User-Name) for sending MAC-based Authentication Bypass (MAB) requests from the client to the RADIUS server.</p> <p>The authenticator sends a request to the authentication server with the MAC address of the client (by default 'hh:hh:hh:hh:hh:hh') as the User-Name. This attribute is sent irrespective of the authentication type configured on the MAB interface.</p> <p>To configure the MAB attribute format, click the <b>Edit</b> icon and enter the desired settings in the available fields. To reset the MAB attribute to the default values, click the <b>Reset</b> icon and confirm the action. After you click <b>Edit</b>, the Set MAB Attribute window appears and includes the following fields:</p> <ul style="list-style-type: none"> <li>• Group Size—The group size used by the switch to format the RADIUS attribute 1 (User-Name) of the MAB request. The size is the number of characters included in a group. <ul style="list-style-type: none"> <li>– In the following example, the group size is 1: 0:0:1:0:1:8:9:9:F:2:B:3</li> <li>– In the following example, the group size is 2: 00:10:18:99:F2:B3</li> <li>– In the following example, the group size is 4: 0010:1899:F2B3</li> <li>– In the following example, the group size is 12: 00101899F2B3</li> </ul> </li> <li>• Separator—The separator used by the switch to format the RADIUS attribute 1 (User-Name) of the MAB request. <ul style="list-style-type: none"> <li>– In the following example, the separator is - (hyphen): 00-10-18-99-F2-B3</li> <li>– In the following example, the separator is : (colon): 00:10:18:99:F2:B3</li> </ul> </li> <li>• Case—The case of any letters used by the switch to format the RADIUS attribute 1 (User-Name) of the MAB request. <ul style="list-style-type: none"> <li>– In the following example, the case is lowercase: 00:d0:18:99:f2:b3</li> <li>– In the following example, the case is uppercase: 00:D0:18:99:F2:B3</li> </ul> </li> </ul>
RADIUS Attributes	



**Table 286.** RADIUS Configuration Fields (continued)

Field	Description
NAS-IP-ADDRESS (Attribute 4)	The network access server (NAS) IP address for the RADIUS server. To specify an address, click the <b>Edit</b> icon and enter the IP address of the NAS in the available field. The address should be unique to the NAS within the scope of the RADIUS server. The NAS IP address is used only in Access-Request packets. To reset the NAS IP address to the default value, click the Reset icon and confirm the action.
CALLED-STATION-ID (Attribute 30)	Specifies the format in which the MAC address is sent to the RADIUS server in attribute 30. To specify a format, click the <b>Edit</b> icon and select one of the following: <ul style="list-style-type: none"> <li>Legacy Lowercase – Format the MAC address as xx:xx:xx:xx:xx:xx</li> <li>Legacy Uppercase – Format the MAC address as XX:XX:XX:XX:XX:XX</li> <li>IETF Lowercase – Format the MAC address as xx-xx-xx-xx-xx-xx</li> <li>IETF Uppercase – Format the MAC address as XX-XX-XX-XX-XX-XX</li> <li>Unformatted Lowercase – Format the MAC address as aaaabbbbcccc</li> <li>Unformatted Uppercase – Format the MAC address as AAAABBBBCCCC</li> </ul>
CALLING-STATION-ID (Attribute 31)	Specifies the format in which the MAC address is sent to the RADIUS server in attribute 31 (Calling-Station-ID). To specify a format, click the <b>Edit</b> icon and select one of the following: <ul style="list-style-type: none"> <li>Legacy Lowercase – Format the MAC address as xx:xx:xx:xx:xx:xx</li> <li>Legacy Uppercase – Format the MAC address as XX:XX:XX:XX:XX:XX</li> <li>IETF Lowercase – Format the MAC address as xx-xx-xx-xx-xx-xx</li> <li>IETF Uppercase – Format the MAC address as XX-XX-XX-XX-XX-XX</li> <li>Unformatted Lowercase – Format the MAC address as aaaabbbbcccc</li> <li>Unformatted Uppercase – Format the MAC address as AAAABBBBCCCC</li> </ul>
NAS-IDENTIFIER (Attribute 32 MAC Format)	Specifies the format in which the MAC address is sent to the RADIUS server in attribute 32 (NAS-Identifier). To specify a format, click the <b>Edit</b> icon and select one of the following: <ul style="list-style-type: none"> <li>Legacy Lowercase – Format the MAC address as xx:xx:xx:xx:xx:xx</li> <li>Legacy Uppercase – Format the MAC address as XX:XX:XX:XX:XX:XX</li> <li>IETF Lowercase – Format the MAC address as xx-xx-xx-xx-xx-xx</li> <li>IETF Uppercase – Format the MAC address as XX-XX-XX-XX-XX-XX</li> <li>Unformatted Lowercase – Format the MAC address as aaaabbbbcccc</li> <li>Unformatted Uppercase – Format the MAC address as AAAABBBBCCCC</li> </ul>

**Table 286.** RADIUS Configuration Fields (continued)

Field	Description
NAS-IDENTIFIER (Attribute 32 Include in Access/Accounting Request)	<p>Determines whether the RADIUS attribute 32 (NAS-Identifier) is sent to the RADIUS server in access-request and accounting-request messages and in which format.</p> <p>To configure the settings, click the <b>Edit</b> icon and configure the following:</p> <ul style="list-style-type: none"><li>• <b>Include in Access/Accounting Request</b>—When selected, the attribute is sent to the RADIUS server in access-request and accounting-request messages.</li><li>• <b>Format</b>—Configures the format of an optional string sent in access-request and accounting-request messages in attribute 32 (NAS-Identifier). The format can be one of the following:<ul style="list-style-type: none"><li>– %m – MAC address</li><li>– %i – IP address</li><li>– %h – Host name</li><li>– %d – Domain name</li><li>– Any String – A string including any or all of the above formatting options</li></ul></li></ul> <p>If you configure the format, the string sent in attribute 32 (NAS-Identifier) includes a MAC address, an IP address, a Host name or a Domain name based on the configured format.</p>
ACCT-SESSION-ID (Attribute 44)	<p>Determines whether the RADIUS attribute 44 (ACCT-SESSION-ID) is sent to the RADIUS server in access-request and accounting-request messages.</p> <p>To configure the settings, click the <b>Edit</b> icon and select the option to indicate that the attribute should be included in the messages. Clear the option to prevent the attribute from being sent.</p>
NAS-IPV6-ADDRESS (Attribute 95)	<p>The network access server (NAS) IPv6 address for the RADIUS server.</p> <p>If the specific IPv6 address is configured while enabling this attribute, the RADIUS client uses that IPv6 address while sending NAS-IPV6-Address attribute in RADIUS communication. The address should be unique to the NAS within the scope of the RADIUS server.</p>

Use the buttons at the bottom of the page to perform the following actions:

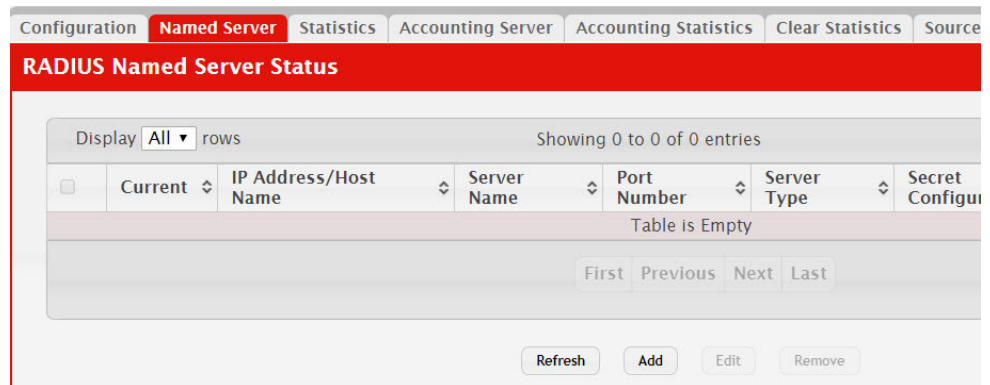
- Click **Refresh** to update the page with the most current information.
- If you make changes to the page, click **Submit** to apply the changes to the system.

## Named Server Status

The RADIUS Named Server Status page shows summary information about the RADIUS servers configured on the system.

To access the RADIUS Named Server Status page, click **Security > RADIUS > Named Server** in the navigation menu.

**Figure 292.** Named Server Status



Use the buttons to perform the following tasks:

- To add a RADIUS authentication server to the list of servers the RADIUS client can contact, click **Add**.
- To change the settings for a configured RADIUS server, select the entry to modify and click **Edit**. You cannot change the IP address or host name for a server after it has been added.
- To remove a configured RADIUS server from the list, select the entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 287.** RADIUS Server Status Fields

Field	Description
Current	An asterisk (*) in the column Indicates that the server is the current server for the authentication server group. If no asterisk is present, the server is a backup server.  If more than one RADIUS server is configured with the same name, the switch selects one of the servers to be the current server from the group of servers with the same name.  When the switch sends a RADIUS request to the named server, the request is directed to the server selected as the current server. Initially the primary server is selected as the current server. If the primary server fails, one of the other servers becomes the current server.
RADIUS Server Host Address	Shows the IP address of the RADIUS server.
RADIUS Server Name	Shows the RADIUS server name. Multiple RADIUS servers can have the same name. In this case, RADIUS clients can use RADIUS servers with the same name as backups for each other.
Port Number	Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.
Server Type	Shows whether the server is a Primary or Secondary server.
Secret Configured	Indicates whether the shared secret for this server has been configured.
Message Authenticator	Shows whether the message authenticator attribute for the selected server is enabled or disabled.

Click **Refresh** to update the page with the most current information.

## Server Statistics

Use the RADIUS Server Statistics page to view statistical information for each RADIUS server configured on the system.

To access the RADIUS Server Statistics page, click **Security > RADIUS > Statistics** in the navigation menu.

**Figure 293.** RADIUS Server Statistics

**Table 288.** RADIUS Server Statistics Fields

Field	Description
IP Address/Host Name	The IP address or host name of the RADIUS server associated with the rest of the data in the row. When viewing the detailed statistics for a RADIUS server, this field identifies the RADIUS server.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to the server. This number does not include retransmissions.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from the server.
Pending Requests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response.
Timeouts	The number of times a response was not received from the server within the configured timeout value.
Packets Dropped	The number of RADIUS packets received from the server on the authentication port and dropped for some other reason.
Access Retransmissions	The number of RADIUS Access-Request packets that had to be retransmitted to the server because the initial Access-Request packet failed to be successfully delivered.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from the server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from the server.

**Table 288.** RADIUS Server Statistics Fields (continued)

Field	Description
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators, signature attributes, and unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from the server.
Unknown Types	The number of RADIUS packets of unknown type which were received from the server on the authentication port.

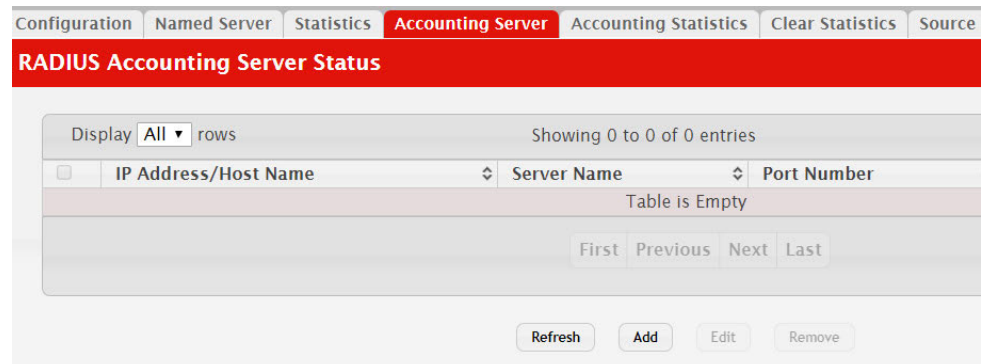
Click **Refresh** to update the page with the most current information.

## Named Accounting Server Status

The RADIUS Named Accounting Server Status page shows summary information about the accounting servers configured on the system.

To access the RADIUS Accounting Server Status page, click **Security > RADIUS > Accounting Server** in the navigation menu.

**Figure 294.** RADIUS Accounting Server Status



Use the buttons to perform the following tasks:

- To add a RADIUS accounting server to the list of servers the RADIUS client can contact, click **Add**.
- To change the settings for a configured RADIUS accounting server, select the entry to modify and click **Edit**. You cannot change the IP address or host name for a server after it has been added.
- To remove a configured RADIUS accounting server from the list, select the entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 289.** RADIUS Accounting Server Status Fields

Field	Description
IP Address/Host Name	The IP address or host name of the RADIUS accounting server. Host names must be resolvable by DNS and are composed of a series of labels separated by dots.
Server Name	The name of the RADIUS accounting server. RADIUS servers that are configured with the same name are members of the same named RADIUS server group. RADIUS accounting servers in the same group serve as backups for each other.
Port Number	The UDP port on the RADIUS accounting server to which the local RADIUS client sends request packets.
Secret Configured	Indicates whether the shared secret for this server has been configured.
Secret	The shared secret text string used for authenticating and encrypting all RADIUS communications between the RADIUS client on the device and the RADIUS accounting server. The secret specified in this field must match the shared secret configured on the RADIUS accounting server.

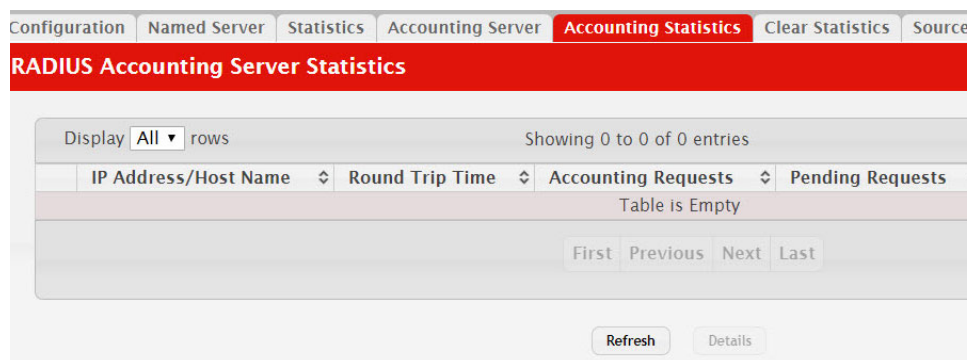
Click **Refresh** to update the page with the most current information.

## Accounting Statistics

Use the RADIUS Accounting Statistics page to view statistical information for each RADIUS server configured on the system.

To access the RADIUS Accounting Statistics page, click **Security > RADIUS > Accounting Statistics** in the navigation menu.

**Figure 295.** RADIUS Accounting Statistics



**Table 290.** RADIUS Accounting Statistics Fields

Field	Description
IP Address/Host Name	The IP address or host name of the RADIUS accounting server associated with the rest of the data in the row. When viewing the detailed statistics for a RADIUS accounting server, this field identifies the server.

**Table 290.** RADIUS Accounting Statistics Fields (continued)

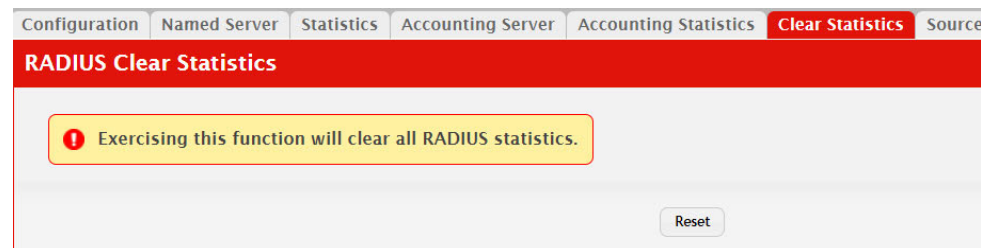
Field	Description
Round Trip Time	Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Accounting Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Pending Requests	The number of RADIUS Accounting-Request packets destined for the server that have not yet timed out or received a response.
Timeouts	The number of times a response was not received from the server within the configured timeout value.
Packets Dropped	The number of RADIUS packets received from the server on the accounting port and dropped for some other reason.
Accounting Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to the server.
Accounting Responses	The number of RADIUS packets received on the accounting port from the server.
Timeouts	The number of accounting timeouts to this server.
Malformed Access Responses	The number of malformed RADIUS Accounting-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets that contained invalid authenticators received from the accounting server.
Unknown Types	The number of RADIUS packets of unknown type which were received from the server on the accounting port.

## Clear Statistics

Use the RADIUS Clear Statistics page to reset all RADIUS authentication and accounting statistics to zero.

To access the RADIUS Clear Statistics page, click **Security > RADIUS > Clear Statistics** in the navigation menu.

**Figure 296.** RADIUS Clear Statistics



To clear all statistics for the RADIUS authentication and accounting server, click **Reset**. After you confirm the action, the statistics on both the **RADIUS Server Statistics** and **RADIUS Accounting Server Statistics** pages are reset.

## Source Interface Configuration

Use this page to specify the physical or logical interface to use as the RADIUS client source interface. When an IP address is configured on the source interface, this address is used for all RADIUS communications between the local RADIUS client and the remote RADIUS server. The IP address of the designated source interface is used in the IP header of RADIUS management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device.

To access the RADIUS Source Interface Configuration page, click **Security > RADIUS > Source Interface Configuration** in the navigation menu.

**Figure 297.** RADIUS Source Interface Configuration

**Table 291.** RADIUS Source Interface Configuration Fields

Field	Description
Type	The type of interface to use as the source interface: <ul style="list-style-type: none"> <li>• <b>None</b> – The primary IP address of the originating (outbound) interface is used as the source address.</li> <li>• <b>Interface</b> – The primary IP address of a physical port is used as the source address.</li> <li>• <b>VLAN</b> – The primary IP address of a VLAN routing interface is used as the source address.</li> <li>• <b>Loopback</b> – The primary IP address of the loopback interface is used as the source address. A loopback is always reachable, as long as any routing interface is up.</li> <li>• <b>Network</b> – The network source IP is used as the source address.</li> <li>• <b>Service Port</b> – The management port source IP is used as the source address.</li> </ul>
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.
Loopback Interface	When the selected Type is Loopback, select the loopback interface to use as the source interface.

Click **Refresh** to update the page with the most current information.



# TACACS+ Settings

To access the TACACS+ Configuration page, click **Security > TACACS+ > Configuration** in the navigation menu.

**Figure 298.** TACACS+ Configuration

Configuration | Server Summary | Server Configuration | Source Interface Configuration

### TACACS+ Configuration

Key String	<input type="text"/>		
Connection Timeout	<input type="text" value="5"/>	(1 to 30 secs)	

Submit Refresh Cancel

**Table 292.** TACACS+ Configuration Fields

Field	Description
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The key must match the key configured on the TACACS+ server.
Connection Timeout	The maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server.

Click **Refresh** to update the page with the most current information.

If you make any changes to the page, click **Submit** to apply the changes to the system.

# TACACS+ Server Summary

Use this page to view and configure information about the TACACS+ Server(s).

