Alcatel·Lucent Enterprise

Software User Manual

OS2220 Websmart

Administrator's Guide

SOFTWARE VERSION 8.3.1

060522-10 Rev. A

April 2018

26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500 FAX (818) 880-3505

Service & Support Contact Information

North America: 800-995-2696

Latin America: 877-919-9526

EMEA: +800 00200100 (Toll Free) or +1(650)385-2193

Asia Pacific: +65 6240 8484

Web: businessportal2.alcatel-lucent.com

Email: ebg_global_supportcenter@al-enterprise.com

Table of Contents

Section 1: Introduction 8
About This Document 8
Document Organization 8
References 8
About OS2220 Websmart Software Modules 9
Section 2: Getting Started 10
Connecting the Switch to the Network 10
Using the Default Management IP Address 10
Understanding the User Interfaces 11
Using the Web Interface 12
Device View 14
Navigation Menu 15
Configuration and Status Fields 16
Table Sorting 16
Help Page Access 16
User-Defined Fields 17
Using SNMP 17
Section 3: Configuring System Information 18
Viewing the Dashboard 19
Viewing Inventory Information 21
Viewing the System Firmware Status 22
Dual Image Status 22
Dual Image Configuration and Upgrade 23
Defining General Device Information 25
System Description 26
Defining System Information 27
Switch Configuration 27
IPv4 Network Connectivity Configuration 28
HTTP Configuration 29
Debug Telnet Server 30
Management Access Control and Administration List 31
User Accounts 32
User Domain Name 33
Select Authentication List 35
Denial of Service 36

Configuring and Searching the Forwarding Database 38
Switch Configuration 38
Managing Logs 39
Log Configuration 39
Buffered Log 41
Event Log 42
Hosts Log Configuration 43
Adding a Remote Logging Host 44
Deleting a Remote Logging Host 45
Configuring Power Over Ethernet (PoE) and PoE Statistics 46
PoE Configuration 46
PoE Port Configuration 47
PoE Port Statistics 50
Viewing Device Port Information 51
Port Summary 51
Port Description 55
Cable Test 56
Mirroring 57
Configuring a Port Mirroring Session 58
Configuring a Port Mirroring Source 59
Configuring the Destination Port for a Port Mirroring Session 61
Removing or Modifying a Port Mirroring Session 61
Mirroring Summary 62
Port Green Mode Statistics 63
Port Green Mode EEE History 64
Defining SNMP Parameters 65
SNMP v1 and v2 65
SNMP v3 65
SNMP Community Configuration 66
Trap Receiver v1/v2 Configuration 67
Supported MIBs 69
Viewing System Statistics 69
Switch Detailed Statistics 70
Port Summary 71
Using System Utilities 73
System Reset 73
Transfer 74
Core Dump 77
Core Dump Test 79

Configuring Time Ranges 80
Time Range Configuration 80
Time Range Entry Configuration 81
Configuring SNTP Settings 83
SNTP Global Configuration 84
SNTP Global Status 85
SNTP Server Configuration 87
SNTP Server Status 88
Configuring the Time Zone 89
Time Zone Configuration 90
Summer Time Configuration 91
Section 4: Configuring Switching Information 93
Managing VLANs 94
VLAN Status 94
VLAN Port Configuration 96
VLAN Port Summary 98
Switchport Summary 99
Reset VLAN Configuration 101
RSPAN Configuration 101
Voice VLAN Configuration 102
Voice VLAN Interface 103
Creating MAC Filters 104
MAC Filter Configuration 104
Adding MAC Filters 105
Modifying MAC Filters 105
Removing MAC Filters 105
Configuring IGMP Snooping 106
Global Configuration and Status 107
Interface Configuration 108
Source Specific Multicast 109
VLAN Status 110
Multicast Router Configuration 111
Multicast Router VLAN Status 112
Multicast Router VLAN Configuration 113
Creating Port Channels 114
Port Channel Summary 115
Port Channel Configuration 116
Port Channel Statistics 118

Viewing Multicast Forwarding Database Information 119
MFDB Table 119
GMRP Table 121
IGMP Snooping Table 122
MFDB Statistics 123
Configuring Spanning Tree Protocol 124
Switch Configuration/Status 125
CST Configuration 126
CST Port Configuration 128
MST Configuration 131
MST Port Configuration 132
Spanning Tree Statistics 134
Mapping 802.1p Priority 135
Configuring Port Security 136
Port Security Administration 136
Port Security Interface Configuration 137
VLAN MAC Locking 138
Port Security Statically Configured MAC Addresses 139
Port Security Dynamically Learned MAC Addresses 140
Managing LLDP 141
Global Configuration 141
LLDP Interface Configuration 142
Local Devices 145
Remote Devices 146
Statistics 147
LLDP-MED 149
LLDP-MED Global Configuration 149
LLDP-MED Interface Configuration 150
LLDP Local Device Information 151
LLDP-MED Remote Device Information 152
Loop Protection 154
Loop Protection Configuration 154
Section 5: Managing Device Security 156
Port Access Control 157
Global Port Access Control Configuration 158
Port Access Control Port Summary 159
Port Configuration 161
Port Details 163
Statistics 166

Client Summary 168
Privileges Summary 169
History Log Summary 170
RADIUS Settings 171
RADIUS Configuration 171
Named Server Status 172
Server Statistics 173
Named Accounting Server Status 175
Accounting Statistics 176
Clear Statistics 177
Section 6: Configuring Quality of Service 178
Configuring Access Control Lists 179
IP Access Control Lists 179
IP ACL Configuration 180
Access Control List Configuration 181
Access Control List Interface Summary 190
Access Control List VLAN Summary 191
Access Control List Control Plane Configuration 192
Access Control List Statistics 193
Configuring Auto VoIP 195
Protocol Based Auto VoIP 195
Configuring Class of Service 197
IP DSCP Mapping Configuration 197
Interface Configuration 198
Interface Queue Configuration 199
Appendix A: Configuration Examples 201
Configuring VLANs 202
Using the Web Interface to Configure VLANs 203
Using the SNMP to Configure VLANs 204
Configuring Multiple Spanning Tree Protocol 205
Using the Web UI to Configure MSTP 206
Using SNMP to Configure MSTP 207
Configuring 802.1X Network Access Control 209
Using SNMP to configure 802.1X Port-Based Access Control 209

Section 1: Introduction

About This Document

OS2220 Websmart™ software provides rich Layer 2 and Quality of Service (QoS) functionality for switches operating in small office/home office networks. This guide describes how to configure SmartPATH software features by using the Web-based graphical user interface (GUI).

The information in this guide is intended for any of the following individuals:

- System administrators who are responsible for configuring and operating a network using OS2220 Websmart software
- Software engineers who are integrating OS2220 Websmart software into a 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.

Document Organization

This guide contains the following sections:

- Section 2: “Getting Started,” on page 10 contains information about performing the initial system configuration and accessing the user interfaces.
- Section 3: “Configuring System Information,” on page 18 describes how to configure administrative features such as SNMP, system users, and port information.
- Section 4: “Configuring Switching Information,” on page 93 describes how to manage and monitor the layer 2 switching features.
- Section 5: “Managing Device Security,” on page 156 contains information about configuring switch security information such as port access control and RADIUS server settings.
- Section 6: “Configuring Quality of Service,” on page 178 describes how to manage the OS2220 Websmart software ACLs, and how to configure the Class of Service features.
- Appendix A: “Configuration Examples,” on page 201 describe how to configure selected features on the switch by using either the Web interface and/or Simple Network Management Protocol (SNMP).

References

The references in this section may be used in conjunction with this document and can be found on the Service & Support website.

Document (or Item) Name
[1] WebSmart Release Notes

About OS2220 Websmart Software Modules

The OS2220 Websmart software suite includes the following modules:

- Switching (Layer 2)
- Quality of Service
- Management (Web UI and SNMP)

Not all modules are available for all platforms or software releases. The OS2220 Websmart modules can be applied in various combinations to develop advanced Layer 2/3/4+ products. The user-configurable features available on your switch depend on the installed modules.

Note: Not all features supported by all Websmart packages are available on all platforms to which Websmart software has been ported. References to the following features may be found in this guide but they are not currently supported in this release:

- HTTPS
- IPv6
- SNMPv3

Section 2: Getting Started

This section describes how to start the switch and access the user interface. It contains the following sections:

- Connecting the Switch to the Network
- Understanding the User Interfaces

Connecting the Switch to the Network

To enable remote management of the switch through a Web browser or SNMP, the switch must be connected to the network. The switch is preconfigured with an IP address for management purposes. The switch can also be configured to acquire its address from a DHCP server on the network.

Using the Default Management IP Address

By default, the switch is assigned the following static IP information for access to the SmartPATH software:

- IP address: 192.168.1.3
- Network mask: 255.255.255.0

1. Connect the switch to the management PC or to the network using any of the available network ports.
2. Power on the switch.
3. Set the IP address of the management PC's network adapter to be in the same subnet as the switch.

   Example: Set it to IP address 192.168.1.4, mask 255.255.255.0.
4. Enter the IP address shown above in the Web browser. See "Using the Web Interface" on page 12 for browser requirements.

Thereafter, use the Web interface to configure a different IP address or configure the switch as a DHCP client so that it receives a dynamically assigned IP address from the network. See "IPv4 Network Connectivity Configuration" on page 28 for instructions.

Understanding the User Interfaces

OS2220 Websmart software includes a set of comprehensive management functions for configuring and monitoring the system by using one of the following methods:

- Web User Interface
- Simple Network Management Protocol (SNMP)

Each of the standards-based management methods allows you to configure and monitor the components of the OS2220 Websmart software. The method you use to manage the system depends on your network size and requirements, and on your preference.

This guide describes how to use the Web-based interface to manage and monitor the system.

Note: The Web configuration and monitoring pages available for each platform depend on the OS2220 Websmart software version and modules installed. For more information about the modules, see “Getting Started” on page 10.

Using the Web Interface

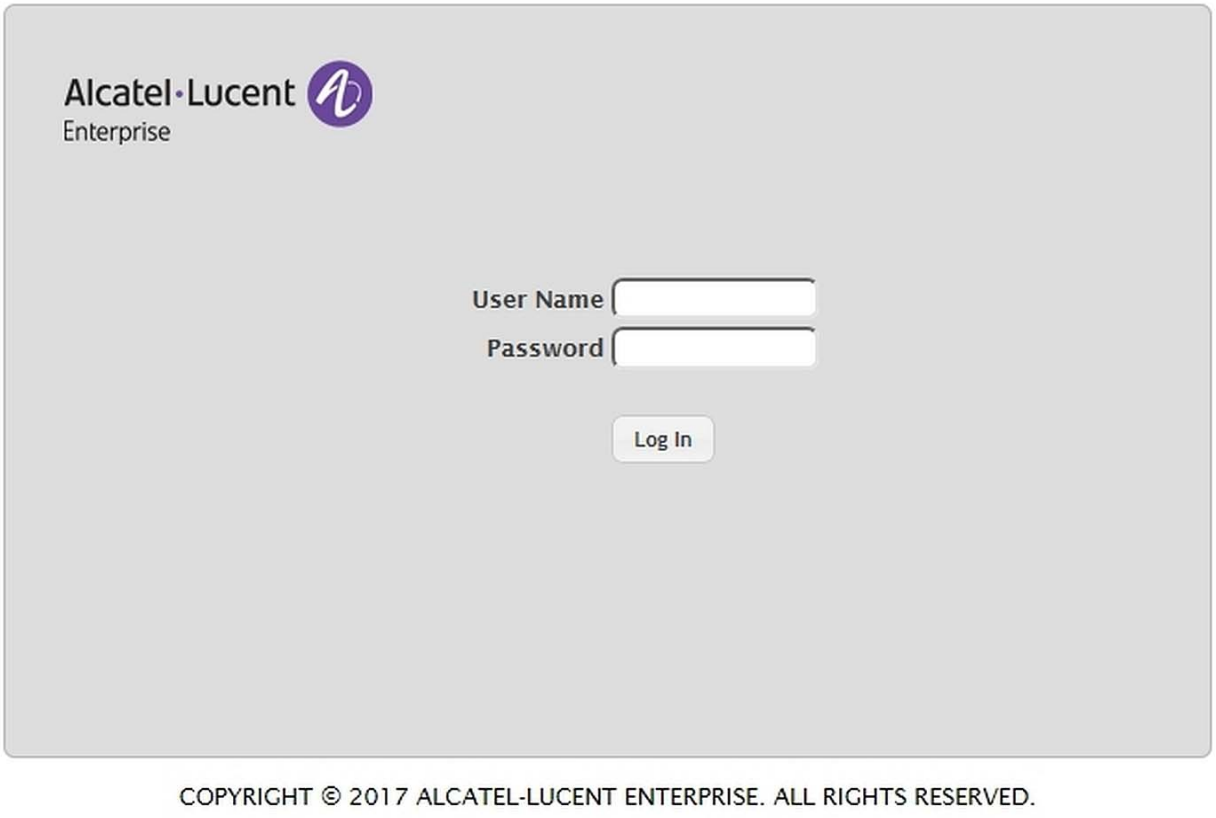
To access the switch by using a Web browser, the browser must meet the following software requirements:

- 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.
2. Type the user name and password into the fields on the login screen, and then click **Login**.

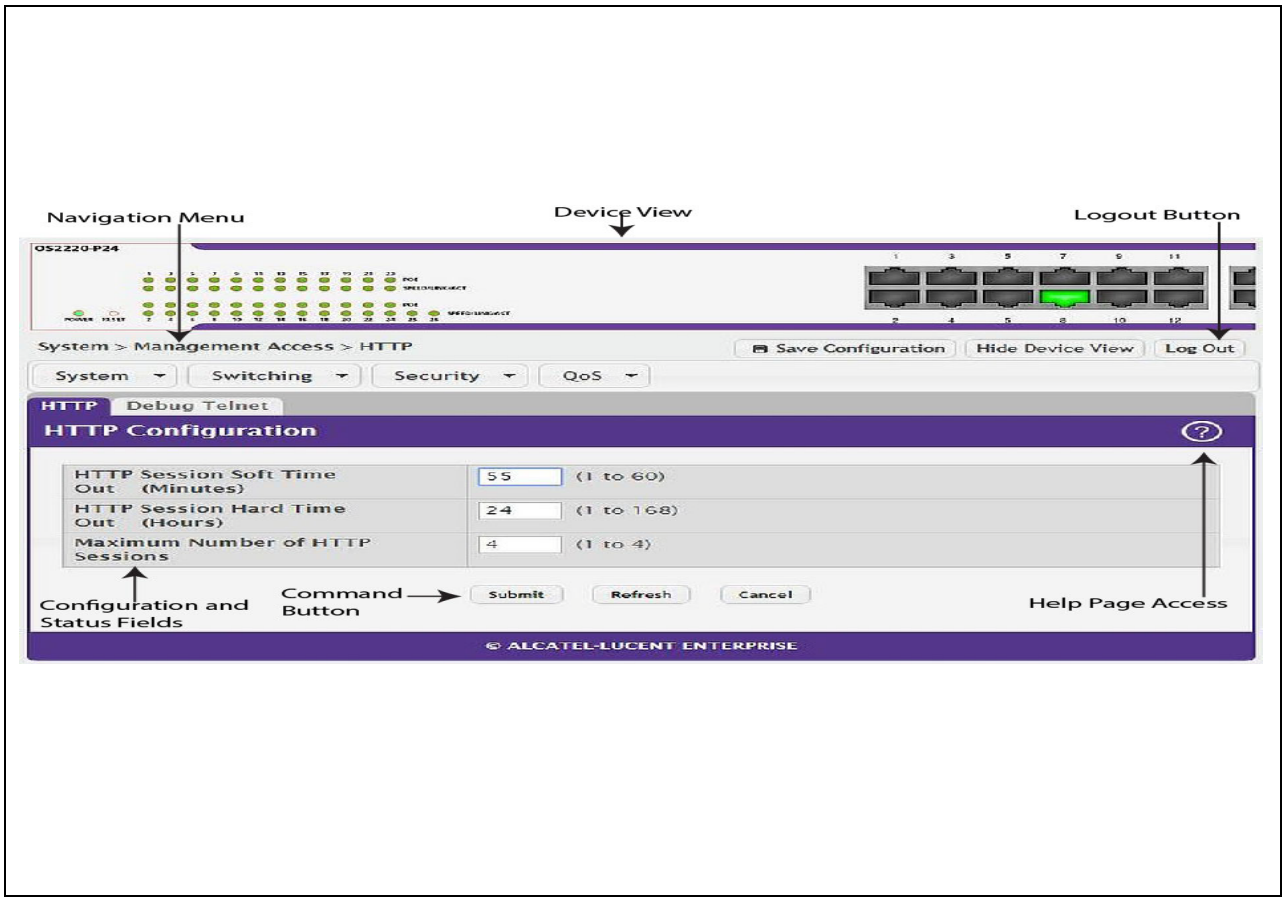
   The user name and password are the same as those you use to log on to the command-line interface. By default, the user name is **admin**, and there is no password. Passwords are case sensitive.



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

Figure 1 shows the layout of the OS2220 Websmart 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



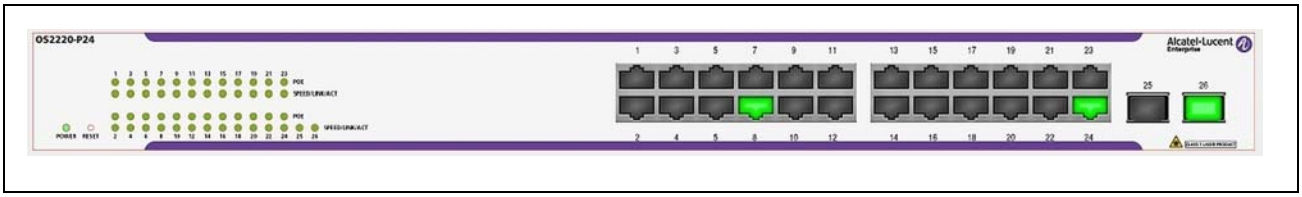
Device View

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 shows the Device View.

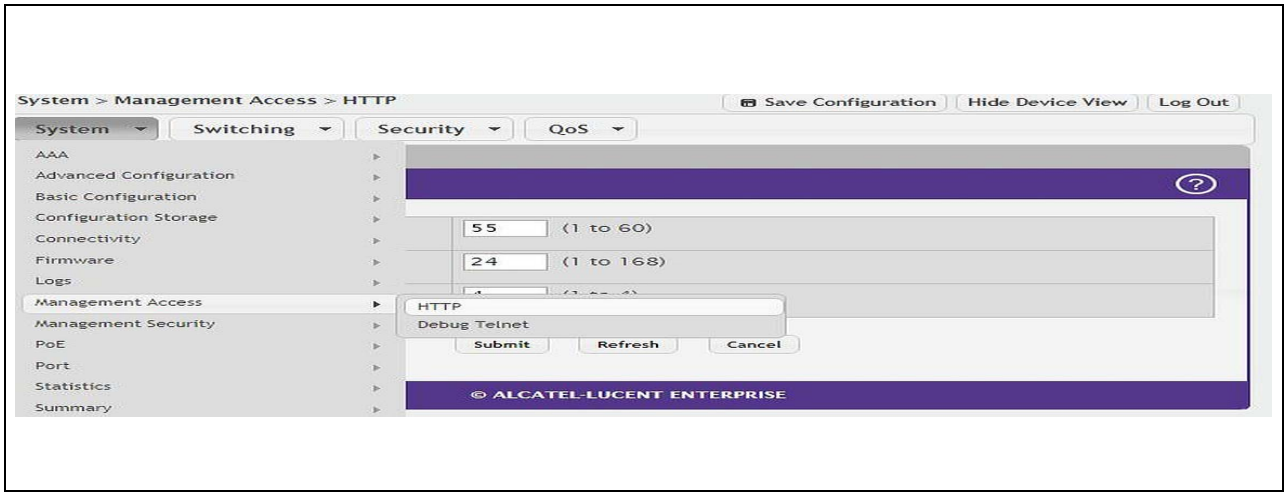
Figure 2: Device View



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

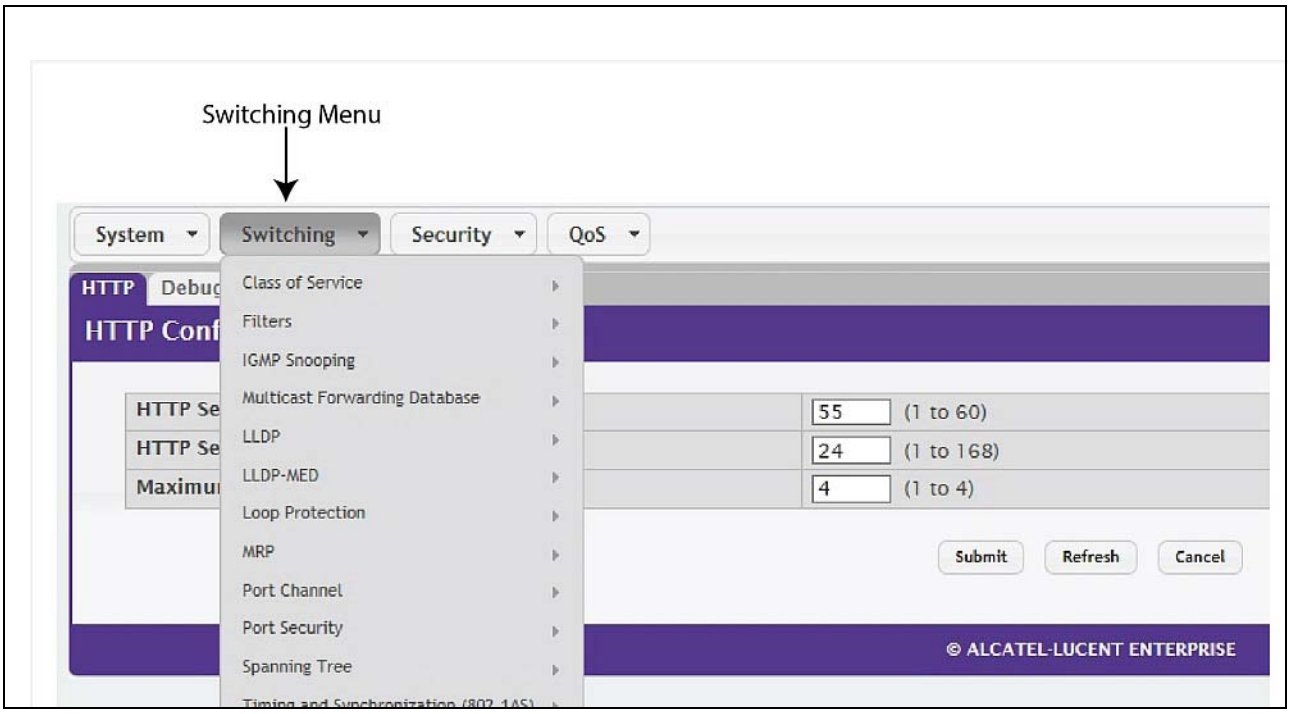


Navigation Menu

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

Table 1: 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 **System > System Utilities > Save All Applied Changes** page and click **Save**.
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.
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 on page 13 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 SNMP

For OS2220 Websmart software that includes the SNMP module, you can configure SNMP groups and users that can manage traps that the SNMP agent generates.

OS2220 Websmart uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. All private MIBs begin with a “-” prefix. The main object for interface configuration is in -SWITCHING-MIB, which is a private MIB. 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, displays the information you need to configure an SNMP manager to access the switch.