To access the TACACS+ Server Summary page, click **Security > TACACS+ > Server Summary** in the navigation menu.

**Figure 299.** TACACS+ Server Summary

Configuration | Server Summary | Server Configuration | Source Interface Configuration

### TACACS+ Server Summary

Display All rows Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Server	Priority	Port	Connection Timeout
Table is Empty				

First Previous Next Last

Refresh Add Edit Remove

Use the buttons to perform the following tasks:

- To add a TACACS+ Server to the list of servers the TACACS+ client can contact, click **Add**. If maximum number of server is added, the button will be disabled
- To edit a configured TACACS+ server from the list, select the entry and click **Edit**.
- To remove a configured TACACS+ server from the list, select the entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 293.** TACACS+ Server Summary Fields

Field	Description
Server	Specifies the TACACS+ Server IP address or Hostname.
Priority	Specifies the order in which the TACACS+ servers are used.
Port	Specifies the authentication port.
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The key must match the encryption used on the TACACS+ server.
Connection Timeout	The amount of time that passes before the connection between the device and the TACACS+ server time out.

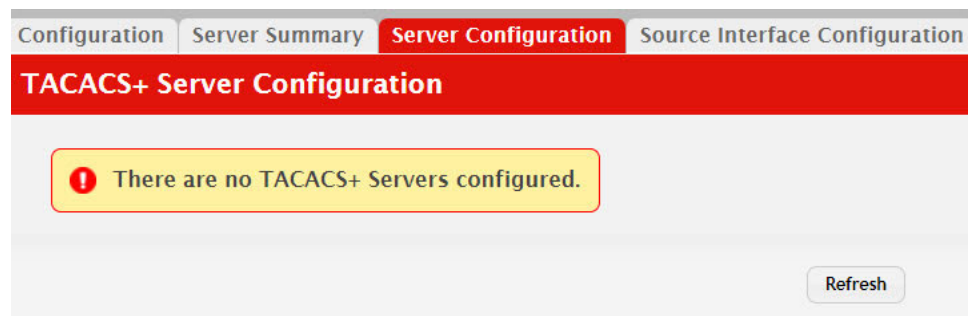
Click **Refresh** to update the page with the most current information.

## TACACS+ Server Configuration

Use this page to view and configure information about the TACACS+ Server(s).

To access the TACACS+ Server Configuration page, click **Security > TACACS+ > Server Configuration** in the navigation menu.

**Figure 300.** TACACS+ Server Configuration



**Table 294.** TACACS+ Server Configuration Fields

Field	Description
Server	Specifies the TACACS+ Server IP address or Hostname.
Priority	Specifies the order in which the TACACS+ servers are used.
Port	Specifies the authentication port.
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The key must match the encryption used on the TACACS+ server.

**Table 294.** TACACS+ Server Configuration Fields (continued)

Field	Description
Connection Timeout	The amount of time that passes before the connection between the device and the TACACS+ server time out.

Click **Refresh** to update the page with the most current information.

If you make any changes to the page, click **Submit** to apply the changes to the system.

## TACACS+ Source Interface Configuration

Use this page to specify the physical or logical interface to use as the TACACS+ client source interface. When an IP address is configured on the source interface, this address is used for all TACACS+ communications between the local TACACS+ client and the remote TACACS+ server. The IP address of the designated source interface is used in the IP header of TACACS+ management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device.

To access the TACACS+ Source Interface Configuration page, click **Security > TACACS+ > Source Interface Configuration** in the navigation menu.

**Figure 301.** TACACS+ Source Interface Configuration

**Table 295.** TACACS+ Source Interface Configuration Fields

Field	Description
Type	<p>The type of interface to use as the source interface:</p> <ul style="list-style-type: none"> <li>• <b>None</b> – The primary IP address of the originating (outbound) interface is used as the source address.</li> <li>• <b>Interface</b> – The primary IP address of a physical port is used as the source address.</li> <li>• <b>VLAN</b> – The primary IP address of a VLAN routing interface is used as the source address.</li> <li>• <b>Loopback</b> – The primary IP address of the loopback interface is used as the source address. A loopback is always reachable, as long as any routing interface is up.</li> <li>• <b>Network</b> – The network source IP is used as the source address.</li> <li>• <b>Service Port</b> – The management port source IP is used as the source address.</li> </ul>

**Table 295.** TACACS+ Source Interface Configuration Fields (continued)

Field	Description
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.
Loopback Interface	When the selected Type is Loopback, select the loopback interface to use as the source interface.

Click **Refresh** to update the page with the most current information.

If you make any changes to the page, click **Submit** to apply the changes to the system. These changes will not be retained across a power cycle unless a Save Configuration is performed.

# Authentication Manager

The Authentication Manager feature allows you to configure the authentication methods used on the individual interface.

## Authentication Manager Configuration

Use this page to control the administrative mode of the Authentication Manager feature, which enables configuration of the sequence and priority of the authentication methods per interface.

To access the **Authentication Manager Configuration** page, click **Security > Authentication Manager > Configuration** in the navigation menu.

**Figure 302.** Authentication Manager Configuration

Configuration	Interface Configuration	Authentication Tiering	Authenticated Clients	Statistics	History
<b>Authentication Manager Configuration</b>					
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
Dynamic VLAN Creation Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
VLAN Assignment Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
Authentication Monitor Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
Critical Recovery Max Re-Authentication	<input type="text" value="10"/> (1 to 50)				
Authenticated Clients	<input type="text" value="0"/>				
Clients in Monitor Mode	<input type="text" value="0"/>				
<input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="Cancel"/>					

**Table 296.** Authentication Manager Configuration Fields

Field	Description
Admin Mode	The administrative mode of the Authentication Manager feature. When Authentication Manager is enabled globally, the authentication methods configured on an interface are executed in the order configured as the device attempts to authenticate clients on that interface.
Dynamic VLAN Creation Mode	The administrative mode of dynamic VLAN creation on the device. If RADIUS-assigned VLANs are enabled, the RADIUS server is expected to include the VLAN ID in the 802.1X tunnel attributes of its response message to the device. If dynamic VLAN creation is enabled on the device and the RADIUS-assigned VLAN does not exist, then the assigned VLAN is dynamically created. This implies that the client can connect from any port and can get assigned to the appropriate VLAN. This feature gives flexibility for clients to move around the network without much additional configuration required.

**Table 296.** *Authentication Manager Configuration Fields (continued)*

Field	Description
VLAN Assignment Mode	The administrative mode of RADIUS-based VLAN assignment on the device. When enabled, this feature allows a port to be placed into a particular VLAN based on the result of the authentication or type of 802.1X authentication a client uses when it accesses the device. The authentication server can provide information to the device about which VLAN to assign the client.
Authentication Monitor Mode	The administrative mode of the Monitor Mode feature on the device. Monitor mode is a special mode that can be enabled in conjunction with port-based access control. Monitor mode provides a way for network administrators to identify possible issues with the port-based access control configuration on the device without affecting the network access to the users of the device. It allows network access even in cases where there is a failure to authenticate, but it logs the results of the authentication process for diagnostic purposes. If the device fails to authenticate a client for any reason (for example, RADIUS access reject from the RADIUS server, RADIUS timeout, or the client itself is 802.1X unaware), the client is authenticated and is undisturbed by the failure condition(s). The reasons for failure are logged and buffered into the local logging database for tracking purposes.
Critical Recovery Max Re-Authentication	The number of critical recovery maximum client re-authentications per second.
Authenticated Clients	The total number of clients authenticated on the switch except the ones in the Monitor mode.
Clients in Monitor Mode	The number of clients authorized by the Monitor mode on the switch.

Use the buttons at the bottom of the page to perform the following actions:

- Click **Submit** to apply the settings to the running configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save configuration** is performed.
- Click **Refresh** to display the latest information from the switch.
- Click **Cancel** to cancel the change.

## Authentication Manager Interface Configuration

Use this page to configure the Authentication Manager interface.

To access the **Authentication Manager Interface Configuration** page, click **Security > Authentication Manager > Interface Configuration** in the navigation menu.

**Figure 303.** Authentication Manager Interface Configuration

Configuration **Interface Configuration** Authentication Tiering Authenticated Clients Statistics History

**Authentication Manager Interface Configuration**

Interface	1/0/1 ▾
Control Mode	<input type="radio"/> Force Unauthorized <input type="radio"/> Force Authorized <input checked="" type="radio"/> Auto
Host Mode	Multiple Domain/Host ▾
Re-Authentication	<input type="checkbox"/>
Re-Authentication Period (Seconds)	<input type="text"/> (1 to 65535)
Re-Authentication Timeout from Server	<input checked="" type="checkbox"/>
Maximum Users	48 (1 to 48)
Guest VLAN ID	0 (1 to 4093), 0 for None
Authentication Retry Attempts	3 (1 to 5)
Unauthenticated VLAN ID	0 (1 to 4093), 0 for None
Authentication Violation Mode	<input type="radio"/> Protect <input checked="" type="radio"/> Restrict <input type="radio"/> Shutdown
Authentication Server Alive Action	<input checked="" type="radio"/> None <input type="radio"/> Reinitialize
Authentication Server Dead Action for Voice	<input checked="" type="radio"/> None <input type="radio"/> Authorize
Authentication Server Dead Action	<input checked="" type="radio"/> None <input type="radio"/> Reinitialize <input type="radio"/> Authorize
Critical VLAN ID	0 (1 to 4093), 0 for None
MAB Mode	<input type="checkbox"/>
Operational MAB Mode	Disabled
MAB Authentication Type	<input checked="" type="radio"/> EAP-MD5 <input type="radio"/> PAP <input type="radio"/> CHAP

Submit Refresh Cancel

**Table 297.** Authentication Manager Interface Configuration Fields

Field	Description
Interface	The interface with the settings to view or configure.
Control Mode	<p>The authentication control mode on the port, which is one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Force Unauthorized</b>—The port ignores supplicant authentication attempts and does not provide authentication services to the client.</li> <li>• <b>Force Authorized</b>—The port sends and receives normal traffic without client port-based authentication.</li> <li>• <b>Auto</b>—The port is unauthorized until a successful authentication exchange has taken place.</li> </ul>

**Table 297.** *Authentication Manager Interface Configuration Fields (continued)*

Field	Description
Host Mode	The authentication host mode on the port determines the number and type of clients that can be authenticated and authorized on the port. The port host mode can be one of the following: <ul style="list-style-type: none"> <li>• <b>Single Authentication</b>—Only one data client can be authenticated on a port and the client is granted access to the port.</li> <li>• <b>Multiple Host</b>—Only one data client can be authenticated on a port. However, once authentication succeeds, access is granted to all clients connected to the port.</li> <li>• <b>Multiple Domain</b>—One data client and one voice client can be authenticated on a port and both clients are granted access to the port.</li> <li>• <b>Multiple Authentication</b>—One voice client and multiple data clients can be authenticated on a port and these clients are granted access to the port.</li> <li>• <b>Multiple Domain/Host</b>—One voice client and one data client can be authenticated on a port and these clients are granted access to the port. However, once a data client is authenticated, access is granted to all clients connected to the port and they are considered data clients.</li> </ul>
Re-Authentication	Indicates if the connected clients can re-authenticate periodically.
Re-Authentication Period (Seconds)	The amount of time that clients can be connected to the port without being re-authenticated. If Re-Authentication is disabled, connected clients are not forced to re-authenticate periodically.
Re-Authentication Timeout from Server	The amount of time, obtained from the RADIUS server, that clients can be connected to the port without being re-authenticated.
Maximum Users	The maximum number of clients supported on the port.
Guest VLAN ID	The VLAN ID for the guest VLAN. The guest VLAN allows the port to provide a distinguished service to unauthenticated users. This feature provides a mechanism to allow users access to hosts on the guest VLAN.
Authentication Retry Attempts	The maximum number of failed client authentication attempts on the port.
Unauthenticated VLAN ID	The VLAN ID of the unauthenticated VLAN. Hosts that fail the authentication might be denied access to the network or placed on a VLAN created for unauthenticated clients. This VLAN might be configured with limited network access and is used for 802.1X aware clients only.
Authentication Violation Mode	The authentication violation mode on the port. The authentication violation can occur when a device tries to connect to a port on which the maximum number of devices has exceeded. Action taken on the port when a security violation occurs can be one of the following: <ul style="list-style-type: none"> <li>• Protect</li> <li>• Restrict</li> <li>• Shutdown</li> </ul>
Authentication Server Alive Action	The action configured on the RADIUS server that is alive after all are dead. The alive-server action can be one of the following: <ul style="list-style-type: none"> <li>• <b>Reinitialize</b>—Dot1x triggers the re-authentication of clients authenticated on the critical VLAN.</li> <li>• <b>None</b>—No action is configured.</li> </ul>



**Table 297.** *Authentication Manager Interface Configuration Fields (continued)*

Field	Description
Authentication Server Dead Action for Voice	The action configured to allow critical voice VLAN support on the port when all the RADIUS servers are marked dead. The dead-server action can be one of the following: <ul style="list-style-type: none"> <li>• <b>Authorize</b>—Allows port access on the voice VLAN when all RADIUS servers are dead.</li> <li>• <b>None</b>—No action is configured.</li> </ul>
Authentication Server Dead Action	The action configured on the RADIUS server that is marked dead. The dead-server action can be one of the following: <ul style="list-style-type: none"> <li>• <b>Reinitialize</b>—Authentication Manager triggers re-authentication of all authenticated clients on the port. Supplicants on voice VLAN, unauthenticated VLAN, and guest VLAN are not disturbed. During re-authentication if all the servers are still dead, the client is authenticated successfully and placed on the critical VLAN.</li> <li>• <b>Authorize</b>—Dot1x authorizes the authenticated clients to the critical VLAN. Clients on the RADIUS assigned VLAN, voice VLAN, unauthenticated VLAN, and guest VLAN are not disturbed. Clients authorized on the port PVID are re-authorized on the critical VLAN.</li> <li>• <b>None</b>—No action is configured.</li> </ul>
Critical VLAN ID	The VLAN ID of the critical VLAN. Critical VLAN allows supplicants to authenticate on the VLAN when all RADIUS servers are dead.
MAB Mode	The MAC-based Authentication Bypass (MAB) mode on the port, which can be enabled or disabled.
Operational MAB Mode	The operational MAB mode on the port.
MAB Authentication Type	The authentication type to be used for MAB access requests sent to the RADIUS server, which is one of the following: <ul style="list-style-type: none"> <li>• <b>CHAP</b>—The port uses CHAP authentication and sends a randomly generated 16-octet challenge as the CHAP-Challenge (RADIUS attribute 60) along with the CHAP-Password (RADIUS attribute 3) to the authentication server.</li> <li>• <b>EAP-MD5</b>—The port uses EAP-MD5 authentication and sends the MD5 hash of the MAC address as the password in the EAP-Message (RADIUS attribute 79) to the authentication server.</li> <li>• <b>PAP</b>—The port uses PAP authentication and sends the MAC address of the client as the password (clear text) in the User-Password (RADIUS attribute 2) to the authentication server.</li> </ul>

Use the buttons at the bottom of the page to perform the following actions:

- Click **Submit** to apply the settings to the running configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save configuration** is performed.
- Click **Refresh** to display the latest information from the switch.
- Click **Cancel** to cancel the change.

## Authentication Tiering

Use this page to configure the sequence and priority of the authentication methods for the interfaces on the device. When Authentication Manager is enabled globally, the authentication methods configured on an interface are executed in the order configured as the device attempts to authenticate clients on that interface. The default method order is Dot1x, MAC Authentication Bypass (MAB), and Captive Portal.

To access the **Authentication Tiering** page, click **Security > Authentication Manager > Authentication Tiering** in the navigation menu.

**Figure 304.** Authentication Tiering

Interface	Configured Order	Enabled Order	Configured Priority	Enabled Priority
1/0/1	Dot1x, MAB		Dot1x, MAB	
1/0/2	Dot1x, MAB		Dot1x, MAB	
1/0/3	Dot1x, MAB		Dot1x, MAB	
1/0/4	Dot1x, MAB		Dot1x, MAB	
1/0/5	Dot1x, MAB		Dot1x, MAB	
1/0/6	Dot1x, MAB		Dot1x, MAB	
1/0/7	Dot1x, MAB		Dot1x, MAB	
1/0/8	Dot1x, MAB		Dot1x, MAB	
1/0/9	Dot1x, MAB		Dot1x, MAB	
1/0/10	Dot1x, MAB		Dot1x, MAB	

**Table 298.** Authentication Tiering Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When editing information for one or more interfaces, this field identifies the interfaces that are being configured.
Configured Order	The order in which the authentication methods are used to authenticate a client connected to an interface, which can be one or more of the following: <ul style="list-style-type: none"> <li>• <b>Dot1x</b> – The port-based authentication method.</li> <li>• <b>MAB</b> – MAC Authentication Bypass method that uses the MAC address of the client to determine the kind of network access to provide.</li> <li>• <b>Captive Portal</b> – The authentication method that prevents clients from accessing the network until user verification has been established.</li> </ul> Captive portal must always be the last method in the list.
Enabled Order	The methods from the list of authentication methods configured on an interface which are administratively enabled in the device.

**Table 298.** *Authentication Tiering Fields (continued)*

Field	Description
Configured Priority	The priority of the authentication methods. The default priority of a method is equivalent to its position in the order of the authentication list configured per interface. If the priority of the methods is changed, all clients authenticated using a lower priority method are forced to re-authenticate.
Enabled Priority	The methods from the list of authentication method priorities configured on an interface which are administratively enabled in the device.
Authenticated Clients	Number of clients authenticated on an interface.
Re-Authentication Timer	Interval, in seconds, after which an attempt is made to authenticate an unauthorized port.

Use the buttons at the bottom of the page to perform the following actions:

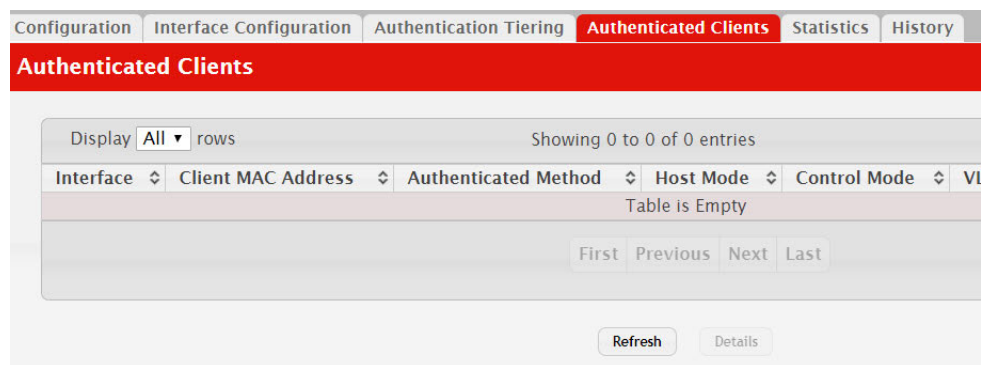
- Click **Refresh** to display the latest information from the switch.
- Click **Edit** to configure the settings for one or more interfaces, select each entry to modify. The settings are applied to all selected interfaces.