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

Section 3: Configuring System Information

Use the features in the System feature menu to define the switch's relationship to its environment. The **System** folder contains links to the following features:

- Viewing the Dashboard
- Viewing Inventory Information
- Viewing the System Firmware Status
- Defining General Device Information
- Configuring and Searching the Forwarding Database
- Managing Logs
- Viewing Device Port Information
- Defining SNMP Parameters
- Viewing System Statistics
- Using System Utilities
- Configuring Time Ranges
- Configuring SNTP Settings

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

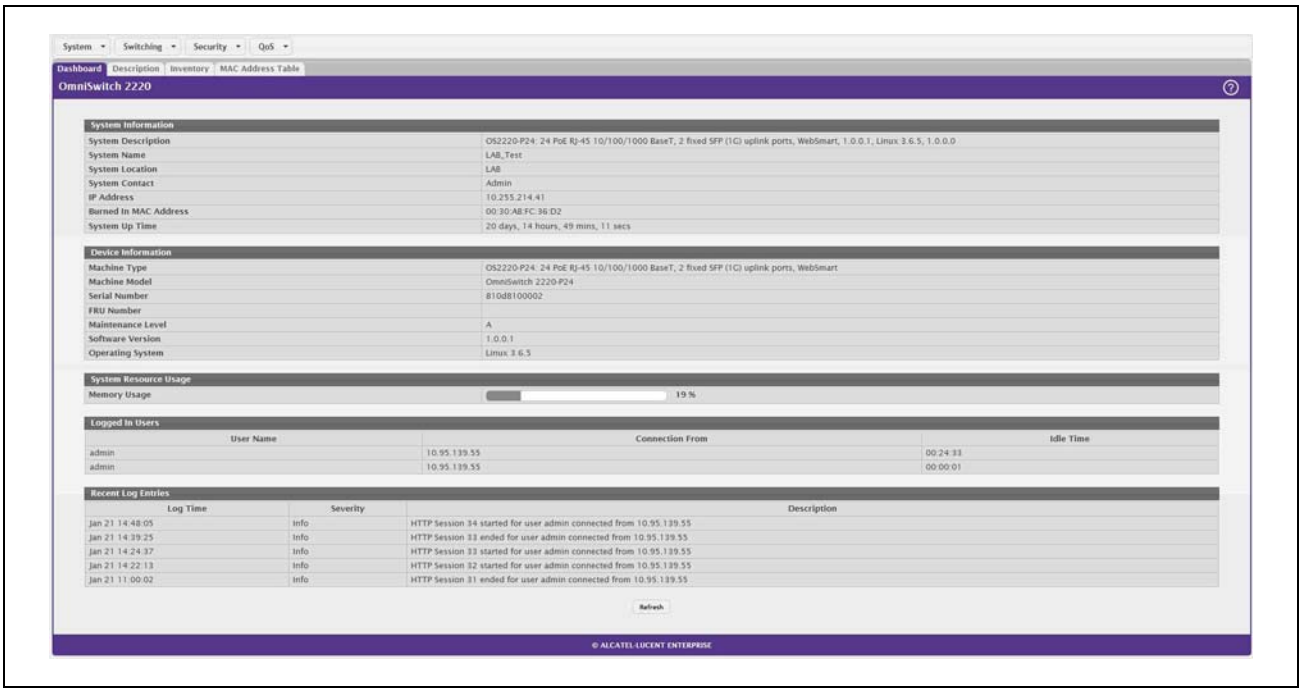


Table 2: Dashboard Fields

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.
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.

Table 2: Dashboard Fields (Cont.)

Field	*Description*
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	
Memory Usage	The percentage of total available system memory (RAM) 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 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 7: Inventory Information

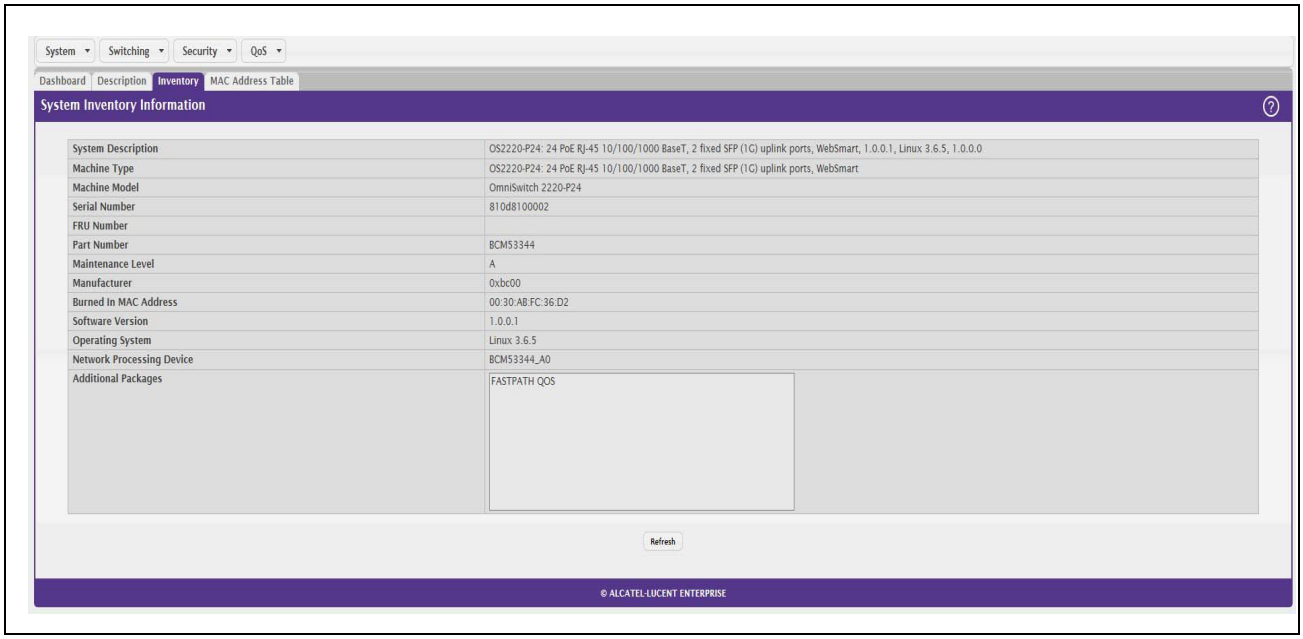


Table 3: Inventory Information Fields

Field	*Description*
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.
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 “1.2.4.”
Operating System	The operating system currently running on the switch.

Table 3: Inventory Information Fields (Cont.)

Field	Description
Network Processing Device	Identifies the network processor hardware.
Additional Packages	A list of the optional software packages installed on the switch, if any.

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 OS2220 Websmart 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 8: Dual Image Status

Table 4: 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 73.

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 as the backup image.

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

Figure 9: Dual Image Configuration and Upgrade

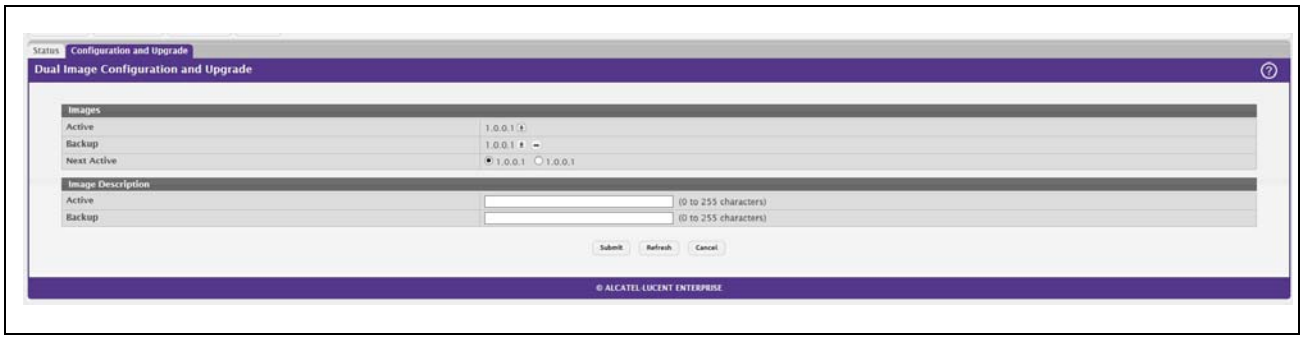


Table 5: Dual Image Status Fields

Field	*Description*
Unit	Use this field to select the unit with the code image to activate, upgrade, delete, or describe.
Active	The active code file version. Use the icons to the right of the field to perform the file transfer. • To transfer a new code image to the device, click the **File Transfer** icon. The **Firmware Upgrade** window opens. Click **Choose File** to browse to the file to transfer. After you select the appropriate file, click **Begin Transfer** to launch the HTTP transfer process. The active image is overwritten by the file that you transfer.
Backup	The backup code file version. Use the icons to the right of the field to perform the following tasks: • To transfer a new code image to the device, click the **File Transfer** icon. The **Firmware Upgrade** window opens. Click **Choose File** to browse to the file to transfer. After you select the appropriate file, click **Begin Transfer** to launch the HTTP transfer process. If a backup image already exists on the device, it is overwritten by the file that you transfer. • To delete the backup image from permanent storage, click the **–** (minus) icon. You must confirm the action before the image is deleted.
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.

Table 5: Dual Image Status Fields

Field	*Description*
Backup Description	Use this field to specify a description to associate with the image that is currently the backup code file.
Select File	These three are all described in Help but I don't see them in the UI 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.
Digital Signature Verification	When this option is checked, the file download will be verified with the digital signature.
Status	Provides information about the status of the file transfer.

Defining General Device Information

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

- "System Description" on page 26
- "Switch Configuration" on page 27
- "IPv4 Network Connectivity Configuration" on page 28
- "HTTP Configuration" on page 29
- "Debug Telnet Server" on page 30
- "User Accounts" on page 32
- "User Domain Name" on page 33
- "Select Authentication List" on page 35
- "Denial of Service" on page 36

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 10: System Description

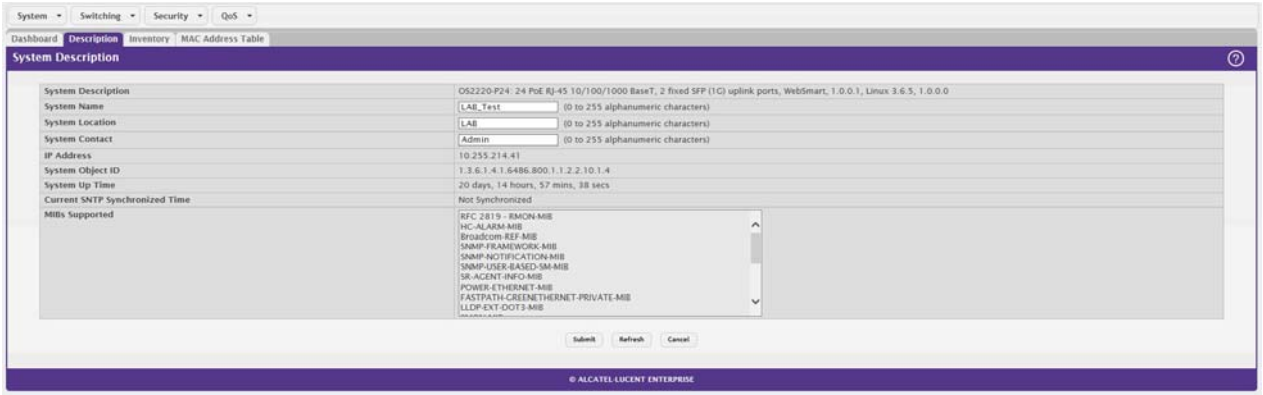


Table 6: System Description Fields

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 “IPv4 Network Connectivity Configuration” on page 28.
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 “Not Synchronized.” To specify an SNTP server, see “Configuring SNTP Settings” on page 83.
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

IEEE 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss. When 802.3x flow control is enabled, lower speed switches can communicate with higher speed switches by requesting that the higher speed switch refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

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

Figure 11: Switch 802.3x Flow Control

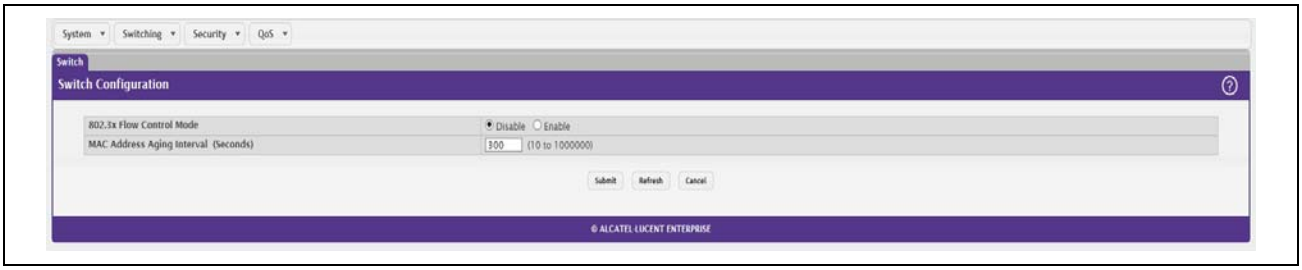


Table 7: Switch Configuration Fields

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: • **Disabled** – The switch does not send PAUSE frames if the port buffers become full. • **Enabled** – The switch can send PAUSE frames to a peer device if the port buffers become full.
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.