## Authenticated Clients

Use this page to view information about the clients connected on the interfaces. If there are no clients connected, the table is empty.

To access the **Authentication Clients** page, click **Security > Authentication Manager > Authenticated Clients** in the navigation menu.

**Figure 305.** Authenticated Clients



**Table 299.** *Authenticated Clients Fields*

Field	Description
Interface	The local interface associated with the rest of the data in the row.
Logical Interface	The logical port number associated with the client that is connected to the port.
Client MAC Address	The MAC address of the client that is connected to the port.

**Table 299.** *Authenticated Clients Fields (continued)*

Field	Description
Authenticated Method	The authentication method used to authenticate a client connected to an interface, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Dot1x</b> – The port-based authentication method.</li> <li>• <b>MAB</b> – MAC Authentication Bypass method that uses the MAC address of the client to determine the kind of network access to provide.</li> <li>• <b>Captive Portal</b> – The authentication method that prevents clients from accessing the network until user verification has been established.</li> </ul>
Authentication State	The current client authentication state, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Success</b> – Indicates authentication succeeded.</li> <li>• <b>Failure</b> – Indicated authentication failed.</li> </ul>
Authentication Status	The client authentication status, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Authorized</b> – Indicates client is authorized on the port.</li> <li>• <b>Unauthorized</b> – Indicates client is not authorized on the port.</li> </ul>

Use the buttons at the bottom of the page to perform the following actions:

- Click **Refresh** to display the latest information from the switch.

## Authenticated Statistics

Use this page to view information about the Authentication Manager client authentication attempts and failures per interface.

To access the **Authentication Statistics** page, click **Security > Authentication Manager > Statistics** in the navigation menu.

**Figure 306.** Authentication Statistics

Configuration	Interface Configuration	Authentication Tiering	Authenticated Clients	Statistics	History
<b>Authentication Statistics</b>					
Display <b>10</b> rows		Showing 1 to 10 of 28 entries			
<input type="checkbox"/>	Interface	Dot1x Attempts	Dot1x Failures	MAB Attempts	
<input type="checkbox"/>	1/0/1	0	0	0	
<input type="checkbox"/>	1/0/2	0	0	0	
<input type="checkbox"/>	1/0/3	0	0	0	
<input type="checkbox"/>	1/0/4	0	0	0	
<input type="checkbox"/>	1/0/5	0	0	0	
<input type="checkbox"/>	1/0/6	0	0	0	
<input type="checkbox"/>	1/0/7	0	0	0	
<input type="checkbox"/>	1/0/8	0	0	0	
<input type="checkbox"/>	1/0/9	0	0	0	
<input type="checkbox"/>	1/0/10	0	0	0	
<div style="text-align: right;"> <span>First</span> <span>Previous</span> <span>1</span> <span>2</span> <span>3</span> <span>Next</span> <span>Last</span> </div> <div style="text-align: center; margin-top: 10px;"> <span>Refresh</span> <span>Clear</span> </div>					

**Table 300.** *Authentication Statistics Fields*

Field	Description
Interface	The interface associated with the rest of the data in the row.
Dot1x Attempts	The number of attempts made to authenticate a client using the Dot1x authentication method.
Dot1x Failures	The number of attempts that failed when Dot1x method is used for client authentication.
MAB Attempts	The number of attempts made to authenticate a client using the MAC Authentication Bypass (MAB) authentication method.
MAB Failures	The number of attempts that failed when MAB method is used for client authentication.
Captive Portal Attempts	The number of attempts made to authenticate a client using the Captive Portal authentication method.
Captive Portal Failures	The number of attempts that failed when Captive Portal method is used for client authentication.

Use the buttons at the bottom of the page to perform the following actions:

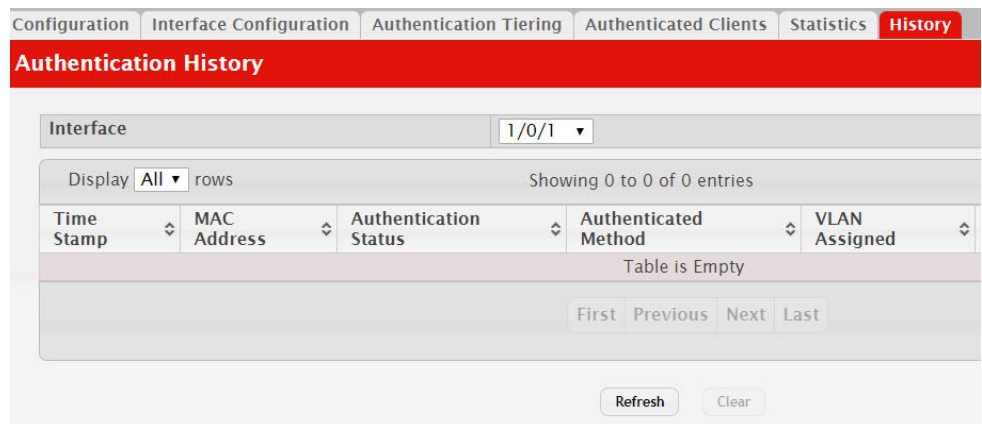
- Click **Refresh** to display the latest information from the switch.
- Click **Clear** to reset all statistics counters to 0 for the selected interfaces.

## Authenticated History

Use this page to view the Authentication Manager history log per interface.

To access the **Authentication History** page, click **Security > Authentication Manager > History** in the navigation menu.

**Figure 307.** Authentication History



**Table 301.** *Authentication History Fields*

Field	Description
Interface	The menu contains all interfaces in the device. To view the history log on a specific interface, select the interface from the menu.
Time Stamp	The absolute time when the authentication event took place.
MAC Address	The MAC address of the client that is connected to the port.

**Table 301.** *Authentication History Fields (continued)*

Field	Description
Authentication Status	The client authentication status, which can be one of the following: <ul style="list-style-type: none"><li>• <b>Authorized</b> – Indicates client is authorized on the port.</li><li>• <b>Unauthorized</b> – Indicates client is not authorized on the port.</li></ul>
Authenticated Method	The authentication method used to authenticate a client connected to an interface, which can be one of the following: <ul style="list-style-type: none"><li>• <b>Dot1x</b> – The port-based authentication method.</li><li>• <b>MAB</b> – MAC Authentication Bypass method that uses the MAC address of the client to determine the kind of network access to provide.</li><li>• <b>Captive Portal</b> – The authentication method that prevents clients from accessing the network until user verification has been established.</li></ul>

Use the buttons at the bottom of the page to perform the following actions:

- Click **Refresh** to display the latest information from the switch.
- Click **Clear** to clear the Authentication Manager history log on the selected interface.

---

## Chapter 8. Configuring Quality of Service

This section gives an overview of Quality of Service (QoS) and explains the QoS features available from the Quality of Service navigation menu.

In a typical switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets have no place to be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given *special treatment* in a QoS capable network. With this in mind, all elements of the network must be QoS-capable. The presence of at least one node which is not QoS-capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

**Note:** Some of the features described in this section may not be supported in CE0128XB/CE0152XB software releases for particular hardware platforms.

---

## Configuring Access Control Lists

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network. CE0128XB/CE0152XB software supports IPv4, IPv6, and MAC ACLs. The total number of MAC and IP ACLs supported by CE0128XB/CE0152XB software is platform-specific.

You first create an IPv4-based, IPv6-based, or MAC-based rule and assign a unique ACL ID. Then, you define the rules, which can identify protocols, source and destination IP and MAC addresses, and other packet-matching criteria. Finally, you use the ID number to assign the ACL to a port or to a VLAN interface.

### IP Access Control Lists

IP access control lists (ACL) allow network managers to define classification actions and rules for specific ports. ACLs are composed of access control entries (ACE), or rules, that consist of the filters that determine traffic classifications. The total number of rules that can be defined for each ACL is platform-specific. These rules are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken, including dropping the packet or disabling the port, and the additional rules are not checked for a match. For example, a network administrator defines an ACL rule that says port number 20 can receive TCP packets. However, if a UDP packet is received the packet is dropped.

The IP Access Control List folder contains links to web pages that allow you to configure and view IP ACLs.

To configure an IP ACL:

1. Use the page [“IP ACL Configuration” on page 464](#) to define the IP ACL type and assign an ID to it.
2. Use the page [“Access Control List Interface Summary” on page 475](#) to create rules for the ACL.
3. Use the page [“Access Control List Configuration” on page 466](#) to view the configuration.

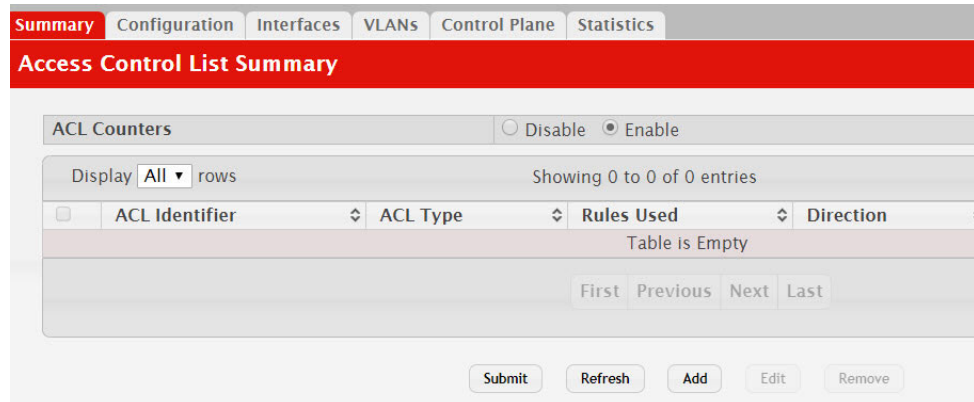
### *IP ACL Configuration*

Use the IP ACL Configuration page to add or remove IP-based ACLs and to enable or disable the ACL counters. On this menu the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the IP ACL are specified/created using the page [“Access Control List Interface Summary” on page 475](#).

To display the Access List Summary page, click **QoS > Access Control Lists > Summary** in the navigation menu.



**Figure 308.** Access Control List Summary



Use the buttons at the bottom of the page to perform the following tasks:

- To add an ACL, click **Add** and configure the ACL type and ID.
- To remove one or more configured ACLs, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.
- To configure rules for an ACL, select the ACL to configure and click **Edit**. You are redirected to the Access Control List Configuration page for the selected ACL.

**Table 302.** Access List Summary Fields

Field	Description
ACL Counters	The administrative status of the ACL counters. This field controls the status of the counters for all ACL types.
ACL Identifier	The name or number that identifies the ACL. The permitted identifier depends on the ACL type. Standard and Extended IPv4 ACLs use numbers within a set range, and Named IPv4 and MAC ACLs use alphanumeric characters.
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows: <ul style="list-style-type: none"> <li>• <b>IPv4 Standard</b> – Match criteria is based on the source address of IPv4 packets.</li> <li>• <b>IPv4 Extended</b> – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets.</li> <li>• <b>IPv4 Named</b> – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number.</li> <li>• <b>IPv6 Named</b> – Match criteria can be based on information including the source and destination IPv6 addresses, source and destination Layer 4 ports, and protocol type within IPv6 packets.</li> <li>• <b>Extended MAC</b> – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.</li> </ul>

**Table 302.** Access List Summary Fields (continued)

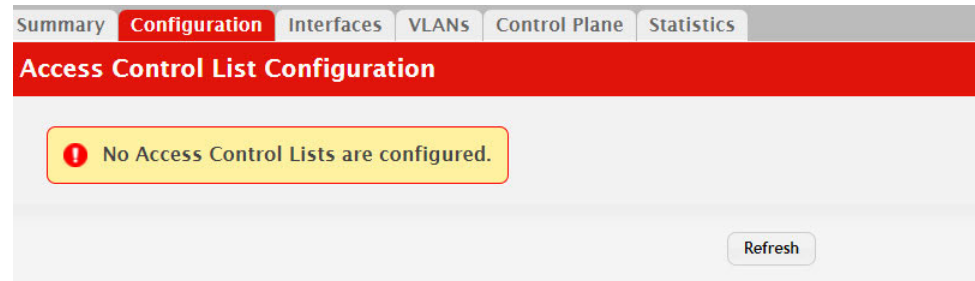
Field	Description
Rules Used	The number of rules currently configured for the ACL.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on an interface (Inbound) or after it has been received, routed, and is ready to exit an interface (Outbound).
Interface	The interface(s) to which the ACL has been applied.
VLAN	Each VLAN to which the ACL has been applied.

## Access Control List Configuration

Use this page to configure rules for the existing Access Control Lists (ACLs) on the system and to view summary information about the rules that have been added to an ACL. Each ACL rule is configured to match one or more aspects of traffic on the network. When a packet matches the conditions in a rule, it is handled according to the configured action (permit or deny) and attributes. Each ACL can have multiple rules, but the final rule for every ACL is an implicit deny all rule. For each rule, a packet must match all the specified criteria in order for the specified rule action (Permit/Deny) to take place.

To display the Access Control List Configuration page, click **QoS > Access Control Lists > Configuration** in the navigation menu.

**Figure 309.** Access Control List Configuration



Use the buttons to perform the following tasks:

- To add an Access List Rule entry, select the ID of the ACL that will include the rule from the ACL Identifier menu. Then, click **Add Rule** and configure the rule criteria and attributes. New rules cannot be created if the maximum number of rules has been reached.
- To remove the most recently configured rule for an ACL, select the ID of the appropriate ACL from the ACL Identifier menu and click **Remove Last Rule**. You must confirm the action before the entry is deleted.
- To resequence rules for an ACL, select the ID of the appropriate ACL from the ACL Identifier menu and click **Resequence Rules**.

**Figure 310.** Edit Access Control List

**Table 303.** IP ACL Summary Fields

Field	Description
ACL Identifier	<p>The menu contains the ID for each ACL that exists on the system. Before you add or remove a rule, you must select the ID of the ACL from the menu. For ACLs with alphanumeric names, click the <b>Edit</b> icon to change the ACL ID.</p> <p>The ID of a Named IPv4 ACL must begin with a letter, and not a number. The ACL identifier for IPv4 Standard and IPv4 Extended ACLs cannot be changed.</p>
Sequence Number	<p>The number that indicates the position of a rule within the ACL. If the sequence number is not specified during rule creation, the rule is automatically assigned a sequence number after it is successfully added to the ACL. The rules are displayed based on their position within the ACL, but can also be renumbered. Packets are checked against the rule criteria in order, from the lowest-numbered rule to the highest. When the packet matches the criteria in a rule, it is handled according to the rule action and attributes. If no rule matches a packet, the packet is discarded based on the implicit deny all rule, which is the final rule in every ACL.</p>
ACL Type	<p>The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows:</p> <ul style="list-style-type: none"> <li>• <b>IPv4 Standard</b> – Match criteria is based on the source address of IPv4 packets.</li> <li>• <b>IPv4 Extended</b> – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets.</li> <li>• <b>IPv4 Named</b> – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number.</li> <li>• <b>IPv6 Named</b> – Match criteria can be based on information including the source and destination IPv6 addresses, source and destination Layer 4 ports, and protocol type within IPv6 packets.</li> <li>• <b>Extended MAC</b> – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.</li> </ul>

**Table 303.** IP ACL Summary Fields (continued)

Field	Description
Status	Indicates whether the ACL is active. If the ACL is a time-based ACL that includes a time range, the ACL is active only during the periods specified within the time range. If an ACL does not include a time range, the status is always active.
Action	The action to take when a packet or frame matches the criteria in the rule: <ul style="list-style-type: none"><li>• <b>Permit</b> – The packet or frame is forwarded.</li><li>• <b>Deny</b> – The packet or frame is dropped.</li></ul> <b>Note:</b> When configuring ACL rules in the Add Access Control List Rule window, the selected action determines which fields can be configured. Not all fields are available for both Permit and Deny actions.
Match Conditions	The criteria used to determine whether a packet or frame matches the ACL rule.
Rule Attributes	Each action (beyond the basic Permit and Deny actions) to perform on the traffic that matches the rule.
Remarks	One or more remarks configured for the selected ACL and associated with the rule during rule creation. To delete a remark associated with the rule, click the – (minus) button preceding remark. You must confirm the action before the rule associated remark is removed.

Use the buttons available in the ACL Remarks table to perform the following tasks:

- To add a remark, click the + (plus) button and enter the remark to add.
- To delete a remark from the list, click the – (minus) button associated with the entry to remove. You must confirm the action before the entry is removed.

**Figure 311.** ACL Remarks

Field	Description
<b>ACL Remarks</b>	Lists the configured remarks for the selected ACL. All remarks present in this table are applied to the next rule created with the <b>Add Rule</b> button.

After you click **Add Rule**, the Add Access Control List Rule window opens and allows you to add a rule to the ACL that was selected from the ACL Identifier field. The fields available in the window depend on the ACL Type. The following information describes the fields in this window. The Match Criteria tables that apply to IPv4 ACLs, IPv6 ACLs, and MAC ACLs are described separately.

**Figure 312.** Add ACL Rule

**Table 304.** Add ACL Rule

Field	Description
Match Criteria (IPv4 ACLs)	The fields in this section specify the criteria to use to determine whether an IP packet matches the rule. The fields described below apply to IPv4 Standard, IPv4 Extended, and IPv4 Named ACLs unless otherwise noted.
Every	When this option is selected, all packets will match the rule and will be either permitted or denied. This option is exclusive to all other match criteria, so if Every is selected, no other match criteria can be configured. To configure specific match criteria, this option must be clear.
Protocol	(IPv4 Extended and IPv4 Named ACLs) The IANA-assigned protocol number to match within the IP packet. You can also specify one of the following keywords: EIGRP, GRE, ICMP, IGMP, IP, IPINIP, OSPF, PIM, TCP, or UDP.

Field	Description
Fragments	(IPv4 Extended and IPv4 Named ACLs) IP ACL rule to match on fragmented IP packets.
Source IP Address / Wildcard Mask	The source port IP address in the packet and source IP wildcard mask (in the second field) to compare to the IP address in a packet header. Wild card masks determines which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored. This field is required when you configure a source IP address.
Source L4 Port	(IPv4 Extended and IPv4 Named ACLs) The TCP/UDP source port to match in the packet header. The Source L4 Port and Destination L4 port are configurable only if protocol is either TCP or UDP. Equal to, Not Equal to, Greater than, and Less than options are available. For TCP protocol: Domain, Echo, FTP, FTP-Data, HTTP, SMTP, Telnet, WWW, POP2, or POP3 For UDP protocol: Domain, Echo, NTP, RIP, SNMP, TFTP, Time, or WHO
Destination IP Address / Wildcard Mask	The destination port IP address in the packet and destination IP wildcard mask (in the second field) to compare to the IP address in a packet header. Wild card masks determines which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A 1 in a bit position of the ACL mask indicates the corresponding bit can be ignored. This field is required when you configure a destination IP address.
Destination L4 Port	(IPv4 Extended and IPv4 Named ACLs) The TCP/UDP destination port to match in the packet header. The Source L4 Port and Destination L4 port are configurable only if protocol is either TCP or UDP. Equal to, Not Equal to, Greater than, and Less than options are available. For TCP protocol: Domain, Echo, FTP, FTP-Data, HTTP, SMTP, Telnet, WWW, POP2, or POP3 For UDP protocol: Domain, Echo, NTP, RIP, SNMP, TFTP, Time, or WHO
TTL Field Value	(IPv4 Extended and IPv4 Named ACLs) IP ACL rule to match on the specified Time-to-Live (TTL) field value.
IGMP Type	(IPv4 Extended and IPv4 Named ACLs) IP ACL rule to match on the specified IGMP message type. This option is available only if the protocol is IGMP.
ICMP Type	(IPv4 Extended and IPv4 Named ACLs) IP ACL rule to match on the specified ICMP message type. This option is available only if the protocol is ICMP.
ICMP Code	(IPv4 Extended and IPv4 Named ACLs) IP ACL rule to match on the specified ICMP message code. This option is available only if the protocol is ICMP.

Field	Description
ICMP Message	(IPv4 Extended and IPv4 Named ACLs) IP ACL rule to match on the ICMP message type and code. Specify one of the following supported ICMP messages: Echo, Echo-Reply, Host-Redirect, Mobile-Redirect, Net-Redirect, Net-Unreachable, Redirect, Packet-Too-Big, Port-Unreachable, Source-Quench, Router-Solicitation, Router-Advertisement, Time-Exceeded, TTL-Exceeded, and Unreachable. This option is available only if the protocol is ICMP.
TCP Flags	(IPv4 Extended and IPv4 Named ACLs) IP ACL rule to match on the TCP flags. When a + flag is specified, a match occurs if the flag is set in the TCP header. When a - flag is specified, a match occurs if the flag is not set in the TCP header. When Established is specified, a match occurs if either RST or ACK bits are set in the TCP header. This option is available only if the protocol is TCP.
Service Type	(IPv4 Extended and IPv4 Named ACLs) The service type to match in the IP header. The options in this menu are alternative ways of specifying a match condition for the same Service Type field in the IP header, but each service type uses a different user notation. After you select the service type, specify the value for the service type in the appropriate field. Only the field associated with the selected service type can be configured. The services types are as follows: <ul style="list-style-type: none"> <li>• <b>IP DSCP</b> – Matches the packet IP DiffServ Code Point (DSCP) value to the rule. The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header.</li> <li>• <b>IP Precedence</b> – Matches the IP Precedence value to the rule. The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header.</li> <li>• <b>IP TOS Bits</b> – Matches on the Type of Service (TOS) bits in the IP header. The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of 0xA0 and a TOS Mask of 0xFF. <ul style="list-style-type: none"> <li>– TOS Bits – Requires the bits in a packet's TOS field to match the two-digit hexadecimal number entered in this field.</li> <li>– TOS Mask – The bit positions that are used for comparison against the IP TOS field in a packet.</li> </ul> </li> </ul>
Time Range Name	The name of the time range that will impose a time limitation on the ACL rule. If a time range with the specified name does not exist, and the ACL containing this ACL rule is associated with an interface, the ACL rule is applied immediately. If a time range with specified name exists, and the ACL containing this ACL rule is associated with an interface, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
Committed Rate / Burst Size	The allowed transmission rate for packets on the interface (Committed Rate), and the number of bytes allowed in a temporary traffic burst (Burst Rate).
Match Criteria (IPv6 ACLs)	The fields in this section specify the criteria to use to determine whether an IP packet matches the rule. The fields described below apply to IPv6 ACLs.

Field	Description
Every	When this option is selected, all packets will match the rule and will be either permitted or denied. This option is exclusive to all other match criteria, so if Every is selected, no other match criteria can be configured. To configure specific match criteria, this option must be clear.
Protocol	The IANA-assigned protocol number to match within the IP packet. You can also specify one of the following keywords: ICMP, IGMP, TCP, UDP, ICMPv6, or IP.
Fragments	IPv6 ACL rule to match on fragmented IP packets.
Source Prefix/Prefix Length	The IPv6 prefix combined with IPv6 prefix length of the network or host from which the packet is being sent.
Source L4 Port	The TCP/UDP source port to match in the packet header. Select one of the following options: Equal, Not Equal, Less Than, Greater Than, or Range and specify the port number or keyword. TCP port keywords include Domain, Echo, FTP, FTP Data, HTTP, SMTP, Telnet, WWW, POP2, and POP3. UDP port keywords include Domain, Echo, NTP, RIP, SNMP, TFTP, TIME, and WHO.
Destination Prefix/Prefix Length	The IPv6 prefix combined with the IPv6 prefix length to be compared to a packet's destination IPv6 address as a match criteria for the IPv6 ACL rule. To indicate a destination host, specify an IPv6 prefix length of 128.
Destination L4 Port	The TCP/UDP destination port to match in the packet header. Select one of the following options: Equal, Not Equal, Less Than, Greater Than, or Range and specify the port number or keyword.  TCP port keywords include Domain, Echo, FTP, FTP Data, HTTP, SMTP, Telnet, WWW, POP2, and POP3.  UDP port keywords include Domain, Echo, NTP, RIP, SNMP, TFTP, TIME, and WHO.
ICMP Type	IPv6 ACL rule to match on the specified ICMP message type. This option is available only if the protocol is ICMPv6.
ICMP Code	IPv6 ACL rule to match on the specified ICMP message code. This option is available only if the protocol is ICMPv6.
ICMP Message	IPv6 ACL rule to match on the ICMP message type and code. Specify one of the following supported ICMPv6 messages: Destination-Unreachable, Echo-Request, Echo-Reply, Header, Hop-Limit, MLD-Query, MLD-Reduction, MLD-Report, ND-NA, ND-NS, Next-Header, No-Admin, No-Route, Packet-Too-Big, Port-Unreachable, Router-Solicitation, Router-Advertisement, Router-Renumbering, Time-Exceeded, and Unreachable. This option is available only if the protocol is ICMPv6.
TCP Flags	IPv6 ACL rule to match on the TCP flags. When a + flag is specified, a match occurs if the flag is set in the TCP header. When a - flag is specified, a match occurs if the flag is not set in the TCP header. When Established is specified, a match occurs if either RST or ACK bits are set in the TCP header. This option is available only if the protocol is TCP.
Flow Label	A 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers.
IP DSCP	The IP DSCP value in the IPv6 packet to match to the rule. The DSCP value is defined as the high-order six bits of the Service Type octet in the IPv6 header.
Routing	IPv6 ACL rule to match on routed packets.



Field	Description
Match Criteria (MAC ACLs)	The fields in this section specify the criteria to use to determine whether an Ethernet frame matches the rule. The fields described below apply to MAC ACLs.
Every	When this option is selected, all packets will match the rule and will be either permitted or denied. This option is exclusive to all other match criteria, so if Every is selected, no other match criteria can be configured. To configure specific match criteria, this option must be clear.
CoS	The 802.1p user priority value to match within the Ethernet frame.
Secondary CoS	The secondary 802.1p user priority value to match within the Ethernet frame.
Ethertype	The EtherType value to match in an Ethernet frame. Specify the number associated with the EtherType or specify one of the following keywords: AppleTalk, ARP, IBM SNA, IPv4, IPv6, IPX, MPLS, Unicast, NETBIOS, NOVELL, PPPoE, or RARP.
Source MAC Address / Mask	The MAC address to match to an Ethernet frame's source port MAC address. If desired, enter the MAC Mask associated with the source MAC to match. The MAC address mask specifies which bits in the source MAC to compare against an Ethernet frame. Use F's and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa_bb_cc_dd_ee_ff, and the mask is 00_00_ff_ff_ff_ff, all MAC addresses with aa_b-b_xx_xx_xx result in a match (where x is any hexadecimal number).
Destination MAC Address / Mask	The MAC address to match to an Ethernet frame's destination port MAC address. If desired, enter the MAC Mask associated with the destination MAC to match. The MAC address mask specifies which bits in the destination MAC to compare against an Ethernet frame. Use F's and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa_bb_c-c_dd_ee_ff, and the mask is 00_00_ff_ff_ff_ff, all MAC addresses with aa_bb_xx_xx_xx result in a match (where x is any hexadecimal number).
VLAN	The VLAN ID to match within the Ethernet frame.
Secondary VLAN	The secondary VLAN ID to match within the Ethernet frame.
Rule Attributes	The fields in this section provide information about the actions to take on a frame or packet that matches the rule criteria. The attributes specify actions other than the basic Permit or Deny actions.
Assign Queue	The number that identifies the hardware egress queue that will handle all packets matching this rule.
Interface	The interface to use for the action: <ul style="list-style-type: none"> <li>• <b>Redirect</b> – Allows traffic that matches a rule to be redirected to the selected interface instead of being processed on the original port. The redirect function and mirror function are mutually exclusive.</li> <li>• <b>Mirror</b> – Provides the ability to mirror traffic that matches a rule to the selected interface. Mirroring is similar to the redirect function, except that in flow-based mirroring a copy of the permitted traffic is delivered to the mirror interface while the packet itself is forwarded normally through the device.</li> </ul>

Field	Description
Log	When this option is selected, logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule went into effect during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval.
Redirect External Agent	The number that identifies the external agent that will receive all packets matching this rule.
Time Range Name	The name of the time range that will impose a time limitation on the ACL rule. If a time range with the specified name does not exist, and the ACL containing this ACL rule is associated with an interface, the ACL rule is applied immediately. If a time range with specified name exists, and the ACL containing this ACL rule is associated with an interface, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
Committed Rate / Burst Size	The allowed transmission rate for frames on the interface (Committed Rate), and the number of bytes allowed in a temporary traffic burst (Burst Rate).

After you click the **Resequence Rules** button, the **Resequence ACL Rules** window opens and allows you to resequence rules of the ACL selected from the **ACL Identifier** field. The following information describes the fields in this window.

**Table 305.** *Resequence ACL Rules*

Field	Description
Sequence Start	The starting sequence number for resequencing the existing rules.
Sequence Step	The increment of sequence numbers for resequencing the existing rules.

Click **Refresh** to update the information on the screen.

After you click the + (plus) button next to **ACL Remarks**, the Add ACL Remark window opens and allows you to add a remark.

**Figure 313.** Add ACL Remark

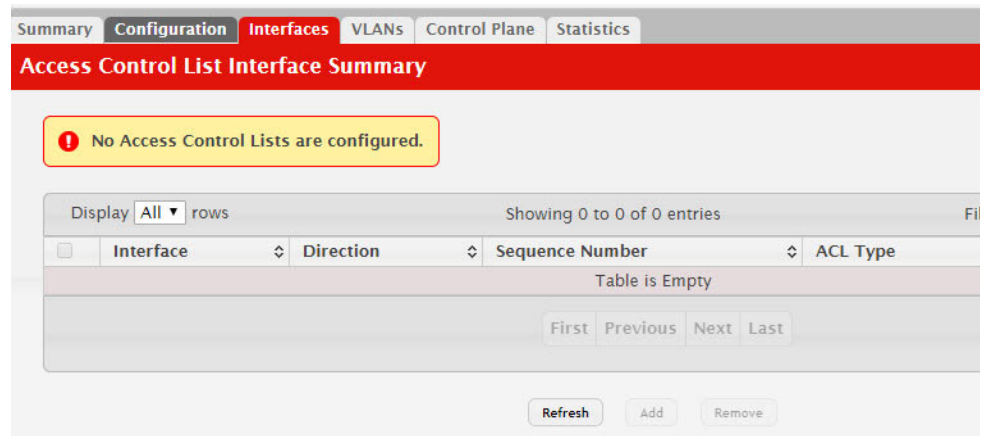
The screenshot shows a window titled "Add ACL Remark". Inside the window, there is a text input field with the label "New ACL Remark" and a character count "(1-31)" to its right. The window has a light gray background and a title bar.

## Access Control List Interface Summary

Use this page to associate one or more ACLs with one or more interfaces on the device. When an ACL is associated with an interface, traffic on the port is checked against the rules defined within the ACL until a match is found. If the traffic does not match any rules within an ACL, it is dropped because of the implicit deny all rule at the end of each ACL.

To display the Access Control List Interface Summary page, click **QoS > Access Control Lists > Interfaces** in the navigation menu.

**Figure 314.** Access Control List Interface Summary



Use the buttons to perform the following tasks:

- To apply an ACL to an interface, click **Add** and configure the settings in the available fields.
- To remove the association between an interface and an ACL, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 306.** Access Control List Interface Summary Fields

Field	Description
Interface	The interface that has an associated ACL.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on an interface (Inbound) or after it has been received, routed, and is ready to exit an interface (Outbound).
Sequence Number	The order the ACL is applied to traffic on the interface relative to other ACLs associated with the interface in the same direction. When multiple ACLs are applied to the same interface in the same direction, the ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.

**Table 306.** Access Control List Interface Summary Fields (continued)

Field	Description
ACL Type	<p>The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows:</p> <ul style="list-style-type: none"> <li>• IPv4 Standard – Match criteria is based on the source address of IPv4 packets.</li> <li>• IPv4 Extended – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets.</li> <li>• IPv4 Named – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number.</li> <li>• IPv6 Named – Match criteria can be based on information including the source and destination IPv6 addresses, source and destination Layer 4 ports, and protocol type within IPv6 packets.</li> <li>• Extended MAC – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.</li> </ul>
ACL Identifier	<p>The name or number that identifies the ACL. When applying an ACL to an interface, the ACL Identifier menu includes only the ACLs within the selected ACL Type.</p>

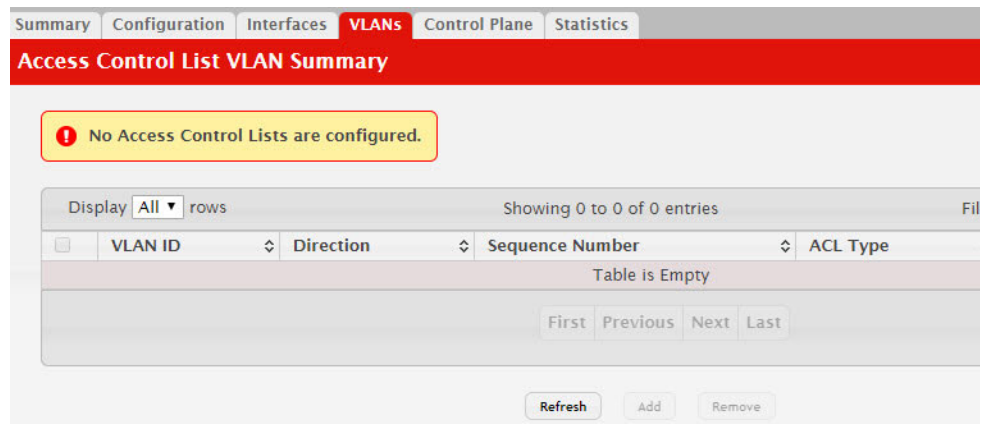
## Access Control List VLAN Summary

Use this page to associate one or more ACLs with one or more VLANs on the device.

**Note:** You can also associate an ACL with a VLAN routing interface.

To display the Access Control List VLAN Summary page, click **QoS > Access Control Lists > VLANs** in the navigation menu.

**Figure 315.** Access Control List VLAN Summary



Use the buttons to perform the following tasks:

- To associate an ACL with a VLAN, click **Add** and configure the settings in the available fields.
- To remove the association between a VLAN and an ACL, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 307.** *Access Control List VLAN Summary Fields*

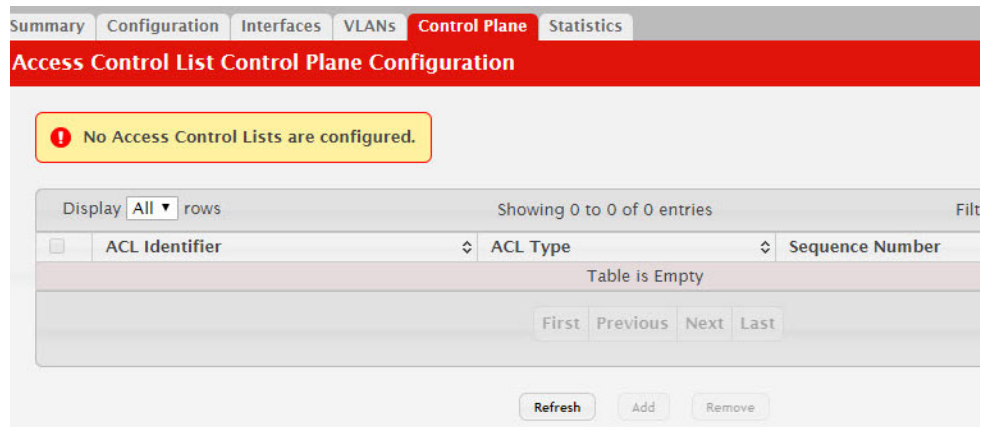
Field	Description
VLAN ID	The ID of the VLAN associated with the rest of the data in the row. When associating a VLAN with an ACL, use this field to select the desired VLAN.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on a VLAN (Inbound) or after it has been received, routed, and is ready to exit a VLAN (Outbound).
Sequence Number	The order the ACL is applied to traffic on the VLAN relative to other ACLs associated with the VLAN in the same direction. When multiple ACLs are applied to the same VLAN in the same direction, the ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows: <ul style="list-style-type: none"> <li>• IPv4 Standard – Match criteria is based on the source address of IPv4 packets.</li> <li>• IPv4 Extended – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets.</li> <li>• IPv4 Named – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number.</li> <li>• IPv6 Named – Match criteria can be based on information including the source and destination IPv6 addresses, source and destination Layer 4 ports, and protocol type within IPv6 packets.</li> <li>• Extended MAC – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.</li> </ul>
ACL Identifier	The name or number that identifies the ACL. The permitted identifier depends on the ACL type. Standard and Extended IPv4 ACLs use numbers within a set range, and Named IPv4, IPv6, and MAC ACLs use alphanumeric characters.

## Access Control List Control Plane Configuration

Use this page to define controlled management access to the device. Control plane ACLs allow you to determine which addresses or protocols are allowed to access the management interface on the device. The control plane ACLs are applied to management access through the in-band (production network) ports only. Inbound traffic on the CPU port is checked against the rules defined within the ACL until a match is found. If the traffic does not match any rules within an ACL, it is dropped because of the implicit deny all rule at the end of each ACL.

To display the Access Control List Control Plane Configuration Page, click **QoS > Access Control Lists > Control Plane** in the navigation menu.