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 12: Network Connectivity Configuration for IPv4

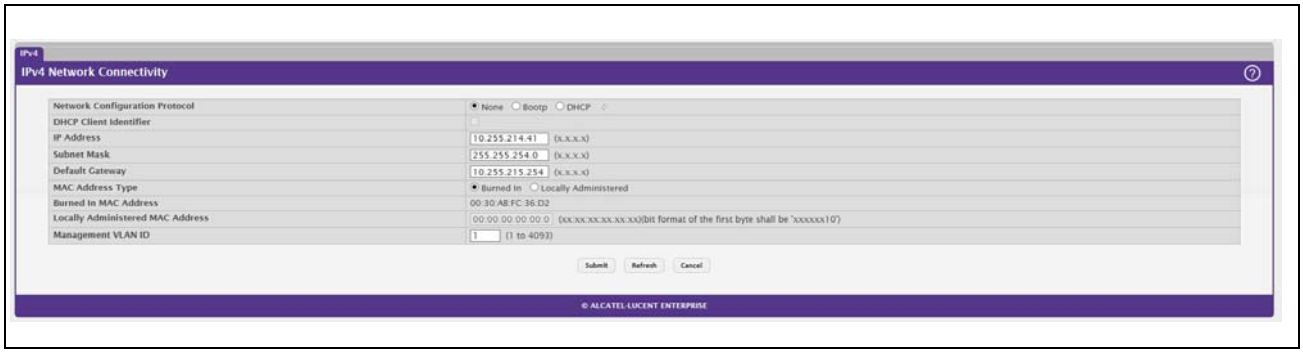


Table 8: Network Connectivity Configuration for IPv4 Fields

Field	*Description*
Network Configuration Protocol	Specify what the switch should do following power-up. The factory default is None. The options are as follows: • **None:** Do not send any requests following power-up. • **Bootp:** Transmit a Bootp request. • **DHCP:** Transmit a DHCP request.
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 ***Note:*** 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

Table 8: Network Connectivity Configuration for IPv4 Fields (Cont.)

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.
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.

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 13: HTTP Configuration

Table 9: HTTP Configuration Fields

Field	Description
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.

Table 9: HTTP Configuration Fields (Cont.)

Field	*Description*
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.

Debug Telnet Server

Incorrect configurations to the network parameters can make the switch inaccessible through the Web or SNMP management interfaces. The switch recovery mode feature provides the ability to fix the incorrect network configuration information. The feature provides ability to restart the Web interface gracefully by freeing the resources held by the UI. Additionally, the feature provides the ability to restore the Burned in MAC address (which is vital for normal operation of switch) from Recovery Mode.

On switches with the switch recovery feature, a telnet server is active (even in normal operational state) on port number: 65530. You can log in to the telnet server by using the same username and password that you use to log in to the Web interface. On successful login, you can access the switch recovery mode.

In recovery mode, use the command-line interface (CLI) to perform the following tasks:

- View or configure switch network IP configuration information
- View or configure the burned in MAC address of the switch
- Initiate a UI restart
- Delete configuration files

Use the Debug Telnet Server page to control the administrative mode of the Telnet server and to view the active TCP port number for the server.

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

Figure 14: Debug Telnet Server

Table 10: Debug Telnet Server Fields

Field	*Description*
Admin Mode	Specifies the Admin mode of the Debug Telnet Server. Default value is Enable. Disabling the Admin mode leads to the debug Telnet connection inaccessible.
Port	Displays the port number on which debug telnet server is active.

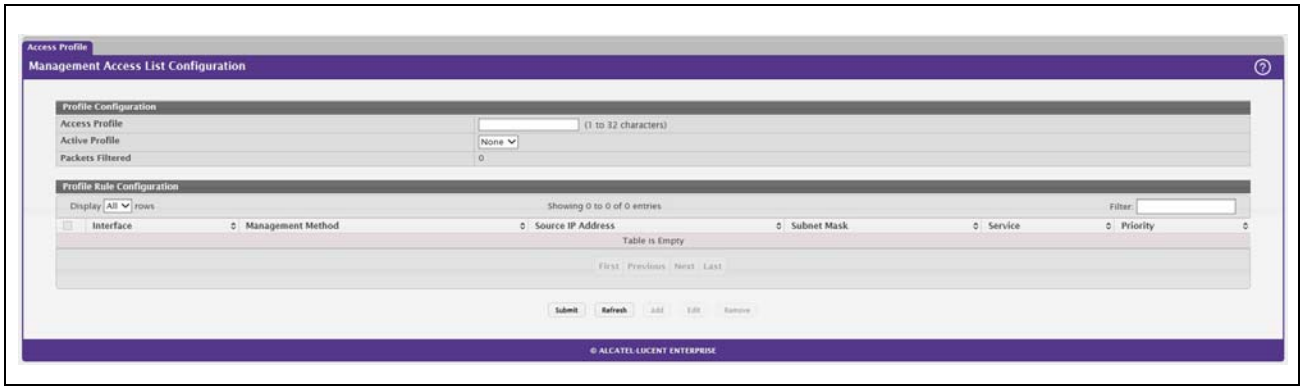
Management Access Control and Administration List

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 15: 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 11: 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.
Interface	The port/interface or trunk ID.
Management Method	The types of action will be taken on access control list. • Permit: To allow conditions for the management access list. • Deny: To deny conditions for the management access list. 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: • ANY • TELNET • HTTP • HTTPS • SNMP • SSH • TFTP • SNTP
Priority	Priority for the rule. Duplicates are not allowed.

User Accounts

By default, the switch contains only an admin user account. The admin user has Read/Write previleges and cannot be deleted.

- There is no option to create or delete a new user or users. Only options are for password / confirm password.
- Access level is fixed. This cannot be modified.
- There is no option for encrypted password.

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

Figure 16: User Accounts

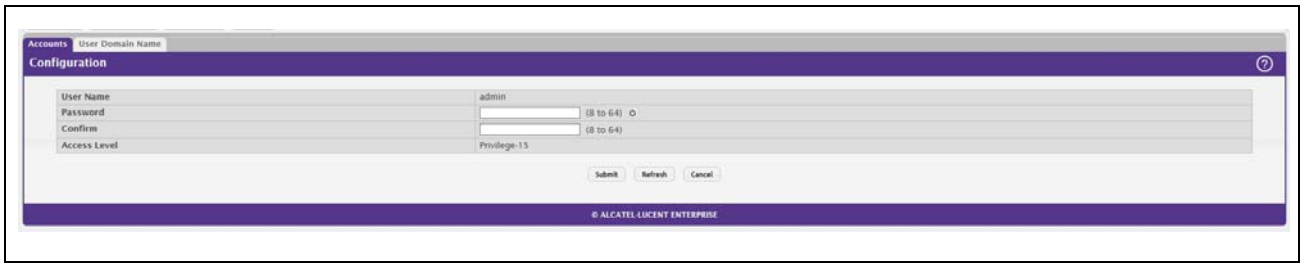


Table 12: User Accounts Fields

Field	*Description*
User Name	The preconfigured user name is *admin*.
Password	The password assigned to the admin user. To reset the password to the default value, click the **Reset** icon to the right of the field. Passwords must be greater than eight characters 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	By default, Access level is fixed and cannot be modified.

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.

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

Figure 17: User Domain Name

Table 13: 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.

Table 13: User Domain Name Fields (Cont.)

Field	*Description*
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.

Select Authentication List

Use the Select Authentication List Configuration page to associate an authentication list with different access methods (HTTP, DOT1x, etc).

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

Figure 18: Select Authentication List

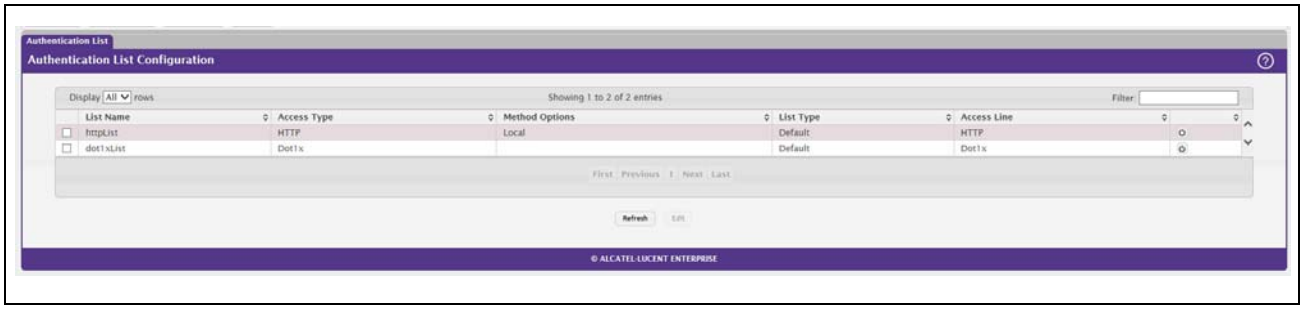


Table 14 describes the fields for the Select Authentication List page.

Table 14: Select Authentication List 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: • **HTTP** – Management-level access to the web-based user interface by using HTTP. • **Dot1x** – Port-based access to the network through a switch port that is controlled by IEEE 802.1X.
Method Options	The method(s) used to authenticate a user who attempts to access the management interface or network. The possible methods are as follows: • **Enable** – Uses the locally configured Enable password to verify the user's credentials. • **Line** – Uses the locally configured Line password to verify the user's credentials. • **Local** – Uses the ID and password in the Local User database to verify the user's credentials. • **RADIUS** – Sends the user's ID and password to the configured RADIUS server to verify the user's credentials. • **None** – No authentication is used. • **IAS** – Uses the local Internal Authentication Server (IAS) database for 802.1X port-based authentication.

Table 14: Select Authentication List Fields (Cont.)

Field	*Description*
List Type	The type of list, which is one of the following: • **Default** – The list is preconfigured on the system. This type of list cannot be deleted, and only the Method Options are configurable. • **Configured** – The list has been added by a user.
Access Line	The access method(s) that use the list for authentication. The settings for this field are configured on the Authentication Selection page.

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.

Denial of Service

Use the Denial of Service (DoS) page to configure DoS control. OS2220 Websmart 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 then 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.
- **SMAC=DMAC:** Source MAC address=Destination MAC address.
- **TCP Por**t: 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 19: Denial of Service

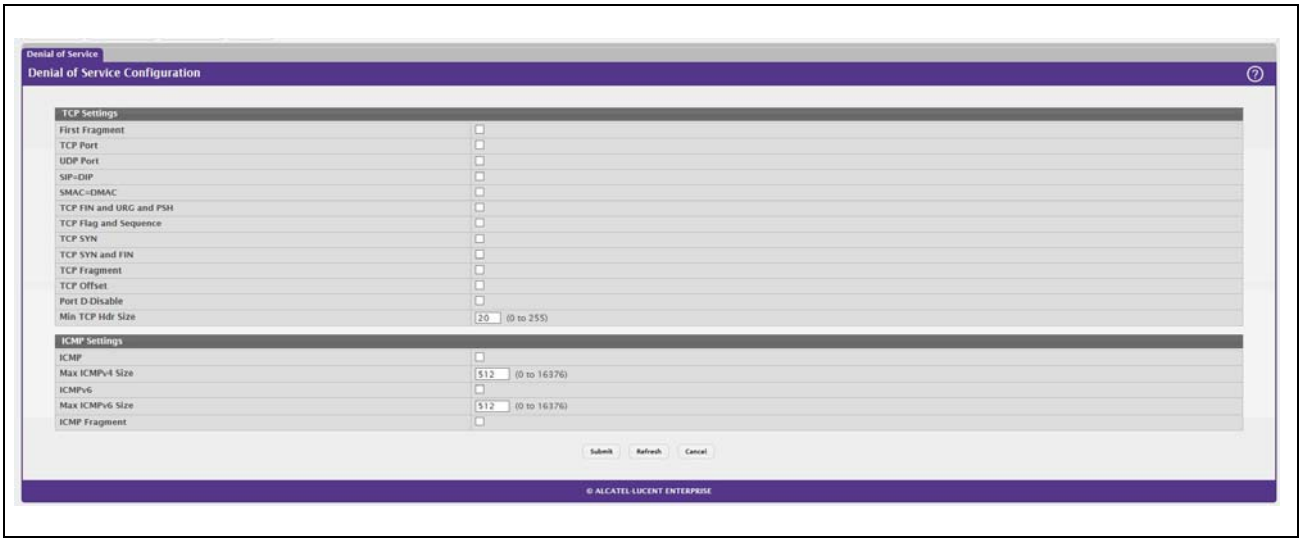


Table 15: Denial of Service Configuration Fields

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.
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.

Table 15: Denial of Service Configuration Fields (Cont.)

Field	*Description*
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 then this configured maximum ICMPv4 packet size.
ICMPv6	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 ICMPv6 Size field.
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.

Configuring and Searching the Forwarding Database

The forwarding database maintains a list of MAC addresses after having received a packet from this MAC address. The transparent bridging function uses the forwarding database entries to determine how to forward a received frame.

Switch Configuration

Use the Switch Configuration page to set the amount of time to keep a learned MAC address entry in the forwarding database. The forwarding database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time.

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

Figure 20: Switch Configuration

Table 16: Switch Configuration Fields

Field	*Description*
802.3x Flow Control Mode	Enable or disable 802.3x flow control on the switch. IEEE 802.3x flow control works by pausing a port when the port becomes oversubscribed. It also allows a port to drop all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss. When enabled, flow control allows lower speed switches to communicate with higher-speed switches by requesting that the higher-speed switch refrain from sending packets. Transmissions are temporarily halted to prevent buffer overflows.
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.