**Figure 316.** Access Control List Control Plane Configuration



Use the buttons to perform the following tasks:

- To apply an ACL to the CPU interface, click **Add** and configure the settings in the available fields.
- To remove the association between the CPU interface and an ACL, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 308.** Access Control List Control Plane Configuration Fields

Field	Description
ACL Identifier	The name or number that identifies the ACL.
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows: <ul style="list-style-type: none"> <li>• <b>IPv4 Standard</b> – Match criteria is based on the source address of IPv4 packets.</li> <li>• <b>IPv4 Extended</b> – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets.</li> <li>• <b>IPv4 Named</b> – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number.</li> <li>• <b>IPv6 Named</b> – Match criteria can be based on information including the source and destination IPv6 addresses, source and destination Layer 4 ports, and protocol type within IPv6 packets.</li> <li>• <b>Extended MAC</b> – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.</li> </ul>
Sequence Number	The order the ACL is applied to traffic on the interface relative to other ACLs associated with the interface in the same direction. When multiple ACLs are applied to the same interface in the same direction, the ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.

## IPv6 ACL Rules

The maximum number of IPv6 rules depends on the following factors:

- If both SRC IPv6 and DST IPv6 are part of the ACL rule, then the maximum number of rules is one quarter the possible number for that device type.
- If DSCP is part of the rule along with any other qualifier, then the maximum number of rules possible are one quarter the possible number for that device type.
- In all other cases, the maximum number of rules are equal to half the maximum possible for that device type or 1021, whichever is smaller.

## Scenarios

In the following scenarios, the BCM56334 device is used (1789 rules maximum).

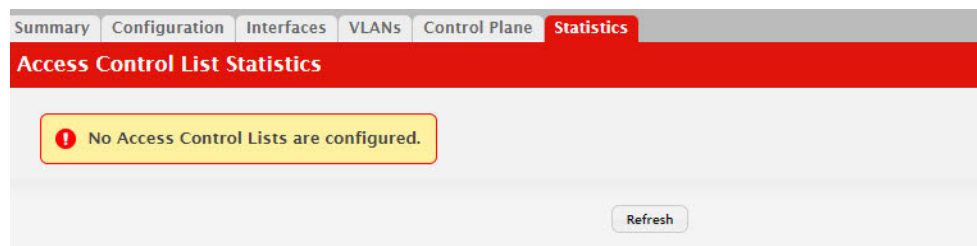
- Scenario #1: If the rules have both SRC IPv6 and DST IPv6, then maximum rules possible are  $1789/4 = 447$ .
- Scenario #2: If the rules have DSCP along with any other qualifier, then the maximum number of rules possible are  $1789/4 = 447$ .
- Scenario #3: In all the other cases, 894 rules can be accommodated.

## Access Control List Statistics

Use this page to display the statistical information about the packets forwarded or discarded by the port that matches the configured rules within an Access Control List (ACL). Each ACL rule is configured to match one or more aspects of traffic on the network. When a packet matches the conditions in a rule, the counter associated with the rule gets incremented, until it reaches the rollover value of the counter. ACL counters do not interact with DiffServ policies or Policy-based Routing counters.

To display the Access Control List Statistics page, click **QoS > Access Control Lists > Statistics** in the navigation menu.

**Figure 317.** Access Control List Statistics



Use the buttons to perform the following tasks:

- To clear the hit count for one or more configured rules within an ACL, select the rule entry and click **Clear Rule Counter**. You must confirm the action before the hit count is cleared for the selected rule(s).
- To clear the hit count for an ACL, select the ACL ID from the ACL Identifier menu and click **Clear ACL Counters**. You must confirm the action before the hit count is cleared for the selected ACL.

- To clear the hit count for an ACL type, select the type from the ACL Type menu and select **All** from the ACL Identifier menu and then click **Clear ACL Counters**. You must confirm the action before the hit count is cleared for the selected ACL type.

**Table 309.** *Access Control List Statistics Fields*

Field	Description
ACL Type	<p>The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic.</p> <p>The ACL types are as follows:</p> <ul style="list-style-type: none"> <li>• <b>IPv4 Standard</b> – Match criteria is based on the source address of the IPv4 packets.</li> <li>• <b>IPv4 Extended</b> – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of the IPv4 packets.</li> <li>• <b>IPv4 Named</b> – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number.</li> <li>• <b>IPv6 Named</b> – Match criteria can be based on information including the source and destination IPv6 addresses, source and destination Layer 4 ports, and protocol type within the IPv6 packets.</li> <li>• <b>Extended MAC</b> – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within the Ethernet frames.</li> </ul>
ACL Identifier	<p>A list of ACL IDs that exist on the system for a given ACL type. To view the rule(s) within an ACL, you must select the ID of the ACL from the list. The ACL rules are not displayed when option <b>All</b> is selected. Option <b>All</b> lets you clear the hit count for an ACL type.</p>
Sequence Number	<p>The number that indicates the position of a rule within the ACL.</p>
Action	<p>The action to take when a packet or frame matches the criteria in the rule:</p> <ul style="list-style-type: none"> <li>• <b>Permit</b> – The packet or frame is forwarded.</li> <li>• <b>Deny</b> – The packet or frame is dropped.</li> </ul>
Match Conditions	<p>The criteria used to determine whether a packet or frame matches the ACL rule.</p>
Rule Attributes	<p>Each action — beyond the basic Permit and Deny actions — to perform on the traffic that matches the rule.</p>
Hit Count	<p>Indicates the number of packets that match the configured rule in an ACL. If a rule is configured without rate limit, then the hit count is the number of matched packets forwarded or discarded by the port. If a rule is configured with rate limit, then if the sent traffic rate exceeds the configured rate, the hit count displays the matched packet count equal to the sent rate, despite packets getting dropped beyond the configured limit. If the sent traffic rate is less than the configured rate, the hit count displays only the matched packet count.</p>



## Configuring Class of Service

The Class of Service (CoS) queuing feature lets you directly configure certain aspects of switch queuing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, transmission rate shaping, etc., are user-configurable at the queue (or port) level.

Seven queues per port are supported. Although the hardware supports eight queues, one queue is always reserved for internal use by the stacking subsystem.

### IP DSCP Mapping Configuration

Use the IP DSCP Mapping Configuration page to map an IP DSCP value to an internal traffic class.

To display the IP DSCP Mapping Configuration page, click **QoS > Class of Service > IP DSCP** in the navigation menu.

**Figure 318.** CoS IP DSCP Mapping Configuration

IP DSCP	Traffic Class
0	<input type="radio"/> 0 <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5 <input type="radio"/> 6
1	<input type="radio"/> 0 <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5 <input type="radio"/> 6
2	<input type="radio"/> 0 <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5 <input type="radio"/> 6
3	<input type="radio"/> 0 <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5 <input type="radio"/> 6
4	<input type="radio"/> 0 <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5 <input type="radio"/> 6
5	<input type="radio"/> 0 <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5 <input type="radio"/> 6

**Table 310.** IP DSCP Mapping Configuration Fields

Field	Description
Interface	The menu contains all CoS configurable interfaces. The only option is Global, which means that the IP DSCP mapping configuration applies to all interfaces and cannot be applied on a per-interface basis.
IP DSCP Values	Lists the IP DSCP values to which you can map an internal traffic class. The values range from 0-63.
Traffic Class	The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent. Valid range is 0 to 6.

If you make changes to the page, click **Submit** to apply the changes to the system. Click Restore Defaults to reset all interfaces to the default trust value.

## Interface Configuration

Use the Interface Configuration page to apply an interface shaping rate to all ports or to a specific port.

To display the Interface Configuration page, click **QoS > Class of Service > Interface** in the navigation menu.

**Figure 319.** Interface Configuration

**Table 311.** Interface Configuration Fields

Field	Description
Interface	Selects the CoS configurable interface to be affected by the Interface Shaping Rate. Select Global to apply a rate to all interfaces. Select an individual port to override the global setting.
Trust Mode	The trust mode for ingress traffic on the interface, which is one of the following: <ul style="list-style-type: none"> <li>untrusted — The interface ignores any priority designations encoded in incoming packets, and instead sends the packets to a traffic queue based on the ingress port's default priority.</li> <li>trust dot1p — The port accepts at face value the 802.1p priority designation encoded within packets arriving on the port.</li> <li>trust ip dscp — The port accepts at face value the IP DSCP priority designation encoded within packets arriving on the port.</li> </ul>
Interface Shaping Rate	Sets the limit on how much traffic can leave a port. The limit on maximum transmission bandwidth has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The specified value represents a percentage of the maximum negotiated bandwidth. The default value is zero (0). Valid values are 0 to 100, in increments of 1. A value of 0 means the maximum is unlimited.

If you make changes to the page, click **Submit** to apply the changes to the system. Click **Restore Defaults** to reset all interfaces to the default trust value.

## Interface Queue Configuration

Use the Interface Queue Configuration page to define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port. Each port has its own CoS queue-related configuration.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally or per-port. A global configuration change is automatically applied to all ports in the system.

To display the Interface Queue Configuration page, click **QoS > Class of Service > Queue** in the navigation menu.

**Figure 320.** Interface Queue Configuration

Queue ID	Minimum Bandwidth (%)	Scheduler Type	Queue M
0	0	Weighted	TailDrop
1	0	Weighted	TailDrop
2	0	Weighted	TailDrop
3	0	Weighted	TailDrop
4	0	Weighted	TailDrop
5	0	Weighted	TailDrop
6	0	Weighted	TailDrop

**Table 312.** Interface Queue Configuration Fields

Field	Description
Interface	Specifies the interface (physical, LAG, or Global) to configure.
Total Minimum Bandwidth Allocated	Shows the sum of individual Minimum Bandwidth values for all queues in the interface. The sum cannot exceed the defined maximum of 100. This value is considered while configuring the Minimum Bandwidth for a queue in the selected interface.
Queue ID	Use the menu to select the queue per interface to be configured.
Minimum Bandwidth	Specify the minimum guaranteed bandwidth allocated to the selected queue on the interface. Setting this value higher than its corresponding Maximum Bandwidth automatically increases the maximum to the same value. The default value is 0. The valid range is 0 to 100, in increments of 1. The value zero (0) means no guaranteed minimum. The sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum 100.
Scheduler Type	<p>Selects the type of queue processing from the drop-down menu. Options are <b>Weighted</b> and <b>Strict</b>. Defining on a per-queue basis allows the user to create the desired service characteristics for different types of traffic.</p> <ul style="list-style-type: none"> <li>• <b>Weighted:</b> Weighted round robin associates a weight to each queue. This is the default.</li> <li>• <b>Strict:</b> Strict priority services traffic with the highest priority on a queue first</li> </ul>

**Table 312.** *Interface Queue Configuration Fields (continued)*

Field	Description
Queue Management Type	Displays the type of queue depth management techniques used for all queues on this interface. This is only used if the device supports independent settings per-queue. Queue Management Type can only be Taildrop. The default value is Taildrop - All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.

- If you make changes to the page, click **Submit** to apply the changes to the system.
- Click **Restore Default** to restore all CoS queue settings on the selected interface to the default values. If Global is selected from the interface menu, all default settings for all interfaces are restored.
- To reset the defaults for all interfaces, select Global from the **Slot/Port** menu before you click the button.

# Configuring DiffServ

Use this page to configure the administrative mode of Differentiated Services (DiffServ) support on the device and to view the current and maximum number of entries in each of the main DiffServ private MIB tables. DiffServ allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

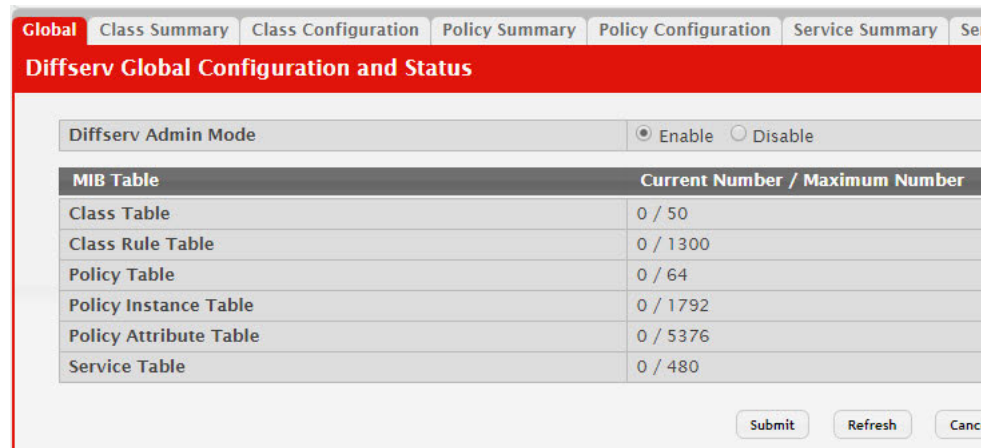
Packets are classified and processed based on defined criteria. The classification criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

## DiffServ Global Configuration and Status

Use this page to configure the Global DiffServ settings on the device.

To display the DiffServ Global Configuration and Status page, click **QoS > Diffserv > Global** in the navigation menu.

**Figure 321.** DiffServ Global Configuration and Status



**Table 313.** DiffServ Global Configuration and Status Fields

Field	Description
Diffserv Admin Mode	The administrative mode of DiffServ on the device. While disabled, the DiffServ configuration is retained and can be changed, but it is not active. While enabled, Differentiated Services are active.
MIB Table	The information in this table displays the number of entries (rows) that are currently in each of the main DiffServ private MIB tables and the maximum number of rows that can exist in each table.
Class Table	The current and maximum number of classifier entries in the table. DiffServ classifiers differentiate among traffic types.

**Table 313.** DiffServ Global Configuration and Status Fields (continued)

Field	Description
Class Rule Table	The current and maximum number of class rule entries in the table. Class rules specify the match criteria that belong to a class definition.
Policy Table	The current and maximum number of policy entries in the table. The policy determines the traffic conditioning or service provisioning actions applied to a traffic class.
Policy Instance Table	The current and maximum number of policy-class instance entries in the table. A policy-class instance is a policy that is associated with an existing DiffServ class.
Policy Attribute Table	The current and maximum number of policy attribute entries in the table. A policy attribute entry attaches various policy attributes to a policy-class instance.
Service Table	The current and maximum number of service entries in the table. A service entry associates a DiffServ policy with an interface and inbound or outbound direction.

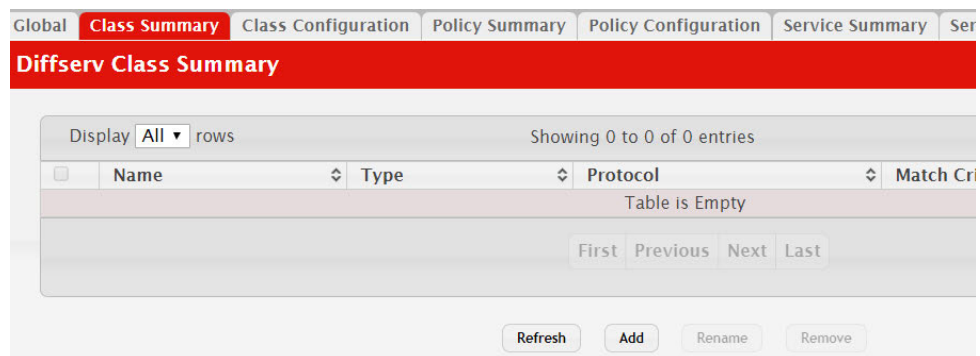
- If you make changes to the page, click **Submit** to apply the changes to the system. Click Restore Defaults to reset all interfaces to the default trust value.
- Click **Refresh** to update the page with the most current data from the switch.

## DiffServ Class Summary

Use this page to create or remove DiffServ classes and to view summary information about the classes that exist on the device. Creating a class is the first step in using DiffServ to provide Quality of Service. After a class is created, you can define the match criteria for the class.

To display the Diffserv Class Summary and Status page, click **QoS > Diffserv > Class Summary** in the navigation menu.

**Figure 322.** DiffServ Class Summary



Use the buttons to perform the following tasks:

- To add a DiffServ class, click **Add** and complete the fields in the **Add Class** window.
- To change the name of an existing class, select the entry to modify and click **Rename**.

- To remove one or more configured classes, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 314.** *DiffServ Class Summary Fields*

Field	Description
Name	The name of the DiffServ class. When adding a new class or renaming an existing class, the name of the class is specified in the Class field of the dialog window.
Type	The class type, which is one of the following: <ul style="list-style-type: none"> <li>• <b>All</b>—All the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria.</li> <li>• <b>Any</b>—Any of various match criteria defined for the class can be satisfied for a packet match.</li> </ul>
Protocol	The Layer 3 protocol to use for filtering class types, which is either IPv4 or IPv6.
Match Criteria	The criteria used to match packets.

Click **Refresh** to update the page with the most current data from the switch.

## DiffServ Class Configuration

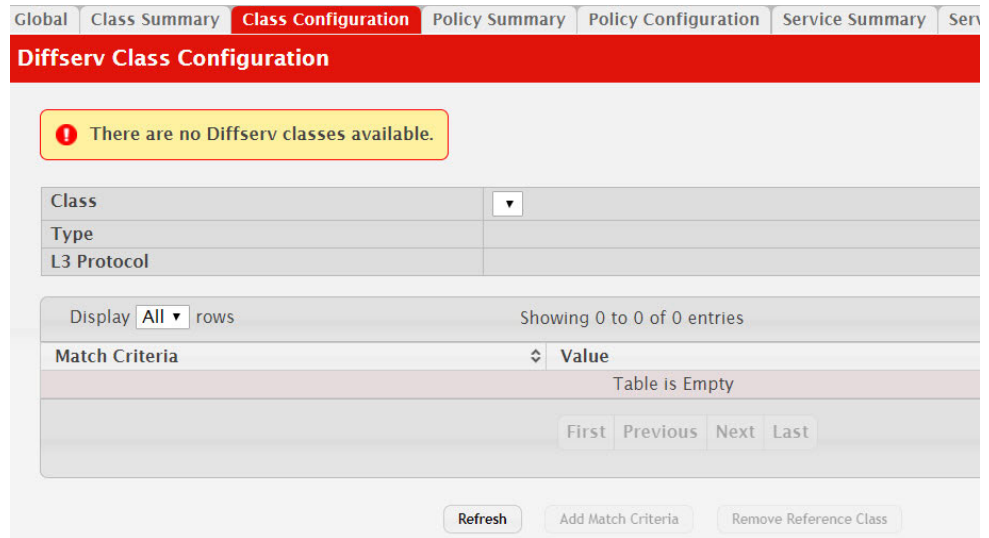
Use this page to define the criteria to associate with a DiffServ class. As packets are received or transmitted, these DiffServ classes are used to classify and prioritize packets. Each class can contain multiple match criteria.

After you select the class to configure from the Class menu, use the buttons to perform the following tasks:

- To define criteria for matching packets within a class, click **Add Match Criteria**. Once you add a match criteria entry to a class, you cannot edit or remove the entry. However, you can add more match criteria entries to a class until the maximum number of entries has been reached for the class.
- To remove the associated reference class from the selected class, click **Remove Reference Class**. Note that unless the reference class is the last entry in the list of match criteria, the Reference Class match type remains in the list as a placeholder, but the associated value is N/A, and the previously referenced class is removed.

To display the Diffserv Class Configuration and Status page, click **QoS > Diffserv > Class Configuration** in the navigation menu.