Note: IEEE 802.1D recommends a default of 300 seconds, which is the factory default.

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

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.

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 21: Log Configuration

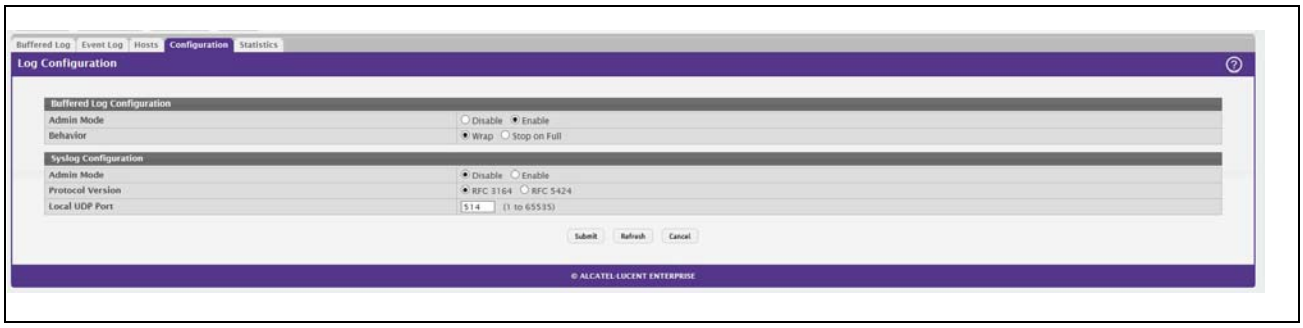


Table 17: Log Configuration Fields

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).
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.
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 22: Buffered Log

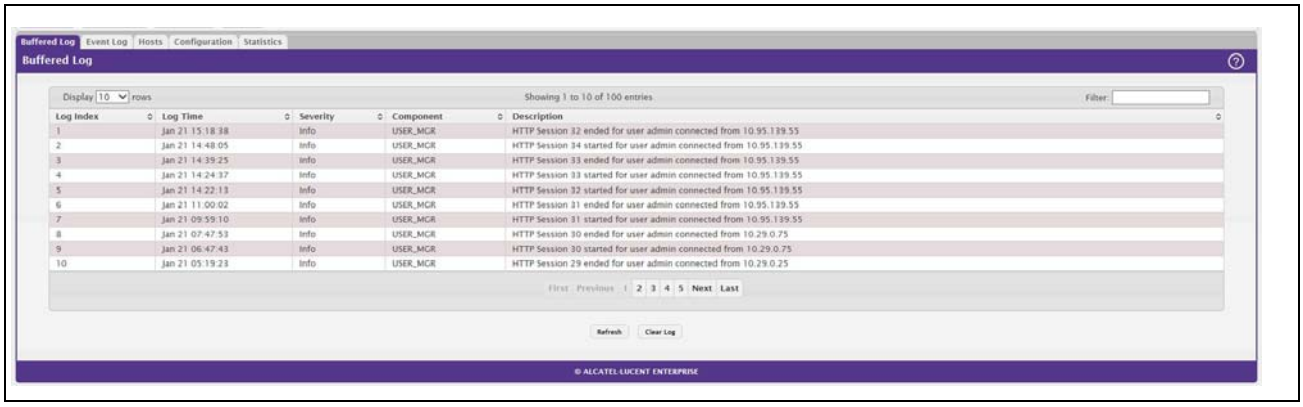


Table 18: Buffered Log Fields

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: • **Emergency (0)**: The device is unusable. • **Alert (1)**: Action must be taken immediately. • **Critical (2)**: The device is experiencing primary system failures. • **Error (3)**: The device is experiencing non-urgent failures. • **Warning (4)**: The device is experiencing conditions that could lead to system errors if no action is taken. • **Notice (5)**: The device is experiencing normal but significant conditions. • **Info (6)**: The device is providing non-critical information. • **Debug (7)**: The device is providing debug-level information.
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 23: Event Log

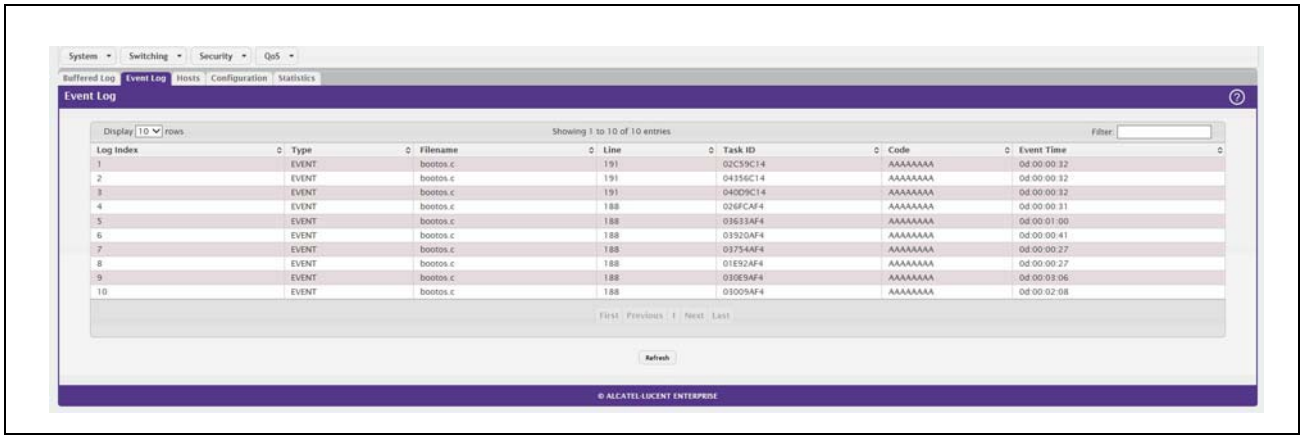


Table 19: Event Log Fields

Field	*Description*
Entry	The number of the entry within the event log. The most recent entry is first.
Type	The incident category that indicates the cause of the log entry: EVENT, ERROR, etc.
Filename	The OS2220 Websmart source code filename identifying the code that detected the event.
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.
Code	The event code passed to the event log handler by the code reporting the event.
Time	The time the event occurred, measured from the previous reset.

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 24 shows the Logging Hosts page.

Figure 24: Logging Hosts

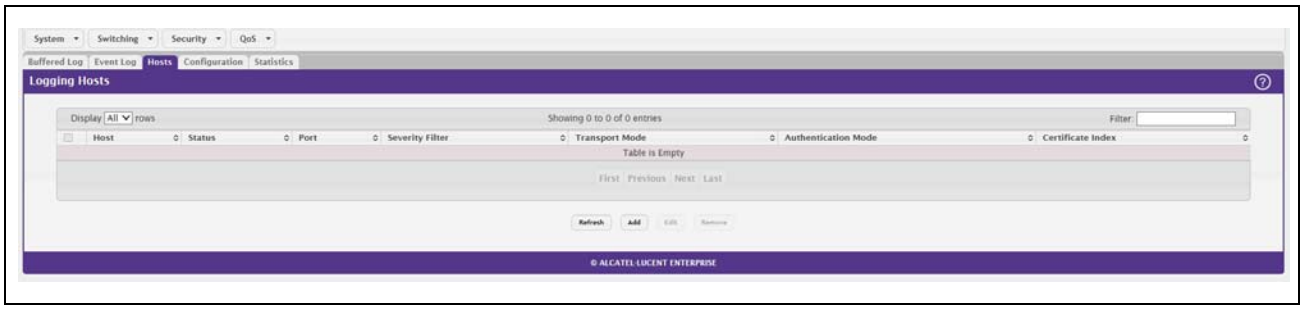


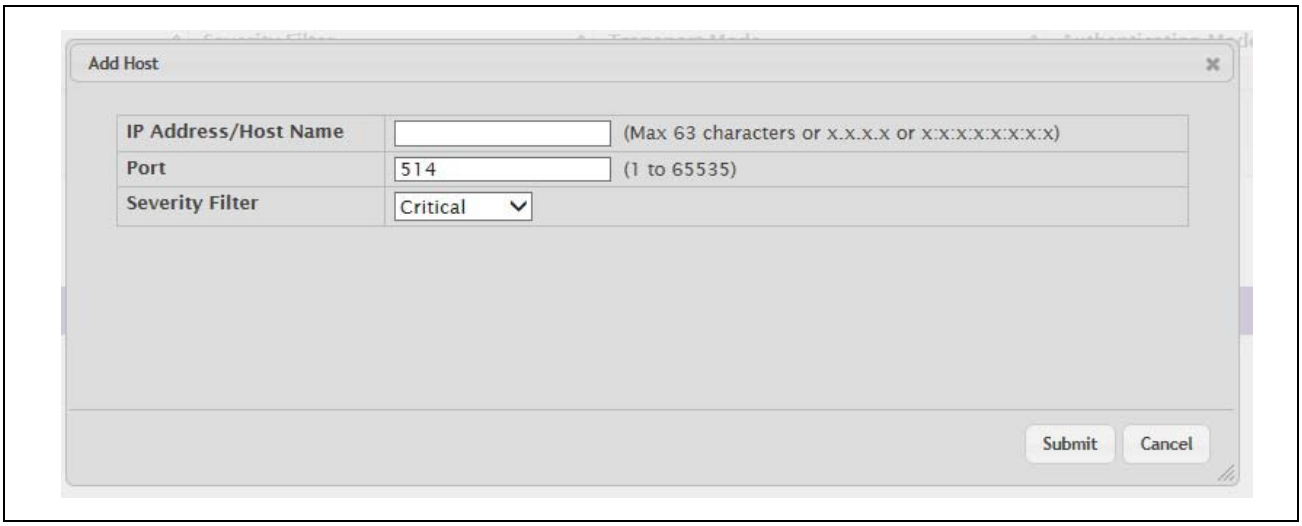
Table 20: Logging Hosts Fields

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 25: Add Host



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

Table 21: 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.
Transport Mode	Transport mode used while sending messages to syslog servers. Supported modes are UDP and TLS. If TLS is not configured then 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.
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**.

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 26: PoE Configuration

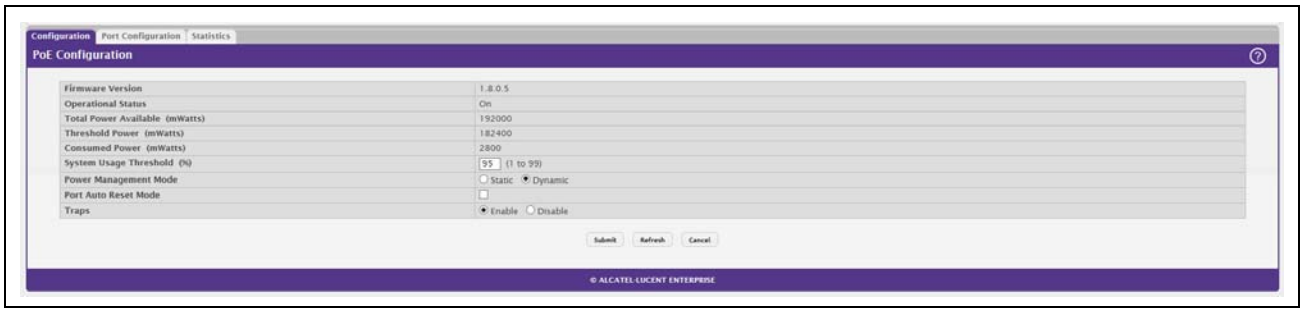


Table 22: PoE Configuration Fields

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: • **On** – At least one port on the switch is delivering power to a connected device. • **Off** – The PoE functionality is operational but no ports are delivering power. • **Faulty** – The PoE functionality is not operational.
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 **System Usage Threshold** percent.
Consumed Power	The amount of power in mWatts currently being consumed by connected PoE devices.
System Usage Threshold	A percentage of the total power available. This percentage determines the **Threshold Power**.

Table 22: PoE Configuration Fields (Cont.)