**Figure 323.** DiffServ Class Configuration



**Table 315.** DiffServ Class Configuration Fields

Field	Description
Class	The name of the class. To configure match criteria for a class, select its name from the menu.
Type	The class type, which is one of the following: <ul style="list-style-type: none"> <li><b>All</b> – All the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria.</li> <li><b>Any</b> – Any of various match criteria defined for the class can be satisfied for a packet match.</li> </ul>
L3 Protocol	The Layer 3 protocol to use for filtering class types, which is either IPv4 or IPv6.
Match Criteria	The type of match criteria defined for the selected class. If the Type is ACL, no information about the match criteria is available on this page.
Value	The configured value of the match criteria that corresponds to the match type.
Any	Select this option to specify that all packets are considered to match the specified class. There is no need to configure additional match criteria if Any is selected because a match will occur on all packets.



**Table 315.** DiffServ Class Configuration Fields (continued)

Field	Description
Reference ACL	<p>Select this option to require packets to match the criteria defined in the associated ACL. When associating an ACL, the ACL (IP or MAC) options are available only if at least one IP or MAC ACL exists on the device.</p> <p>After you select this option, the <b>ACL Identifier</b> field appears. Use this field to associate an ACL for the match criteria. The <b>ACL Identifier</b> field has the following guidelines:</p> <ul style="list-style-type: none"> <li>• The drop-down menu lists the name or number that identifies the ACL for all configured ACLs that are valid for the class type and protocol.</li> <li>• Standard and Extended IPv4 ACLs use numbers in the range 1 to 199. All other ACL types use names.</li> <li>• If you select an IP ACL, you cannot select the No Protocol option to configure the Class as a non-IP L2 match DiffServ class.</li> </ul>
Reference Class	<p>Select this option to reference another class for criteria. The match criteria defined in the referenced class is as match criteria in addition to the match criteria you define for the selected class. After selecting this option, the classes that can be referenced are displayed. Select the class to reference. A class can reference at most one other class of the same type.</p>
Class of Service	<p>Select this option to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value.</p>
Secondary Class of Service	<p>Select this option to require the secondary CoS value in an Ethernet frame header to match the specified secondary CoS value.</p>
Ethertype	<p>Select this option to require the EtherType value in the Ethernet frame header to match the specified EtherType value. After you select this option, specify the EtherType value in one of the following two fields:</p> <ul style="list-style-type: none"> <li>• <b>Ethertype Keyword</b> – The menu includes several common protocols that are mapped to their EtherType values.</li> <li>• <b>Ethertype Value</b> – This field accepts custom EtherType values.</li> </ul>
VLAN	<p>Select this option to require a packet's VLAN ID to match a VLAN ID or a VLAN ID within a continuous range. If you configure a range, a match occurs if a packet's VLAN ID is the same as any VLAN ID within the range. After you select this option, use the following fields to configure the VLAN match criteria:</p> <ul style="list-style-type: none"> <li>• <b>VLAN ID Start</b> – The VLAN ID to match or the VLAN ID with the lowest value within a range of VLANs.</li> <li>• <b>VLAN ID End</b> – The VLAN ID with the highest value within the range of VLANs. This field is not required if the match criteria is a single VLAN ID.</li> </ul>
Secondary VLAN	<p>Select this option to require a packet's VLAN ID to match a secondary VLAN ID or a secondary VLAN ID within a continuous range. If you configure a range, a match occurs if a packet's secondary VLAN ID is the same as any secondary VLAN ID within the range. After you select this option, use the following fields to configure the secondary VLAN match criteria:</p> <ul style="list-style-type: none"> <li>• <b>Secondary VLAN ID Start</b> – The secondary VLAN ID to match or the secondary VLAN ID with the lowest value within a range of VLANs.</li> <li>• <b>Secondary VLAN ID End</b> – The secondary VLAN ID with the highest value within the range of VLANs. This field is not required if the match criteria is a single VLAN ID.</li> </ul>

**Table 315.** DiffServ Class Configuration Fields (continued)

Field	Description
Source MAC Address	<p>Select this option to require a packet's source MAC address to match the specified MAC address. After you select this option, use the following fields to configure the source MAC address match criteria:</p> <ul style="list-style-type: none"> <li>• <b>MAC Address</b> – The source MAC address to match.</li> <li>• <b>MAC Mask</b> – The MAC mask, which specifies the bits in the source MAC address to compare against an Ethernet frame. Use F's and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.</li> </ul>
Destination MAC Address	<p>Select this option to require a packet's destination MAC address to match the specified MAC address. After you select this option, use the following fields to configure the destination MAC address match criteria:</p> <ul style="list-style-type: none"> <li>• <b>MAC Address</b> – The destination MAC address to match.</li> <li>• <b>MAC Mask</b> – The MAC mask, which specifies the bits in the destination MAC address to compare against an Ethernet frame. Use F's and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.</li> </ul>
Source IPv6 Address	<p>Select this option to require the source IPv6 address in a packet header to match the specified values. After you select this option, use the following fields to configure the source IPv6 address match criteria:</p> <ul style="list-style-type: none"> <li>• <b>Source Prefix</b> – The source IPv6 prefix to match.</li> <li>• <b>Source Prefix Length</b> – The IPv6 prefix length.</li> </ul>
Destination IPv6 Address	<p>Select this option to require the destination IPv6 address in a packet header to match the specified values. After you select this option, use the following fields to configure the destination IPv6 address match criteria:</p> <ul style="list-style-type: none"> <li>• <b>Destination Prefix</b> – The destination IPv6 prefix to match.</li> <li>• <b>Destination Prefix Length</b> – The IPv6 prefix length.</li> </ul>
Source L4 Port	<p>Select this option to require a packet's TCP/UDP source port to match the specified port or the port number within a range of port numbers. If you configure a range, a match occurs if a packet's source port number is the same as any source port number within the range. After you select this option, use the following fields to configure a source port keyword, source port number, or source port range for the match criteria:</p> <ul style="list-style-type: none"> <li>• <b>Protocol</b> – Select the desired L4 keyword from the list on which the match is based. If you select a keyword, the other source port configuration fields are not available.</li> <li>• <b>Port End</b> – A user-defined L4 source port number to match or the source port number with the lowest value within a range of ports.</li> <li>• <b>Port Start</b> – The source port with the highest value within the range of ports. This field is not required if the match criteria is a single port.</li> </ul>

**Table 315.** DiffServ Class Configuration Fields (continued)

Field	Description
Destination L4 Port	<p>Select this option to require a packet's TCP/UDP destination port to match the specified port or the port number within a range of port numbers. If you configure a range, a match occurs if a packet's destination port number is the same as any destination port number within the range. After you select this option, use the following fields to configure a destination port keyword, destination port number, or destination port range for the match criteria:</p> <ul style="list-style-type: none"> <li>• <b>Protocol</b> – Select the desired L4 keyword from the list on which the match is based. If you select a keyword, the other destination port configuration fields are not available.</li> <li>• <b>Port End</b> – A user-defined L4 destination port number to match or the destination port number with the lowest value within a range of ports.</li> <li>• <b>Port Start</b> – The destination port with the highest value within the range of ports. This field is not required if the match criteria is a single port.</li> </ul>
IP DSCP	<p>Select this option to require the packet's IP DiffServ Code Point (DSCP) value to match the specified value. The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header. After you select this option, use one of the following fields to configure the IP DSCP match criteria:</p> <ul style="list-style-type: none"> <li>• <b>IP DSCP Keyword</b> – The IP DSCP keyword code that corresponds to the IP DSCP value to match. If you select a keyword, you cannot configure an IP DSCP Value.</li> <li>• <b>IP DSCP Value</b> – The IP DSCP value to match.</li> </ul>
IP Precedence	<p>Select this option to require the packet's IP Precedence value to match the number configured in the IP Precedence Value field. The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header.</p>
IP TOS	<p>Select this option to require the packet's Type of Service (ToS) bits in the IP header to match the specified value. The IP ToS field in a packet is defined as all eight bits of the Service Type octet in the IP header. After you select this option, use the following fields to configure the ToS match criteria:</p> <ul style="list-style-type: none"> <li>• <b>IP TOS Bits</b> – Enter a two-digit hexadecimal number to match the bits in a packet's ToS field.</li> <li>• <b>IP TOS Mask</b> – Specify the bit positions that are used for comparison against the IP ToS field in a packet.</li> </ul>
Protocol	<p>Select this option to require a packet header's Layer 4 protocol to match the specified value. After you select this option, use one of the following fields to configure the protocol match criteria:</p> <ul style="list-style-type: none"> <li>• <b>No Protocol</b> – A non-IP L2 match DiffServ class. If you select this option, you cannot select a protocol keyword or configure a protocol value.</li> <li>• <b>Protocol</b> – The L4 keyword that corresponds to value of the IANA protocol number to match. If you select a keyword, you cannot configure a Protocol Value.</li> <li>• <b>Protocol Value</b> – The IANA L4 protocol number value to match.</li> </ul>
Flow Label	<p>Select this option to require an IPv6 packet's flow label to match the configured value. The flow label is a 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers.</p>

- Click **Refresh** to update the page with the most current data from the switch.

## DiffServ Add Match Criteria

After you click **Add Match Criteria**, the Add Match Criteria window opens and allows you to define the match criteria for the selected class. The window lists the match criteria that are available for the class.

**Figure 324.** DiffServ Add Match Criteria

<input type="checkbox"/>	Any
<input checked="" type="checkbox"/>	Reference ACL
ACL Identifier: < None Available >	
<input type="checkbox"/>	Reference Class
<input type="checkbox"/>	CoS
<input type="checkbox"/>	Secondary CoS
<input type="checkbox"/>	Ethertype
<input type="checkbox"/>	VLAN
<input type="checkbox"/>	Secondary VLAN
<input type="checkbox"/>	Source MAC Address
<input type="checkbox"/>	Destination MAC Address
<input type="checkbox"/>	Source IP Address
<input type="checkbox"/>	Destination IP Address
<input type="checkbox"/>	Source L4 Port
<input type="checkbox"/>	Destination L4 Port
<input type="checkbox"/>	IP DSCP
<input type="checkbox"/>	IP Precedence
<input type="checkbox"/>	IP TOS
<input checked="" type="checkbox"/>	Protocol
No Protocol	<input type="checkbox"/>
Protocol	< value >
Protocol Value	<input type="text"/> (0 to 255)

Submit Cancel

To add match criteria, select the check box associated with the criteria type. The fields to configure the match values appear after you select the match type. Each match criteria type can be used only once within a class. If a reference class includes the match criteria type, it cannot be used as an additional match type within the class, and the match criteria type cannot be selected or configured.

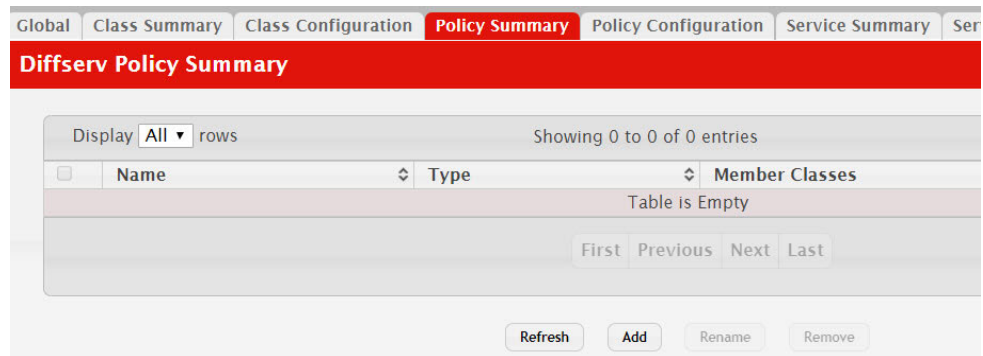
**Note:** Each match type (other than Reference Class and Reference ACL) includes an option to match any value within the match criteria type except the configured value. This is the Exclude option, which indicates a logical NOT for a match criteria type.

## DiffServ Policy Summary

Use this page to create or remove DiffServ policies and to view summary information about the policies that exist on the device. A policy defines the QoS attributes for one or more traffic classes. A policy attribute identifies the action taken when a packet matches a class rule. A policy is applied to a packet when a class match within that policy is found.

To display the Diffserv Policy Summary page, click **QoS > Diffserv > Policy Summary** in the navigation menu.

**Figure 325.** DiffServ Policy Summary



Use the buttons to perform the following tasks:

- To add a DiffServ policy, click **Add**.
- To change the name of an existing policy, select the entry to modify and click **Rename**.
- To remove one or more configured policies, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 316.** *DiffServ Policy Summary Fields*

Field	Description
Name	The name of the DiffServ policy. When adding a new policy or renaming an existing policy, the name of the policy is specified in the Policy field of the dialog window.
Type	The traffic flow direction to which the policy is applied: <ul style="list-style-type: none"> <li>• <b>In</b> – The policy is specific to inbound traffic.</li> <li>• <b>Out</b> – The policy is specific to outbound traffic direction.</li> </ul>
Member Classes	The DiffServ class or classes that have been added to the policy.

- Click **Refresh** to update the page with the most current data from the switch.

## DiffServ Policy Configuration

Use this page to add or remove a DiffServ policy-class association and to configure the policy attributes. The policy attributes identify the action or actions taken when a packet matches a class rule.

After you select the policy to configure from the Policy menu, use the buttons to perform the following tasks:

- To add a class to the policy, click **Add Class**.
- To add attributes to a policy or to change the policy attributes, select the policy with the attributes to configure and click **Add Attribute**.
- To remove the most recently associated class from the selected policy, click **Remove Last Class**.

To display the Diffserv Policy Configuration page, click **QoS > Diffserv > Policy Configuration** in the navigation menu.

**Figure 326.** DiffServ Policy Configuration

**Table 317.** DiffServ Policy Configuration Fields

Field	Description
Policy	The name of the policy. To add a class to the policy, remove a class from the policy, or configure the policy attributes, you must first select its name from the menu.
Type	The traffic flow direction to which the policy is applied.
Class	The DiffServ class or classes associated with the policy. The policy is applied to a packet when a class match within that policy-class is found.
Policy Attribute Details	The policy attribute types and their associated values that are configured for the policy.
Assign Queue	Select this option to assign matching packets to a traffic queue. Use the Queue ID Value field to select the queue to which the packets of this policy-class are assigned.
Drop	Select this option to drop packets that match the policy-class.

**Table 317.** DiffServ Policy Configuration Fields (continued)

Field	Description
Mark CoS	Select this option to mark all packets in a traffic stream with the specified Class of Service (CoS) queue value. Use the Class of Service field to select the CoS value to mark in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted.
Mark Secondary CoS	Select this option to mark all packets in a traffic stream with the specified secondary CoS queue number. Use the Class of Service field to select the CoS value to mark in the priority field of the 802.1p header in the secondary (inner) 802.1Q tag of a double VLAN tagged packet. If the packet does not already contain this header, one is inserted.
Mark IP DSCP	Select this option to mark all packets in the associated traffic stream with the specified IP DSCP value. After you select this option, use one of the following fields to configure the IP DSCP value to mark in packets that match the policy-class: <ul style="list-style-type: none"> <li>• <b>IP DSCP Keyword</b> – The IP DSCP keyword code that corresponds to the IP DSCP value. If you select a keyword, you cannot configure an IP DSCP Value.</li> <li>• <b>IP DSCP Value</b> – The IP DSCP value.</li> </ul>
Mark IP Precedence	Select this option to mark all packets in the associated traffic stream with the specified IP Precedence value. After you select this option, use the IP Precedence Value field to select the IP Precedence value to mark in packets that match the policy-class.
Mirror Interface	Select this option to copy the traffic stream to a specified egress port (physical or LAG) without bypassing normal packet forwarding. This action can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. Use the Interface menu to select the interface to which traffic is mirrored.
Police Simple	Select this option to enable the simple traffic policing style for the policy-class. The simple form of the police attribute uses a single data rate and burst size, resulting in two outcomes (conform and violate). After you select this option, configure the following policing criteria: <ul style="list-style-type: none"> <li>• <b>Color Mode</b> – The type of color policing used in DiffServ traffic conditioning.</li> <li>• <b>Color Conform Class</b> – For color-aware policing, packets in this class are metered against both the committed information rate (CIR) and the peak information rate (PIR). The class definition used for policing color awareness is only allowed to contain a single, non-excluded class match condition identifying one of the supported comparison fields: CoS, IP DSCP, IP Precedence, or Secondary CoS.</li> <li>• <b>Committed Rate (Kbps)</b> – The maximum allowed arrival rate of incoming packets for this class.</li> <li>• <b>Committed Burst Size (Kbytes)</b> – The amount of conforming traffic allowed in a burst.</li> <li>• <b>Conform Action</b> – The action taken on packets that are considered conforming (below the police rate).</li> <li>• <b>Violate Action</b> – The action taken on packets that are considered non-conforming (above the police rate).</li> </ul>

**Table 317.** DiffServ Policy Configuration Fields (continued)

Field	Description
Police Single Rate	<p>Select this option to enable the single-rate traffic policing style for the policy-class. The single-rate form of the police attribute uses a single data rate and two burst sizes, resulting in three outcomes (conform, exceed, and violate). After you select this option, configure the following policing criteria:</p> <ul style="list-style-type: none"><li>• <b>Color Mode</b> – The type of color policing used in DiffServ traffic conditioning.</li><li>• <b>Color Conform Class</b> – For color-aware policing, packets are metered against the committed information rate (CIR) and the peak information rate (PIR). The class definition used for policing color awareness is only allowed to contain a single, non-excluded class match condition identifying one of the supported comparison fields: CoS, IP DSCP, IP Precedence, or Secondary CoS. This field is available only if one or more classes that meets the color-awareness criteria exist.</li><li>• <b>Color Exceed Class</b> – For color-aware policing, packets are metered against the PIR only.</li><li>• <b>Committed Rate (Kbps)</b> – The maximum allowed arrival rate of incoming packets for this class.</li><li>• <b>Committed Burst Size (Kbytes)</b> – The amount of conforming traffic allowed in a burst.</li><li>• <b>Excess Burst Size (Kbytes)</b> – The amount of conforming traffic allowed to accumulate beyond the Committed Burst Size (Kbytes) value during longer-than-normal idle times. This value allows for occasional bursting.</li><li>• <b>Conform Action</b> – The action taken on packets that are considered conforming (below the police rate).</li><li>• <b>Exceed Action</b> – The action taken on packets that are considered to exceed the committed burst size but are within the excessive burst size.</li><li>• <b>Violate Action</b> – The action taken on packets that are considered non-conforming (above the police rate).</li></ul>



**Table 317.** DiffServ Policy Configuration Fields (continued)

Field	Description
Police Two Rate	<p>Select this option to enable the two-rate traffic policing style for the policy-class. The two-rate form of the police attribute uses two data rates and two burst sizes. Only the smaller of the two data rates is intended to be guaranteed. After you select this option, configure the following policing criteria:</p> <ul style="list-style-type: none"> <li>• <b>Color Mode</b> – The type of color policing used in DiffServ traffic conditioning.</li> <li>• <b>Color Conform Class</b> – For color-aware policing, packets are metered against the committed information rate (CIR) and the peak information rate (PIR). The class definition used for policing color awareness is only allowed to contain a single, non-excluded class match condition identifying one of the supported comparison fields: CoS, IP DSCP, IP Precedence, or Secondary COS. This field is available only if one or more classes that meets the color-awareness criteria exist.</li> <li>• <b>Color Exceed Class</b> – For color-aware policing, packets are metered against the PIR.</li> <li>• <b>Committed Rate (Kbps)</b> – The maximum allowed arrival rate of incoming packets for this class.</li> <li>• <b>Committed Burst Size (Kbytes)</b> – The amount of conforming traffic allowed in a burst.</li> <li>• <b>Peak Rate (Kbps)</b> – The maximum peak information rate for the arrival of incoming packets for this class.</li> <li>• <b>Excess Burst Size (Kbytes)</b> – The maximum size of the packet burst that can be accepted to maintain the Peak Rate (Kbps).</li> <li>• <b>Conform Action</b> – The action taken on packets that are considered conforming (below the police rate).</li> <li>• <b>Exceed Action</b> – The action taken on packets that are considered to exceed the committed burst size but are within the excessive burst size.</li> <li>• <b>Violate Action</b> – The action taken on packets that are considered non-conforming (above the police rate).</li> </ul>
Redirect Interface	<p>Select this option to force a classified traffic stream to the specified egress port (physical port or LAG). Use the Interface field to select the interface to which traffic is redirected.</p>

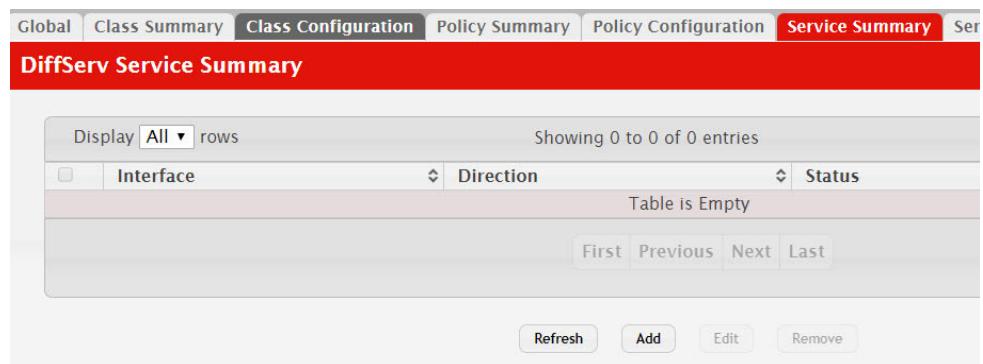
- Click **Refresh** to update the page with the most current data from the switch.

## DiffServ Service Summary

Use this page to add DiffServ policies to interfaces, remove policies from interfaces, and edit policy-interface mappings.

To display the DiffServ Service Summary page, click **QoS > Diffserv > Service Summary** in the navigation menu.

**Figure 327.** DiffServ Service Summary



Use the buttons to perform the following tasks:

- To add a policy to an interface, click **Add**.
- To edit a configured interface-policy association, select the entry to modify and click **Edit**.
- To remove one or more configured interface-policy associations, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

**Table 318.** DiffServ Service Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. Only interfaces that have an associated policy are listed in the table.
Direction	The traffic flow direction to which the policy is applied: <ul style="list-style-type: none"> <li>• <b>Inbound</b> – The policy is applied to traffic as it enters the interface.</li> <li>• <b>Outbound</b> – The policy is applied to traffic as it exits the interface.</li> </ul>
Status	The status of the policy on the interface. A policy is Up if DiffServ is globally enabled, and if the interface is administratively enabled and has a link. Otherwise, the status is Down.
Policy	The DiffServ policy associated with the interface.
When you click <b>Add</b> or <b>Edit</b> , the Configure Service window opens and allows you to configure DiffServ interface policies. Specifying 'None' for a policy has no effect when adding or editing interface policies. To remove an interface policy mapping, use the Remove button on the parent page. The following information describes the fields in this window.	
Interface	Select an interface to associate with a policy.
Policy In	The menu lists all policies configured with a type of In. Select the policy to apply to traffic as it enters the interface.
Policy Out	The menu lists all policies configured with a type of Out. Select the policy to apply to traffic as it exits the interface.

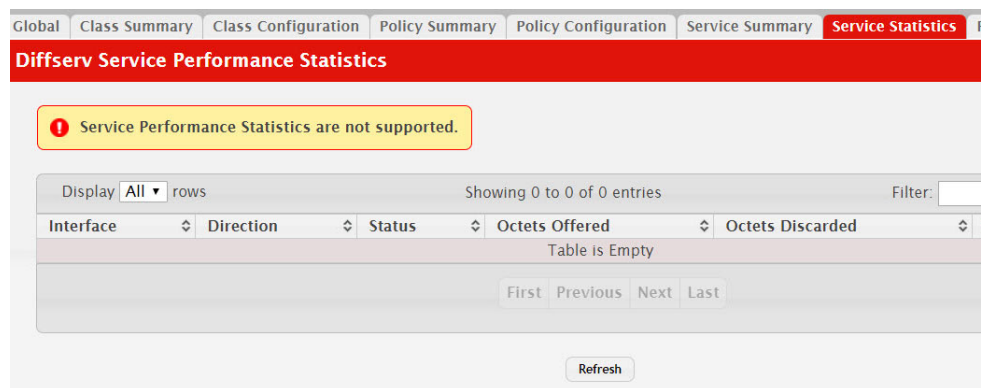
- Click **Refresh** to update the page with the most current data from the switch.

## DiffServ Service Statistics

This page displays service-level statistical information for all interfaces in the system to which a DiffServ policy has been attached.

To display the Diffserv Service Statistics page, click **QoS > Diffserv > Service Statistics** in the navigation menu.

**Figure 328.** DiffServ Service Performance Statistics



**Table 319.** DiffServ Service Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. The table displays all interfaces that have a DiffServ policy currently attached in a traffic flow direction.
Direction	The traffic flow direction to which the policy is applied: <ul style="list-style-type: none"> <li>• <b>In</b> – The policy is applied to traffic as it enters the interface.</li> <li>• <b>Out</b> – The policy is applied to traffic as it exits the interface.</li> </ul>
Status	The operational status of this service interface, either Up or Down.
Octets Offered	The total number of octets offered to all class instances in this service policy before their defined DiffServ treatment is applied. This is the overall count per-interface, per-direction.
Octets Discarded	The total number of octets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.
Octets Sent	The total number of octets forwarded for all class instances in this service policy after their defined DiffServ treatments were applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function of an outbound link transmission element. This is the overall count per-interface, per-direction.

- Click **Refresh** to update the page with the most current data from the switch.

## DiffServ Service Policy Statistics

This page displays class-oriented statistical information for the policy, which is specified by the interface and direction.

To display the Diffserv Service Policy Statistics page, click **QoS > Diffserv > Policy Statistics** in the navigation menu.

**Figure 329.** DiffServ Service Policy Statistics



**Table 320.** DiffServ Service Policy Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. The table displays all interfaces that have a DiffServ policy currently attached in a traffic flow direction.
Direction	The traffic flow direction to which the policy is applied: <ul style="list-style-type: none"> <li>• <b>In</b> – The policy is applied to traffic as it enters the interface.</li> <li>• <b>Out</b> – The policy is applied to traffic as it exits the interface.</li> </ul>
Policy	The name of the policy currently attached to the interface.
Status	The operational status of the policy currently attached to the interface.
Class	The DiffServ class currently defined for the attached policy.
Octets Offered	The total number of octets offered to all class instances in this service policy before their defined DiffServ treatment is applied. This is the overall count per-interface, per-direction.
Octets Discarded	The total number of octets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.
Packets Offered	The total number of packets offered to all class instances in this service policy before their defined DiffServ treatment is applied. This is the overall count per-interface, per-direction.
Packets Discarded	The total number of packets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.

- Click **Refresh** to update the page with the most current data from the switch.

## Chapter 9. Configuring Stacking

CE0128XB/CE0152XB supports stacking. Use the links in the Stacking navigation menu folder to manage stacking on the system.

### Managing Stack Summary

Use the Stacking Summary page to view summary information about each unit in the stack and to add or remove stack units. A stack is a set of multiple devices that are connected through their stacking ports. One of the devices controls the operation of the stack and is called the stack manager. All other devices in the stack are stack members. The stack members use stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire stack as a single entity to the network.

To display the Stacking Summary page, click **Stacking > Base > Stack Summary** in the navigation menu.

Switch ID	Status	Management Status	Standby Switch	Preconfigured Model Identifier	Plugged-in Model Identifier	Software Version
1	OK	Management Switch		CE0128PB	CE0128PB	1.4.23.37

Use the buttons to perform the following tasks:

- To preconfigure a unit before physically adding it to the stack, click **Add**. When a unit is physically connected to the stack and powered on, it is automatically added to the stack and its entry will appear in the table. A preconfigured unit allows for the adjustment of certain settings which will be applied to the unit when it is physically connected and powered on.
- To change the settings for a unit, select the entry to update and click **Edit**.
- To remove one or more preconfigured units from the stack before it is connected, select each preconfigured entry to remove and click **Remove**. A unit that is physically connected to the stack and powered on cannot be manually removed from the table.

**Table 321: Stacking Summary Fields**

Field	Description
Switch ID	The ID of the unit in the stack. The Switch ID does not impact whether the unit is the stack manager or a stack member. The maximum number of units allowed in the stack is 8. A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a switch stack, its default stack member number changes to the lowest available member number in the stack. The stack manager cannot be removed.
Status	The unit status: <ul style="list-style-type: none"> <li>• <b>OK</b> – The unit is operating within the stack. It is physically connected to the stack and is powered on.</li> <li>• <b>Not Present</b> – The unit is not operating within the stack.</li> </ul>
Management Status	The role of the unit within the stack: <ul style="list-style-type: none"> <li>• <b>Management Unit</b> – The unit is performing the stack manager functions for the stack and is the single point of stack-wide management. The stack manager maintains the saved and running configuration files for the switch stack.</li> <li>• <b>Stack Member</b> – The unit is not a stack manager, but it has connectivity to the stack manager.</li> <li>• <b>Unassigned</b> – The management status of the unit has not been assigned. This status might occur because the maximum number of units already exist in the stack or the unit is not present.</li> </ul>
Standby Switch	The standby status of the unit. The standby unit in the stack takes over as the stack manager if the current stack manager fails. <ul style="list-style-type: none"> <li>• <b>Operational Standby</b> – The unit has connectivity to the stack manager and has been nominated to take over as manager should the current manager fail.</li> <li>• <b>Configured Standby</b> – The unit has been manually configured to take over as manager should the current manager fail. The unit does not need to be connected to the stack to be configured as the standby unit.</li> <li>• If the field is blank, the unit has not been auto-selected or configured as the standby unit for the stack.</li> </ul>
Preconfigured Model Identifier	The value assigned by the device manufacturer to identify the device.
Plugged-in Model Identifier	The value assigned by the device manufacturer to identify the plugged-in device.
Software Version	The detected software version of code on this unit.
Nonstop Forwarding Unit Support	The nonstop forwarding (NSF) support status of the unit. NSF allows the forwarding plane of stack units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the stack manager and allows the standby unit to quickly take over as the stack manager.
SFS Last Attempt Status	The status of the last attempt to synchronize the firmware of the unit. Stack Firmware Synchronization (SFS) is performed when the feature is enabled and the unit added to the stack has a firmware version different from the master.

Click **Submit** to apply the settings to the running configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save Configuration** is performed.

Click **Refresh** to display the latest information from the switch.

## Configuring Stacking Unit

Use the Stacking Unit Configuration page to view information about each stack unit, renumber a unit, change which unit is the stack manager, configure the standby switch, or select the administrative management preference of a unit.

To display the Stacking Unit Configuration page, click **Stacking > Base > Unit Configuration** in the navigation menu.

Unit Configuration	
Switch ID	1
Serial Number	
Status	OK
Description	Lenovo CE0128PB Switch
Management Status	Management Switch
Hardware Management Preference	Unassigned
Operational Standby Status	No
Standby Switch	<input type="checkbox"/>
Admin Management Preference	Unassigned
Switch Type	0xb1500004
Preconfigured Model Identifier	CE0128PB
Plugged-in Model Identifier	CE0128PB
Detected Software Version	1.4.23.37
Detected Software Version in Flash	1.4.23.37
System Up Time	2 days, 13 hours, 52 mins, 40 secs

**Table 322: Stacking Unit Configuration Fields**

Field	Description
Switch ID	The ID of the unit in the stack. Use the drop-down menu to select the unit with the information to view or configure. A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a switch stack, its default stack member number changes to the lowest available member number in the stack.  To change the Switch ID of a unit, click the <b>Edit</b> icon. In the <b>Edit Switch ID</b> window, use the <b>Change Switch ID To</b> field to select the new Switch ID. Renumbering a non-manager unit requires a unit reset for the renumbering to take effect. Renumbering a manager unit requires a reset of all the switches in the stack for the renumbering to take effect.
Serial Number	The unique device serial number assigned by the device manufacturer.
Status	The unit status: <ul style="list-style-type: none"> <li>• <b>OK</b> – The unit is operating within the stack. It is physically connected to the stack and is powered on.</li> <li>• <b>Not Present</b> – The unit is not operating within the stack.</li> </ul>
Description	The product name of this device.



**Table 322: Stacking Unit Configuration Fields (continued)**

Field	Description
Management Status	<p>The role of the unit within the stack:</p> <ul style="list-style-type: none"> <li>• <b>Management Unit</b> – The unit is performing the stack manager functions for the stack and is the single point of stack-wide management. The stack manager maintains the saved and running configuration files for the switch stack.</li> <li>• <b>Stack Member</b> – The unit is not a stack manager, but it has connectivity to the stack manager.</li> <li>• <b>Unassigned</b> – The management status of the unit has not been assigned. This status might occur because the maximum number of units already exist in the stack or the unit is not present.</li> </ul> <p>To change which unit is the stack manager, click the <b>Move Switch Management</b> icon in the Management Status field. In the <b>Move Switch Management</b> window, use the <b>Move Switch Management To</b> field to select the Switch ID of the unit that should take over the stack manager role. The operation may take three minutes or longer depending on the stack size and configuration.</p>
Hardware Management Preference	<p>A two-byte value set by the device manufacturer that indicates whether this unit is capable of becoming the stack manager. If the value is set to zero then the unit cannot support the stack manager function. A higher value means that the unit is more desirable than another unit with a lower value for running the management function.</p>
Operational Standby Status	<p>The operational standby status of the unit. If the status is Yes, the unit has connectivity to the stack manager and has been nominated to take over as manager should the current manager fail.</p>
Standby Switch	<p>Select the check box to configure the unit as the standby unit. The unit does not need to be connected to the stack to be configured as the standby unit. Only one unit can be configured as the standby unit.</p>
Admin Management Preference	<p>The administrative management preference of the unit. When stack manager election or re-election occurs, the unit with the highest administrative preference value becomes the stack manager. Setting the preference to Disabled makes it ineligible for manager selection.</p>
Switch Type	<p>The hardware type value of this supported device.</p>
Preconfigured Model Identifier	<p>The value assigned by the device manufacturer to identify the device.</p>
Plugged-in Model Identifier	<p>The value assigned by the device manufacturer to identify the plugged-in device.</p>
Detected Software Version	<p>The release number and version number of the code detected on the unit.</p>
Detected Software Version in Flash	<p>The release number and version number of the code detected on flash for the unit.</p>
System Up Time	<p>The time in days, hours, minutes and seconds since the system was last reset.</p>

Click **Submit** to apply the settings to the running configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save Configuration** is performed.

Click **Refresh** to display the latest information from the switch.

## Viewing Supported Switches

Use the Supported Switches page to view information about the devices that can be combined to form a stack. To view additional information about a supported device, select the entry and click **Details**.

To display the Supported Switches page, click **Stacking > Base > Supported Switches** in the navigation menu.

Index	Model ID	Type	Description
1	CE0128TB	B1500003	Lenovo CE0128TB Switch
2	CE0128PB	B1500004	Lenovo CE0128PB Switch
3	CE0152TB	B1500005	Lenovo CE0152TB Switch
4	CE0152PB	B1500006	Lenovo CE0152PB Switch

**Table 323: Supported Switches Fields**

Field	Description
Index	The index assigned to the device type. The Index is used when pre-configuring a stack member by using the CLI or SNMP.
Model ID	The string that identifies the model of the supported switch or card.
Type	The hardware type value of the supported device.
Description	The product name of the device.
Hardware Management Preference	A two-byte value set by the device manufacturer that indicates whether this unit is capable of becoming the stack manager. If the value is set to zero, the unit cannot support the stack manager function. A higher value means that the unit is more desirable than another unit with a lower value for running the management function.
Expected Software Version	The release number and version number of the code that is expected to be loaded on this device.

After you select an entry in the table and click **Details**, the **Supported Switch Details** window opens. The following information describes the additional fields that appear in this window.

**Table 324: Supported Switch Details Fields**

Field	Description
Slot Index	A possible slot index for the supported switch. Support for changing the slot configuration is platform dependent. This value is helpful when configuring the system by using SNMP or the CLI.

**Table 324: Supported Switch Details Fields (continued)**

Field	Description
Card Index	A possible card index that can be inserted into the associated slot. Support for adding cards to a slot is platform dependent. This value is helpful when configuring the system by using SNMP or the CLI.

Applied changes update the running configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save Configuration** is performed.

Click **Refresh** to display the latest information from the switch.

## Updating Firmware

Use the Firmware Update page to update the firmware on one or more units in the stack. The image from the stack manager is copied to the selected stack member as either the active or backup image on the stack member.

To display the Firmware Update page, click **Stacking > Base > Firmware Update** in the navigation menu.

**Table 325: Firmware Update Fields**

Field	Description
Stack Manager Source Image	The list of available images on the stack manager that can be transferred to other units.
Destination Switch ID	Select the unit to which to transfer the stack manager firmware image. The menu lists all units of the stack, including the stack manager.
Destination Image	Select the image on the destination unit to overwrite.
Status	The firmware update status after initiating the update. The status is one of the following: <ul style="list-style-type: none"> <li>• <b>Transfer in progress. Please wait...</b></li> <li>• <b>Transfer completed</b></li> <li>• <b>Transfer failed</b></li> <li>• If the field is blank, a firmware update has not been initiated on the selected unit.</li> </ul>

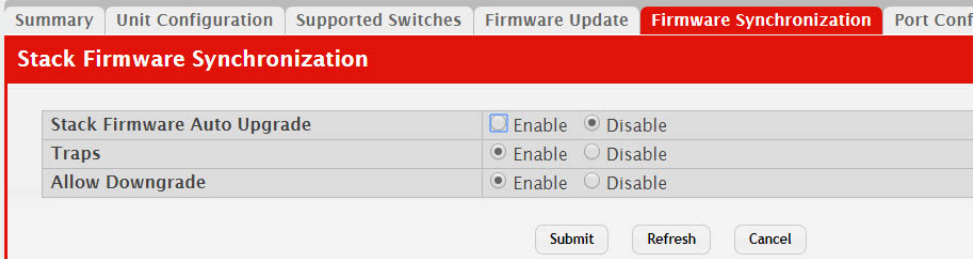
Click **Begin Transfer** to initiate the transfer. Updating the firmware may take several minutes to complete. The update may take longer when more devices are in the stack.