Field	Description
Power Management Mode	The method by which the PoE controller determines supplied power, which can be one of the following: • **Static** – 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. • **Dynamic** – 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.
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 27: PoE Port Configuration

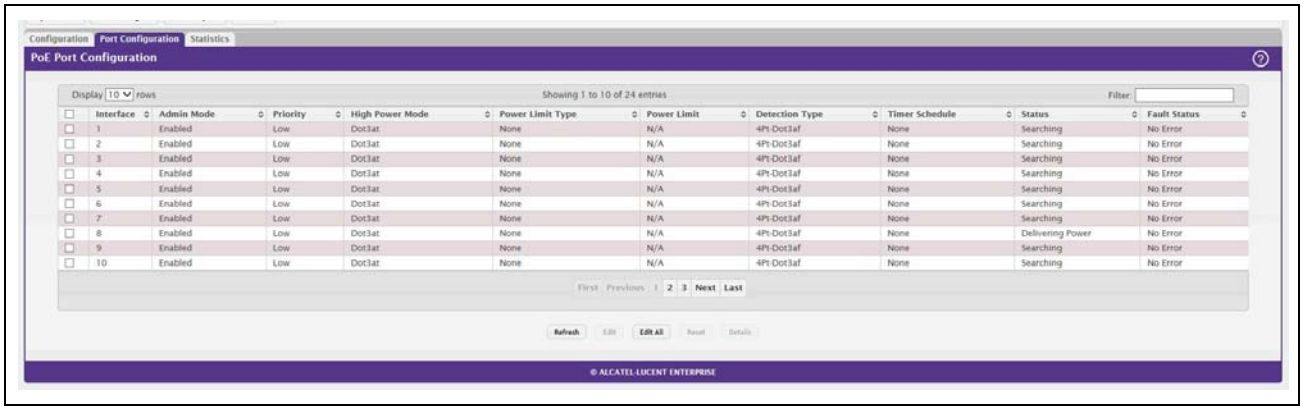


Table 23: PoE Port Configuration Fields

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.

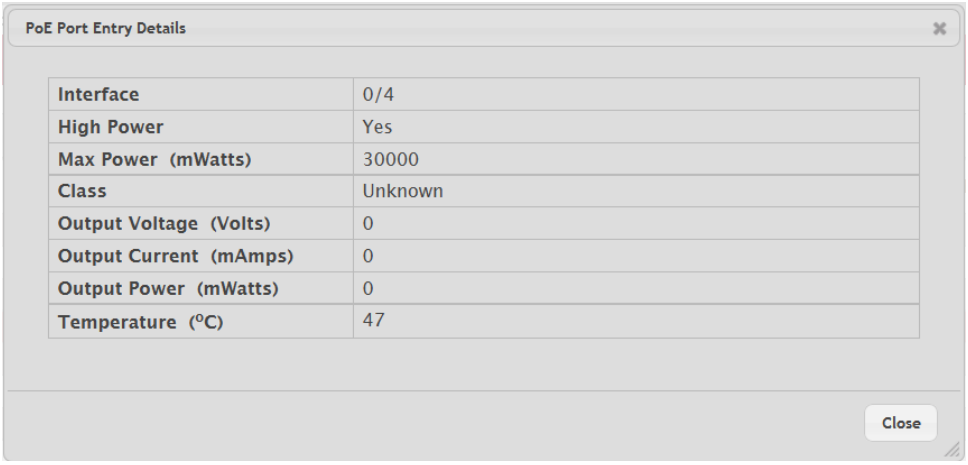
Table 23: PoE Port Configuration Fields (Cont.)

Field	*Description*
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 **Critical**, **High**, and **Low**.
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: • **Class** – 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. • **User** – The power limit is user defined, overriding the LLDP information. When set to **User**, the Power Limit field is enabled.
Power Limit	The power limit for the port, which can be specified. This field displays only when **Power Limit Type** is set to **User**.
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: • **Legacy** – The switch uses a legacy detection scheme not defined in 802.3af. • **4Pt-Dot3af** – The switch uses the 802.3af 4-point detection scheme only. • **4Pt-Dot3af + Legacy** – The switch uses the 802.3af 4-point detection scheme, followed by the legacy detection scheme. • **2Pt-Dot3af** – The switch uses the 802.3af 2-point detection scheme. • **2Pt-Dot3af + Legacy** – The switch uses the 802.3af 2-point detection scheme, followed by the legacy detection scheme. • **None** – No detection is performed.
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: • **Disabled** – The PSE is disabled. • **Delivering Power** – The PSE is delivering power. • **Fault** – The PSE has experienced a fault condition. • **Test** – The PSE is in test mode. • **Other Fault** – The PSE has experienced a variable error condition. • **Searching** – The PSE is transitioning between states. • **Requesting Power** – The PSE is currently not able to deliver power because power is unavailable to the port.

Table 23: PoE Port Configuration Fields (Cont.)

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

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



The following information describes the fields in the **Details** window.

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 28: PoE Port Statistics

Table 24: PoE Port StatisticsFields

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 29: Port Summary

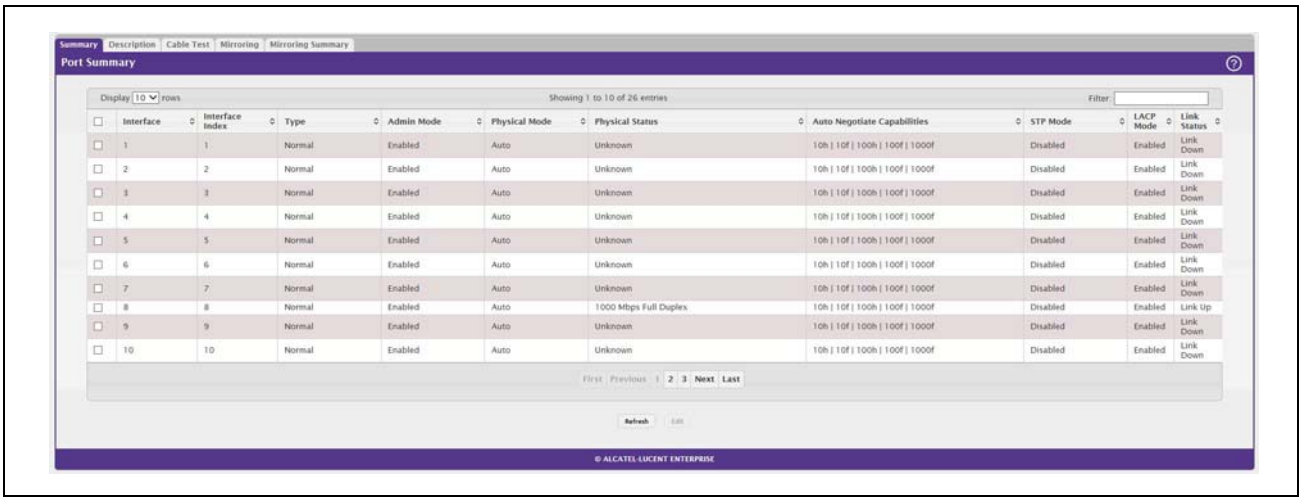


Table 25: Port Summary Fields

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.
Type	For most ports this field is blank. Otherwise, the possible values are: • **Normal -** The port is a normal port, which means it is not a LAG member or configured for port mirroring. • **Trunk Member** - The port is a member of a LAG. • **Mirrored -** 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 “Mirroring” on page 57. • **Probe -** 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 “Mirroring” on page 57.

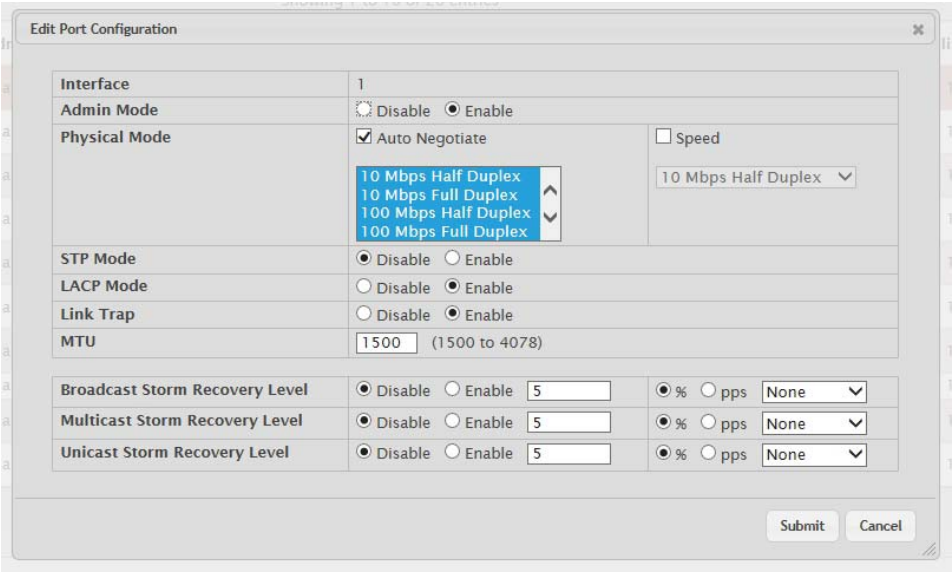
Table 25: Port Summary Fields (Cont.)

Field	*Description*
Admin Mode	Shows the port control administration state, which can be one of the following: • **Enabled:** The port can participate in the network (default). • **Disabled:** The port is administratively down and does not participate in the network.
Physical Mode	Shows the speed and duplex mode at which the port is configured: • **Auto:** 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 • **<Speed> Half Duplex:** The port speeds available from the menu depend on the platform on which the OS2220 Websmart 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. • **<Speed> Full Duplex:** The port speeds available from the menu depend on the platform on which the OS2220 Websmart 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. The physical mode for a LAG is reported as “LAG.”
Physical Status	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.
Auto Negotiate Capabilities	Indicates the list of configured capabilities for a port when Auto Negotiate is on. The Capability status for LAGs is not reported.
STP Mode	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: • **Enable** - Spanning tree is enabled for this port. • **Disable** - Spanning tree is disabled for this port.
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: • **Enable:** Specifies that the port is allowed to participate in a port channel (LAG), which is the default mode. • **Disable:** Specifies that the port cannot participate in a port channel (LAG). • **N/A**: For LAG ports.
Link Status	Indicates whether the Link is up or down.

Table 25: Port Summary Fields (Cont.)

Field	*Description*

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



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. • **Enable:** Specifies that the system sends a trap when the link status changes. • **Disable:** Specifies that the system does not send a trap when the link status changes.
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.
Broadcast Storm Recovery Mode	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. Specifies the broadcast storm recovery action to either Shutdown or Trap for specific interface. If configured to **Shutdown**, the interface which receives broadcast packets at a rate which is above threshold is diagnostically disabled. The **Trap** option sends trap messages at approximately every 30 seconds until broadcast storm control recovers.

Table 25: Port Summary Fields (Cont.)

Field	*Description*
Multicast Storm Recovery Level	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. Specifies the multicast storm recovery action to either Shutdown or Trap for specific interface. If configured to **Shutdown**, the interface which receives multicast packets at a rate which is above threshold is diagnostically disabled. The option **Trap** sends trap messages at approximately every 30 seconds until multicast storm control recovers.
Unicast Storm Recovery Level	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. Specifies the unicast storm recovery action to either Shutdown or Trap for specific interface. If configured to **Shutdown**, the interface which receives unicast packets at a rate which is above threshold is diagnostically disabled. The **Trap** option sends trap messages at approximately every 30 seconds until unicast storm control recovers.

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 30: Port Description

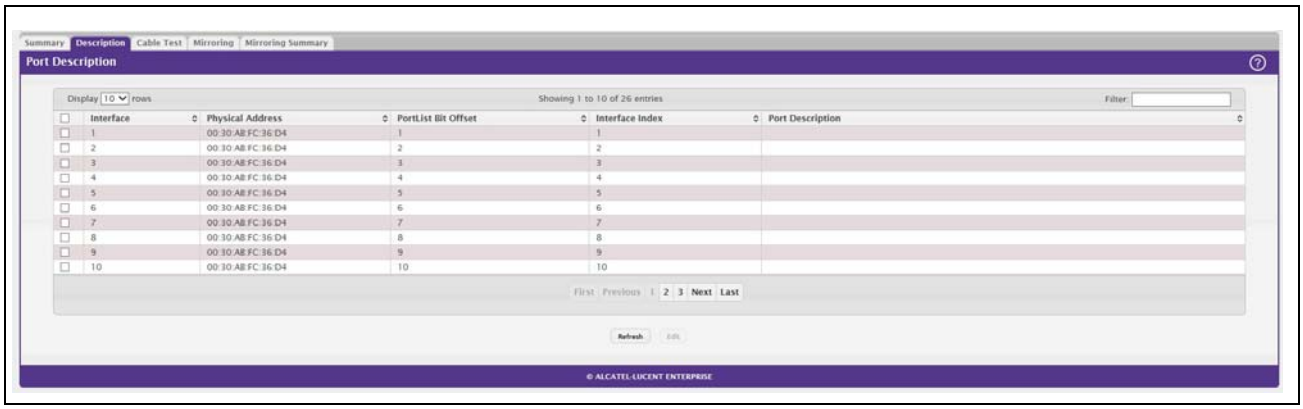


Table 26: Port Description Fields

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 **Submit**.
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 31: Cable Test

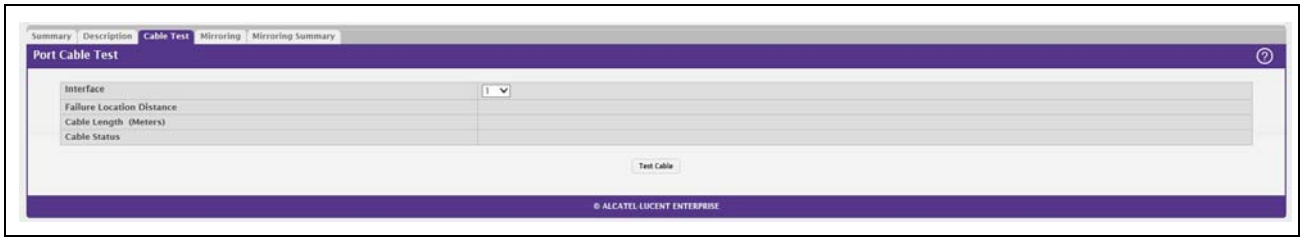


Table 27: Cable Test Fields

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. • **Normal**: The cable is working correctly. • **Open**: The cable is disconnected or there is a faulty connector. • **Open and Short**: There is an electrical short in the cable. • **Cable status Test Failed**: 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.
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. Note: 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. Note: 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 that 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

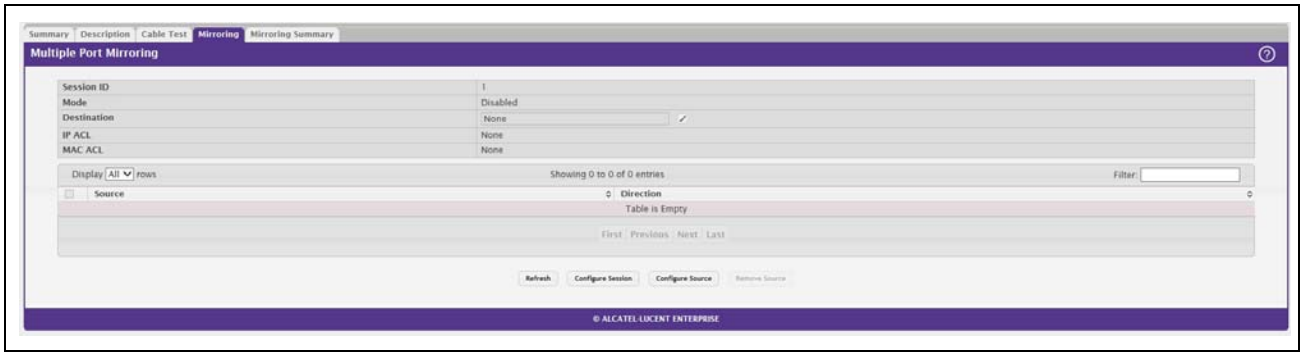
Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port. You have the ability to configure how traffic is mirrored on 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 32: Multiple Port Mirroring



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**.

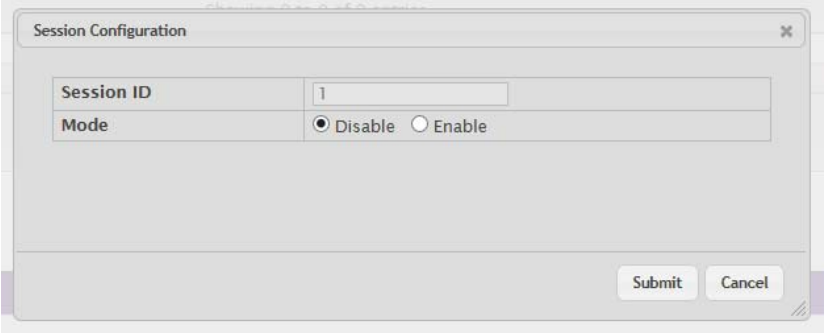
Table 28: Multiple Port Mirroring Fields

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: • **Remote VLAN** – 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. • **Interface** – 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. • **None** – The destination is not configured. ***Note:*** 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.
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: • **Tx and Rx** – Both ingress and egress traffic. • **Rx** – Ingress traffic only. • **Tx** – Egress traffic only.

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, click **Configure Session** to display the **Session Configuration** page.



2. Configure the following fields:

Table 29: Multiple Port Mirroring—Session Configuration

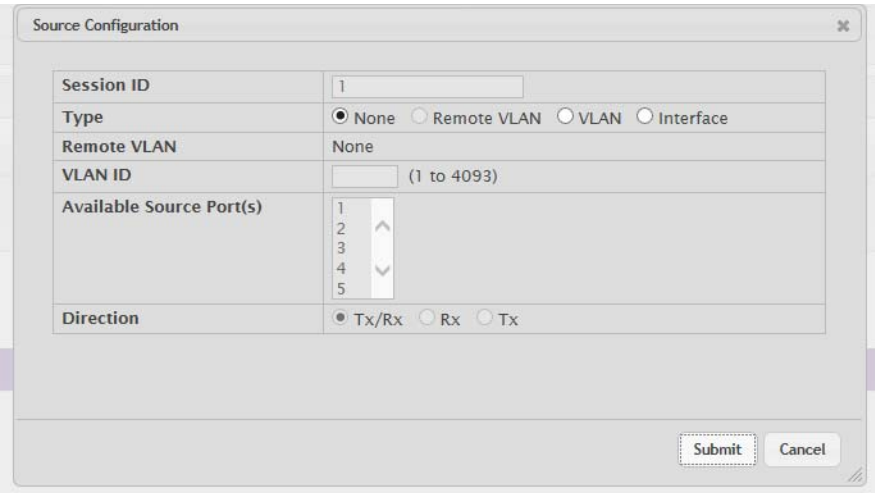
Field	*Description*
Session ID	The port mirroring session ID. The number of sessions allowed is platform specific.
Mode	The administrative mode for the selected port mirroring session. If the mode is disabled, the configured source is not mirroring traffic to the destination.

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 30: Multiple Port Mirroring—Source Configuration

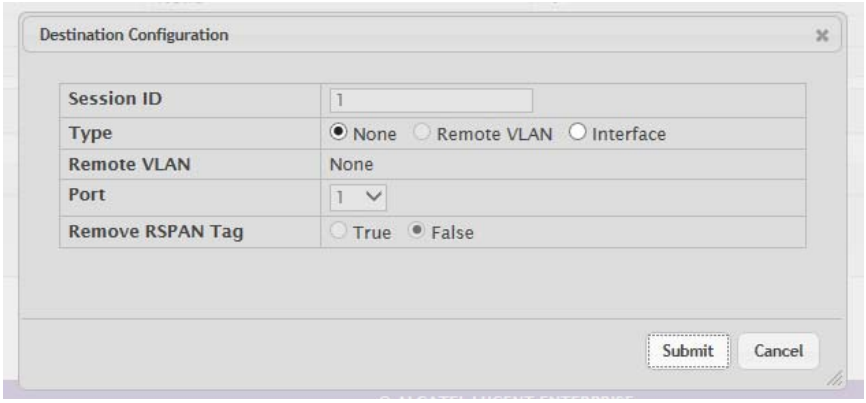
Field	*Description*
Session ID	The port mirroring session ID. The number of sessions allowed is platform specific.
Type	The type of interface to use as the source: • **None** – The source is not configured. • **Remote VLAN** – The VLAN configured as the RSPAN VLAN is the source. In an RSPAN configuration, the remote VLAN is the source on the destination device that has a physical port connected to the network traffic analyzer. • **VLAN** – 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. • **Interface** – Traffic is mirrored from one or more physical ports on the device.
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, CTRL + 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: **Tx and Rx** – Both ingress and egress traffic. **Rx** – Ingress traffic only. **Tx** – 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, click the **Edit** icon in the Destination field.



2. Configure the following fields:

Table 31: 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: • **None** – The destination is not configured. • **Remote VLAN** – 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. • **Interface** – 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.
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 33: Multiple Port Mirroring Summary

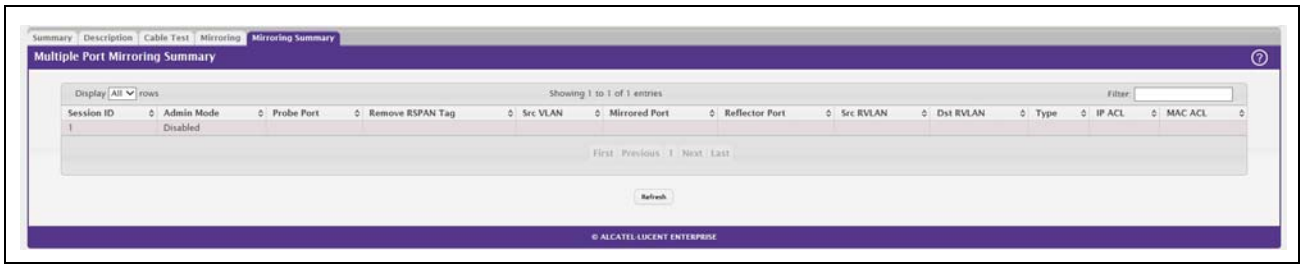


Table 32: Multiple Port Mirroring Summary Fields

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.
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.

Table 32: Multiple Port Mirroring Summary Fields (Cont.)

Field	Description
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: • **Tx and Rx** – Both ingress and egress traffic. • **Rx** – Ingress traffic only. • **Tx** – Egress traffic only.
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 34: Port Green Ethernet Statistics

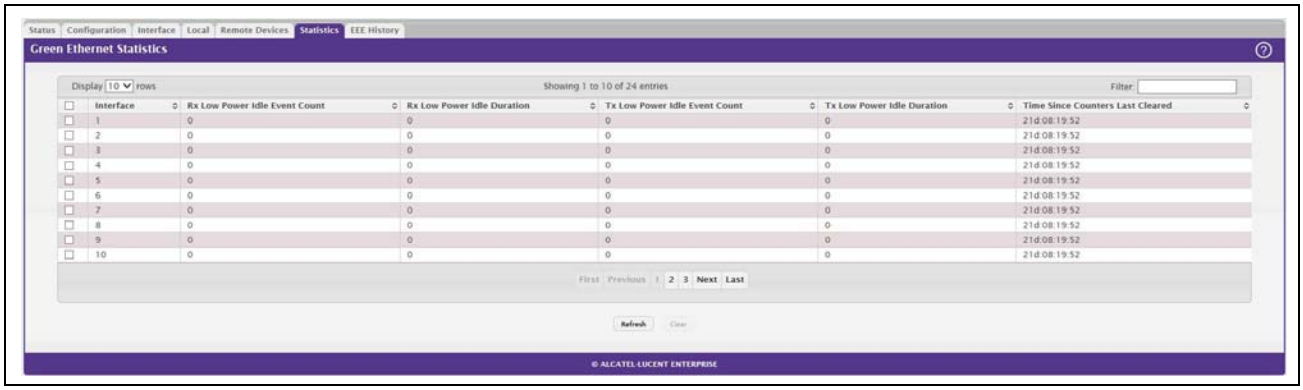


Table 33: Green Ethernet Statistics Fields

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.

Table 33: Green Ethernet Statistics Fields (Cont.)

Field	Description
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 35: Green Mode EEE History

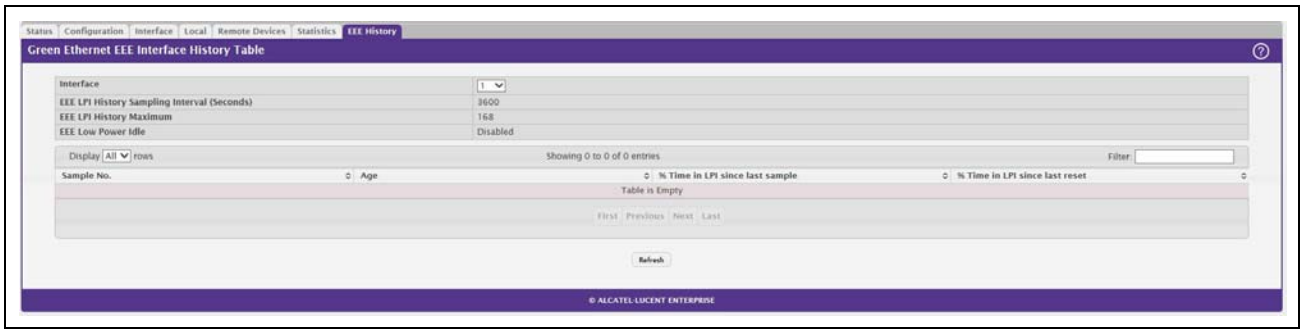


Table 34: Green Mode EEE History Fields

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

Table 34: Green Mode EEE History Fields (Cont.)