Applied changes update the running configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save Configuration** is performed.

## Synchronizing Firmware

Use this page to configure the Stack Firmware Synchronization (SFS) settings on the stack. SFS provides the ability to automatically synchronize firmware for all stack members. If a unit joins the stack and its firmware version is different from the version running on the stack manager, the SFS feature can either upgrade or downgrade the firmware on the mismatched stack member. There is no attempt to synchronize the stack to the latest firmware of a member that joins the stack.

To display the Firmware Synchronization page, click **Stacking > Base > Firmware Synchronization** in the navigation menu.



**Table 326: Stack Firmware Synchronization Fields**

Field	Description
Stack Firmware Auto Upgrade	Enable or disable the Stack Firmware Synchronization feature on the stack. Enabling the feature allows the stack manager to automatically upgrade the firmware version of a unit that joins the stack if the firmware version on the new stack member is older than the firmware version on the stack manager.
Traps	Enable or disable the sending of SNMP traps during SFS start, failure, or finish.
Allow Downgrade	Enable or disable the ability of the stack manager to downgrade the image on a new stack member if the firmware version on the manager is older than the firmware version on the new stack member.

If you make any changes to the page, click **Submit** to apply the changes to the system.

If you want the device to retain these changes across a reset, you must first save the configuration by clicking **Save Configuration**.

Click **Refresh** to redisplay the page with the current data from the switch.

## Configuring Stack Ports

Use Port Configuration page to view and configure stacking functionality on ports that support stacking. For these ports, you can administratively enable stacking mode or Ethernet mode. In Ethernet mode, the port functions like other non-stacking ports. To change the stack mode on a port, select the port to configure and click **Edit**.

Stacks should always be configured in a ring topology in order to support robust failover to the standby unit.

The 10G ports may be configured as stacking or as Ethernet in pairs. Configuring a 10G Ethernet port as stacking will also configure the paired link as stacking. Likewise, configuring a 10G stack port as Ethernet will configure the paired link as Ethernet. On the CE0152XB, ports 49/50 and 51/52 are paired. On the CE0128XB, ports 25/26 and 27/28 are paired.

To display the Port Configuration page, click **Stacking > Base > Port Configuration** in the navigation menu.

Unit	Interface	Configured Stack Mode	Running Stack Mode	Link Status	Link Speed (Gbps)
1	0/25	Stack	Stack	Link Down	10
1	0/26	Stack	Stack	Link Down	10
1	0/27	Stack	Stack	Link Down	10
1	0/28	Stack	Stack	Link Down	10

**Table 327: Stack Port Configuration Fields**

Field	Description
Unit	The number that identifies the unit within the stack (also called Switch ID).
Interface	The stackable interfaces on the unit. The table displays only the ports that can be used for physically connecting multiple devices to form a stack.
Configured Stack Mode	The manually-configured mode for the interface, which is either Stack or Ethernet. If you change the stack mode on a port, the configuration is immediately saved in the NVRAM on the unit on which the port is located. However, the run-time mode is not changed until the unit resets.
Running Stack Mode	The mode in which the interface is currently operating.
Link Status	The link status of the port, which is either Up or Down.
Link Speed	The maximum speed of the stacking port.

After you select a port and click **Edit**, a window opens and allows you to configure the stack port mode. The additional field available in the window is described below.

**Table 328: Stack Port Configuration Fields**

Field	Description
Interface Mode	<p>The stack mode to configure on the port. The options are:</p> <ul style="list-style-type: none"><li>• <b>Ethernet</b> – Configure the port to operate as an Ethernet port that connects to other network devices, such as servers or end-user hosts.</li><li>• <b>Stack</b> – Configure the port to operate as a stacking port that connects to other units within the stack.</li></ul> <p>If you change the stack mode on a port, the configuration is immediately saved in the NVRAM on the unit on which the port is located. However, the run-time mode is not changed until the unit resets.</p>

Applied changes update the device running configuration. If you want the device to retain these changes across a reset, you must first save the configuration by clicking **Save Configuration**.

Click **Refresh** to redisplay the page with the current data from the switch.

## Viewing Port Statistics

Use the Statistics page to view data transmission information for the stacking ports on each stack unit.

To display the Statistics page, click **Stacking > Base > Statistics** in the navigation menu.

Unit	Interface	Transmit Data Rate (Mbps)	Transmit Error Rate (Errors/s)	Transmit Total Errors	Receive Data Rate (Mbps)	Receive Error Rate (Errors/s)	Receive Total Errors
1	0/25	0	0	0	0	0	0
1	0/26	0	0	0	0	0	0
1	0/27	0	0	0	0	0	0
1	0/28	0	0	0	0	0	0

**Table 329: Port Statistics Fields**

Field	Description
Unit	The number that identifies the unit within the stack (also called Switch ID).
Interface	The interface ID of the stackable interface on the unit.
Transmit Data Rate (Mbps)	The approximate rate at which the stack port transmits data.
Transmit Error Rate (Errors/s)	The approximate rate at which the stack port encounters errors when attempting to transmit data.
Transmit Total Errors	The total number of errors the stack port has encountered during data transmission since the unit booted. The counter might wrap if the number of errors exceeds the number the page can display.
Receive Data Rate (Mbps)	The approximate rate at which the stack port receives data.
Receive Error Rate (Errors/s)	The approximate rate at which the stack port encounters errors when attempting to receive data.
Receive Total Errors	The total number of errors the stack port has encountered while attempting to receive data since the unit booted. The counter might wrap if the number of errors exceeds the number the page can display.

Click **Refresh** to redisplay the page with the current data from the switch.



## Viewing Port Diagnostics

Use the Diagnostics page to view diagnostic information about stack ports. The page displays three text fields that are populated by the driver and contain debug and status information. Each text field supports a string of up to 80 characters. The following abbreviations are used in the information messages:

- RBYT: Received bytes (including CRC)
- RPKT: Received packets
- TBYT: Transmit bytes
- TPKT: Transmit packets
- RFCS: Receive FCS (CRC) error packet counter
- RFRG: Fragmented packets received (undersized packets with invalid CRC)
- RJBR: Oversized packets with invalid CRC
- RUND: Undersized packets (contains a valid CRC)
- ROVR: Oversized packets with no errors
- RUNT: Frames that are less than the IEEE 802.3 minimum length of 64 octets
- TFCS: Frames transmitted with an FCS error (CRC checks failed)
- TERR: Frames transmitted with any error

To display the Diagnostics page, click **Stacking > Base > Diagnostics** in the navigation menu.

Unit	Interface	Info 1	Info 2	Info 3
1	0/25	RBYT:0 RPKT:0 TBYT:0 TPKT:0	RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0	TFCS:0 TERR:0
1	0/26	RBYT:0 RPKT:0 TBYT:0 TPKT:0	RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0	TFCS:0 TERR:0
1	0/27	RBYT:0 RPKT:0 TBYT:0 TPKT:0	RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0	TFCS:0 TERR:0
1	0/28	RBYT:0 RPKT:0 TBYT:0 TPKT:0	RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0	TFCS:0 TERR:0

**Table 330: Diagnostics Fields**

Field	Description
Unit	The number that identifies the unit within the stack (also called Switch ID).
Interface	The stackable interface on the unit.
Info 1	Debug and status driver information.
Info 2	Debug and status driver information.
Info 3	Debug and status driver information.

Applied changes update the device running configuration. If you want the device to retain these changes across a reset, you must first save the configuration by clicking **Save Configuration**.

Click **Refresh** to redisplay the page with the current data from the switch.

# Configuring Nonstop Forwarding

Use the Nonstop Forwarding Summary page to configure the administrative mode of the nonstop forwarding (NSF) feature on the system, view NSF status information, or initiate a failover from the stack manager to the standby unit. NSF allows the forwarding plane of stack units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the stack manager and allows the standby unit to quickly take over as the stack manager.

To display the Nonstop Forwarding Summary page, click **Stacking > NSF > Summary** in the navigation menu.

Nonstop Forwarding Summary	
Admin Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Operational Status	Enabled
Last Startup Reason	Power On Start
Time Since Last Restart	2 days, 13 hours, 54 mins, 50 secs
Restart In Progress	No
Warm Restart Ready	No
Running Configuration Backup Copy Status	
Status	No Backup Unit
Backup Configuration Age	Not Yet Copied

**Table 331: Nonstop Forwarding Summary Fields**

Field	Description
Admin Mode	Enable or disable the administrative mode of NSF on the stack. When enabled, the stack selects a standby unit. Applications on the stack manager copy data to the standby unit, which is called data checkpointing. If the stack manager fails, the standby unit takes over as the stack manager without clearing the hardware tables of any of the surviving units. Data traffic continues to be forwarded in hardware while the management functions initialize on the standby unit. A possible reason for disabling NSF would be to redirect the CPU resources consumed by data checkpointing.
Operational Status	Indicates whether NSF is operational on the stack, which may differ from the Admin Mode setting. If a unit that does not support NSF is connected to the stack, then NSF is disabled on all stack members. When a unit that does not support NSF is disconnected from the stack and all other units support NSF (and NSF is administratively enabled), then NSF operation resumes.

**Table 331: Nonstop Forwarding Summary Fields (continued)**

Field	Description
Last Startup Reason	The type of activation that caused the software to start the last time. The possible values are: <ul style="list-style-type: none"> <li>• <b>Power On Start</b> – The switch rebooted, caused by a power cycle or an administrative reload command.</li> <li>• <b>Administrative Move</b> – The administrator issued a command to move the management functions to a different unit within the stack.</li> <li>• <b>Warm Admin Move</b> – The administrator initiated a failover.</li> <li>• <b>Warm</b> – The primary management card restarted due to a failure, and the system executed a nonstop forwarding failover to a standby management unit.</li> <li>• <b>Auto Cold</b> – The system switched from the stack manager to the standby unit and was unable to maintain user data traffic. This is usually caused by multiple failures occurring close together.</li> </ul>
Time Since Last Restart	Time since the current management card became the active management card.
Restart In Progress	Identifies whether a restart is in progress. A restart is not considered complete until all hardware tables have been fully reconciled.
Warm Restart Ready	Indicates whether a failover can currently be initiated on the stack master. The stack manager might not be ready for a warm restart if, for example, no standby unit has been elected, one or more stack members do not support nonstop forwarding, or the initial full checkpoint has not finished.
Status	The status of copying the running configuration to the standby unit.
Backup Configuration Age	The time since the running configuration was last copied from the stack manager to the standby unit.

Click **Initiate Failover** to start a warm restart. On a warm restart, the standby unit becomes the stack manager without clearing its hardware tables (on a cold restart, hardware tables are cleared). Applications apply checkpointed data from the former stack manager to the standby unit as the original stack manager reboots. If the stack manager is not ready for a warm restart the command fails with a warning message.

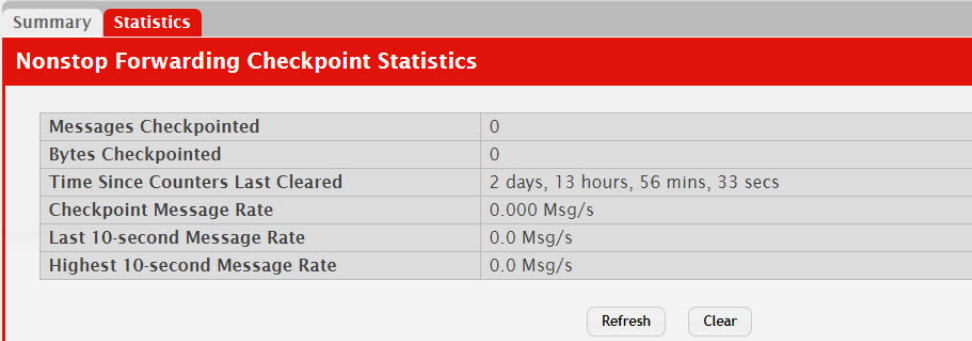
Click **Submit** to apply the settings to the running configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save Configuration** is performed.

Click **Refresh** to display the latest information from the switch.

## Viewing Nonstop Forwarding Checkpoint Statistics

Use the Nonstop Forwarding Checkpoint Statistics page to view information about the checkpoint data that is copied from the stack manager to the standby unit.

To display the Nonstop Forwarding Summary page, click **Stacking > NSF > Statistics** in the navigation menu.



Nonstop Forwarding Checkpoint Statistics	
Messages Checkpointed	0
Bytes Checkpointed	0
Time Since Counters Last Cleared	2 days, 13 hours, 56 mins, 33 secs
Checkpoint Message Rate	0.000 Msg/s
Last 10-second Message Rate	0.0 Msg/s
Highest 10-second Message Rate	0.0 Msg/s

**Table 332: Nonstop Forwarding Statistics Fields**

Field	Description
Messages Checkpointed	The number of messages sent from the stack manager to the standby unit.
Bytes Checkpointed	The amount of data that has been sent from the stack manager to the standby unit.
Time Since Counters Last Cleared	The amount of time since the checkpoint statistics counters were last reset.
Checkpoint Message Rate	The estimated number of messages sent per second.
Last 10-second Message Rate	The average number of messages per second sent over the last 10-second measurement interval.
Highest 10-second Message Rate	The highest number of messages per second sent over any 10-second measurement interval.

Click **Clear** to reset all nonstop forwarding checkpoint statistics values on this page.

Applied changes update the device running configuration. If you want the device to retain these changes across a reset, you must first save the configuration by clicking **Save Configuration**.

Click **Refresh** to display the latest information from the switch.



---

## Appendix A. Getting Help and Technical Assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.

Go to the [Lenovo Support portal](https://datacentersupport.lenovo.com/us/en/) at <https://datacentersupport.lenovo.com/us/en/> to check the product service information.

- Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number
  - Model number
  - Serial number
  - Current firmware levels
  - Other pertinent information such as error messages and logs
- Start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The Lenovo service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most

systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.



---

## Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.  
1009 Think Place - Building One  
Morrisville, NC 27560  
U.S.A.

Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties.

Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

---

## Trademarks

Lenovo, the Lenovo logo, Flex System, System x, NeXtScale System, and X-Architecture are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

---

## Important Notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as total bytes written (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

---

## Open Source Information

This Lenovo Switch may include software made publicly available by Lenovo, including software licensed under the General Public License and/or the Lesser General Public License (the “open source software”).

You may obtain the corresponding machine-readable copy for any such open source software licensed under the General Public License and/or the Lesser General Public License (or any other license requiring us to make a written offer to provide corresponding source code to you) from Lenovo for a period of three years without charge except for the cost of media, shipping, and handling, upon written request to Lenovo. This offer is valid to anyone in receipt of this Lenovo Switch. You may send your request in writing to the address below accompanied by a check or money order for \$5 to:

Lenovo Legal Department

Attn: Open Source Team / Source Code Requests

8001 Development Dr.

Morrisville, NC 27560

Please include both a “NOS” Release version and model number or Machine Type (MT) of your Lenovo Switch as part of your request. Be sure to provide a return address.

The open source software is distributed in hope it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See for example the GNU General Public License and/or the Lesser General Public License for more information.

Visit <https://datacentersupport.lenovo.com/us/en/> and enter the model number or Machine Type (MT) for your Switch to view additional information regarding licenses, acknowledgments and required copyright notices for the open source software used on your Switch.

---

## Recycling Information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to:

<http://www.lenovo.com/recycling>

## Particulate Contamination

**Attention:** Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility..

Contaminant	Limits
Particulate	<ul style="list-style-type: none"> <li>The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2<sup>1</sup>.</li> <li>Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282.</li> <li>The deliquescent relative humidity of the particulate contamination must be more than 60%<sup>2</sup>.</li> <li>The room must be free of conductive contamination such as zinc whiskers.</li> </ul>
Gaseous	<ul style="list-style-type: none"> <li>Copper: Class G1 as per ANSI/ISA 71.04-1985<sup>3</sup></li> <li>Silver: Corrosion rate of less than 300 Å in 30 days</li> </ul>

<sup>1</sup> ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

<sup>2</sup> The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

<sup>3</sup> ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

---

## Telecommunication Regulatory Statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.



---

## Electronic Emission Notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

### Federal Communications Commission (FCC) Statement

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

Properly shielded and grounded cables and connectors must be used to meet FCC emission limits. Lenovo is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

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

### Industry Canada Class A Emission Compliance Statement

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

### Avis de Conformité à la Réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

### Australia and New Zealand Class A Statement

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

### European Union - Compliance to the Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC (until April 19, 2016) and EU Council Directive 2014/30/EU (from April 20, 2016) on the approximation of the laws of the Member States relating to electromagnetic compatibility. Lenovo cannot accept responsibility for

any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

This product has been tested and found to comply with the limits for Class A equipment according to European Standards harmonized in the Directives in compliance. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.



Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

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

## Germany Class A Statement

**Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EG Richtlinie 2004/108/EC (früher 89/336/EWG), für Geräte der Klasse A.**

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die Lenovo (Deutschland) GmbH, Gropiusplatz 10, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 4 Abs. (1) 4:

**Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.**

Nach der EN 55022: "Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen."

Nach dem EMVG: Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG (früher 89/336/EWG) zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

## Deutschland:

### **Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln**

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln" EMVG (früher "Gesetz über die elektromagnetische Verträglichkeit von Geräten"). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG (früher 89/336/EWG) in der Bundesrepublik Deutschland.

### **Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EG Richtlinie 2004/108/EC (früher 89/336/EWG), für Geräte der Klasse A.**

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die Lenovo (Deutschland) GmbH, Gropiusplatz 10, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 4 Abs. (1) 4:

### **Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.**

Nach der EN 55022: "Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen."

Nach dem EMVG: "Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbüchern angegeben, zu installieren und zu betreiben.

## Japan VCCI Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

## Japan Electronics and Information Technology Industries Association (JEITA) Statement

高調波ガイドライン適合品

Japan Electronics and Information Technology Industries Association (JEITA)  
Confirmed Harmonics Guidelines (products less than or equal to 20 A per phase)

高調波ガイドライン準用品

Japan Electronics and Information Technology Industries Association (JEITA)  
Confirmed Harmonics Guidelines with Modifications (products greater than 20 A per phase).

## Korea Communications Commission (KCC) Statement

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

This is electromagnetic wave compatibility equipment for business (Type A).  
Sellers and users need to pay attention to it. This is for any areas other than home.

## Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.  
В жилых помещениях оно может создавать радиопомехи, для  
снижения которых необходимы дополнительные меры

## People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，  
可能需要用户对其干扰采取切实可行的措施。

## Taiwan Class A compliance statement

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