Field	Description
% 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.

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.

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-Bock-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.

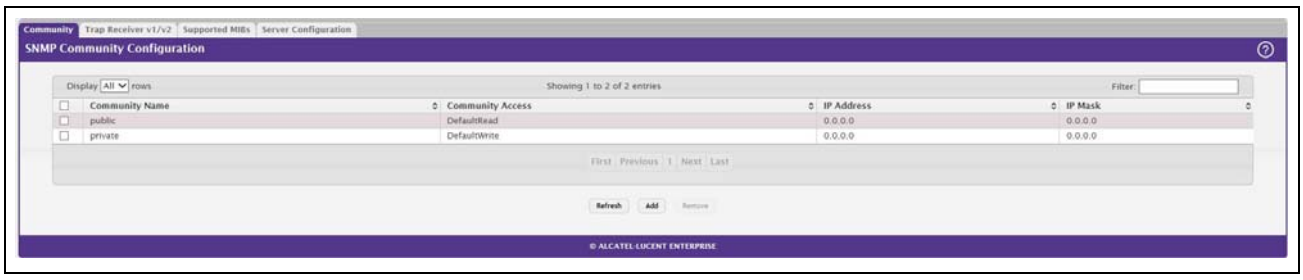
SNMP Community Configuration

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.

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 36: 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 37: SNMP Community Configuration

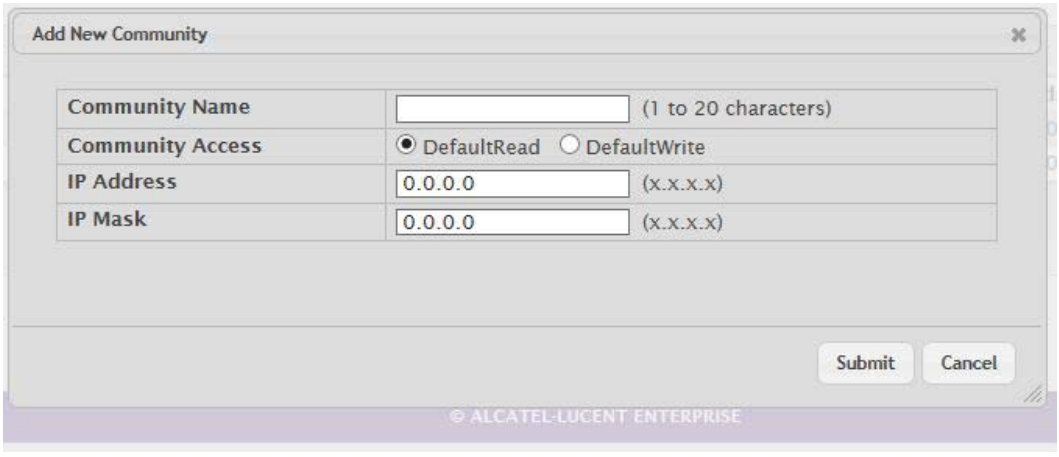


Table 35: Community Configuration Fields

Field	*Description*
Community Name	Contains the predefined and user-defined community strings that act as a password and are used to authenticate the SNMP management station to the device. A community string can contain a maximum of 20 characters. By default, the options available in the menu are as follows: • **public:** This SNMP community has Read Only privileges and its status set to enable • **private:** This SNMP community has Read/Write privileges and its status set to enable.
Community Access	Specifies the access control policy for the community.
Client IP Address	Taken together, the **Client IP Address** and **Client IP Mask** denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (IP Address or IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's IP address is ANDed with the mask, as is the Client IP Address, and, if the values are equal, access is allowed. For example, if the Client IP Address and Client IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose IP address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Client IP Mask value of 255.255.255.255, and use that machine's IP address for Client IP Address.
Client IP Mask	Along with the **Client IP Address**, the **Client IP Mask** denotes a range of IP addresses from which SNMP clients may use that community to access this device.
Access Mode	Specify the access level for this community: • **Read-Only:** The Community has read only access to the MIB objects configured in the view. • **Read-Write:** The Community has read/modify access to the MIB objects configured in the view.
Status	Specify the status of this community: • **Enable:** The community is enabled, and the Community Name must be unique among all valid Community Names or the set request will be rejected. • **Disable:** The Community is disabled and the Community Name becomes invalid.

- 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 38: 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 39: Trap Receiver v1/v2 Configuration

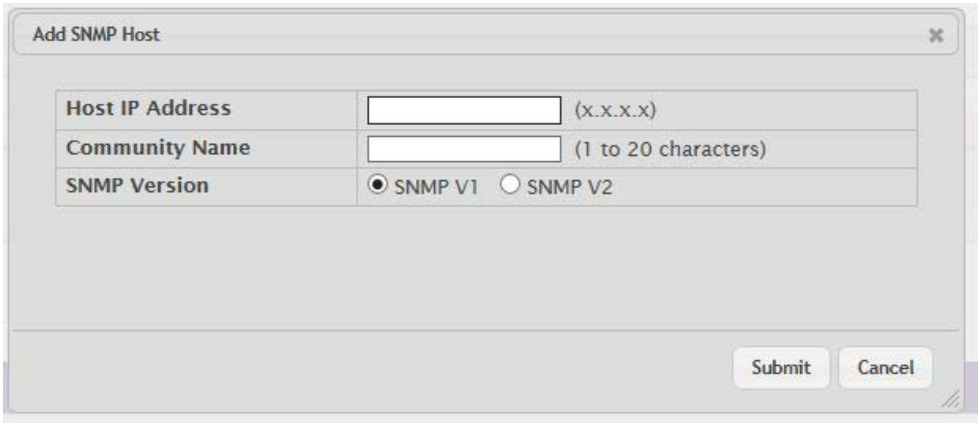


Table 36: Trap Receiver v1/v2 Configuration Fields

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: • **Inform** – 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. • **Trap** – 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.
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.

Table 36: Trap Receiver v1/v2 Configuration Fields (Cont.)

Field	Description
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 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 the MIBs that the system currently supports.

To access the Supported MIBs page, click **System > Advanced Configuration > SNMP > Supported MIBs** in the navigation menu.

Figure 40: Supported MIBs

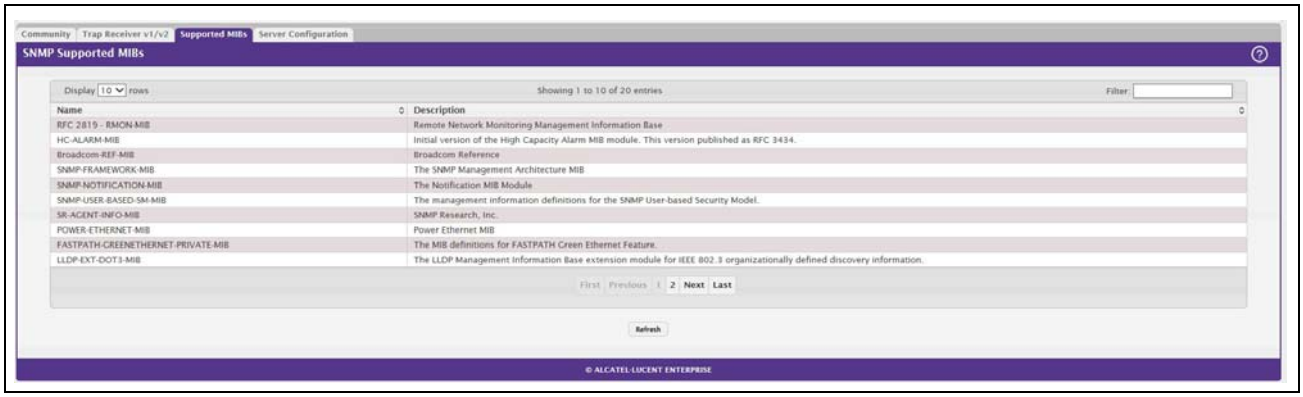


Table 37: Supported MIBs Fields

Field	Description
Name	The RFC number if applicable and the name of the MIB.
Description	The RFC title or MIB description.

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 Detailed Statistics

The Switch Detailed Statistics page shows detailed statistical information about the traffic the switch handles.

To access the Switch Detailed page, click **System > Statistics > System >Switch** in the navigation menu.

Figure 41: Switch Statistics

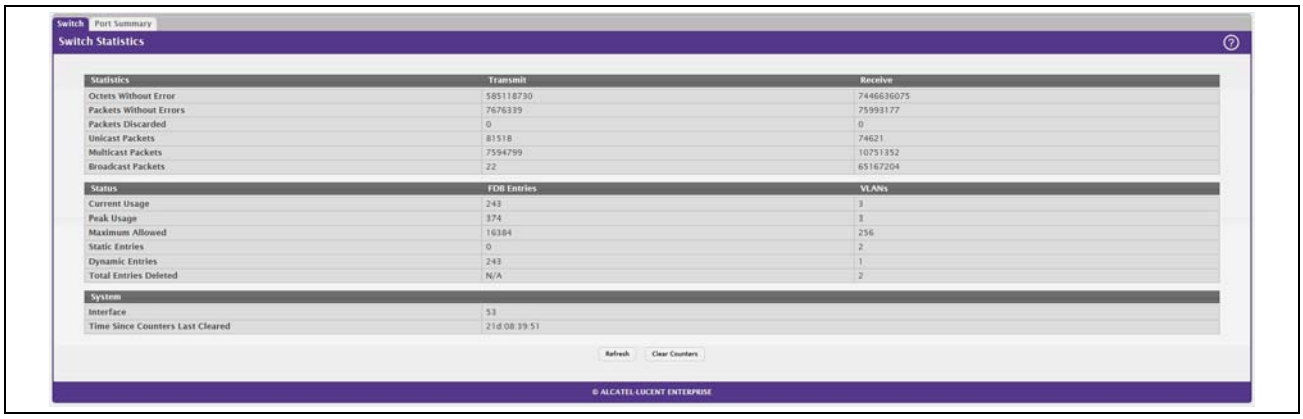


Table 38: Switch Statistics Fields

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.
Multicast Packets	The total number of packets transmitted or received by the device that were directed to a multicast address. Note that 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. Note that 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.

Table 38: Switch Statistics Fields (Cont.)

Field	*Description*
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 42: Port Summary

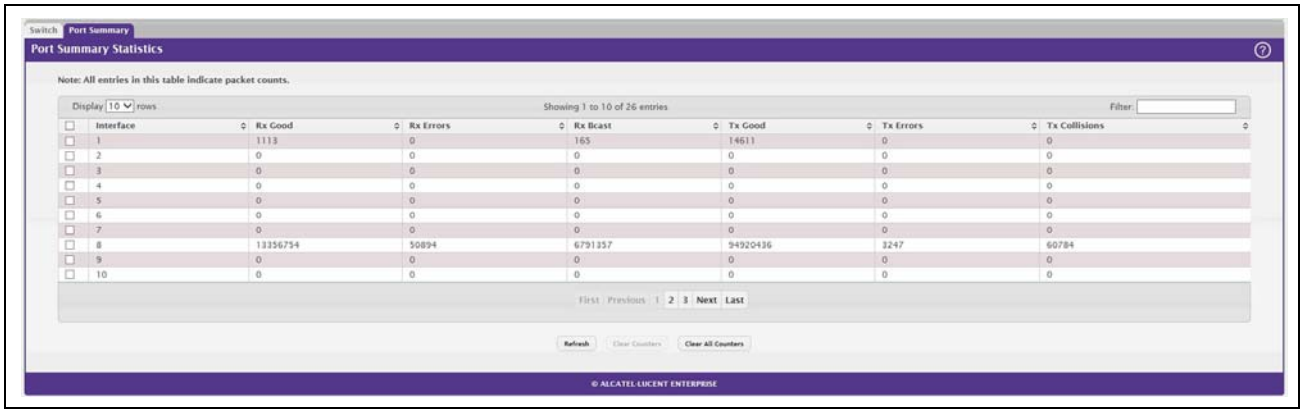


Table 39: Port Summary Fields

Field	*Description*
Interface	Identifies the port or LAG.

Table 39: Port Summary Fields (Cont.)

Field	*Description*
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. Note that 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.

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.

To access the System Reset page, click **System > Utilities > System Reset** in the navigation menu.

Figure 43: System Reset

Table 40: System Reset Fields

Field	*Description*
Generate Core Dump before reset	Generates core dump file on demand.
Reset (Button)	Initiates the system reset action after displaying a confirmation message. Note that 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.

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.

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 44: Transfer

Table 41: 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 **File Upload** 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 **File Download** 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 45: File Upload

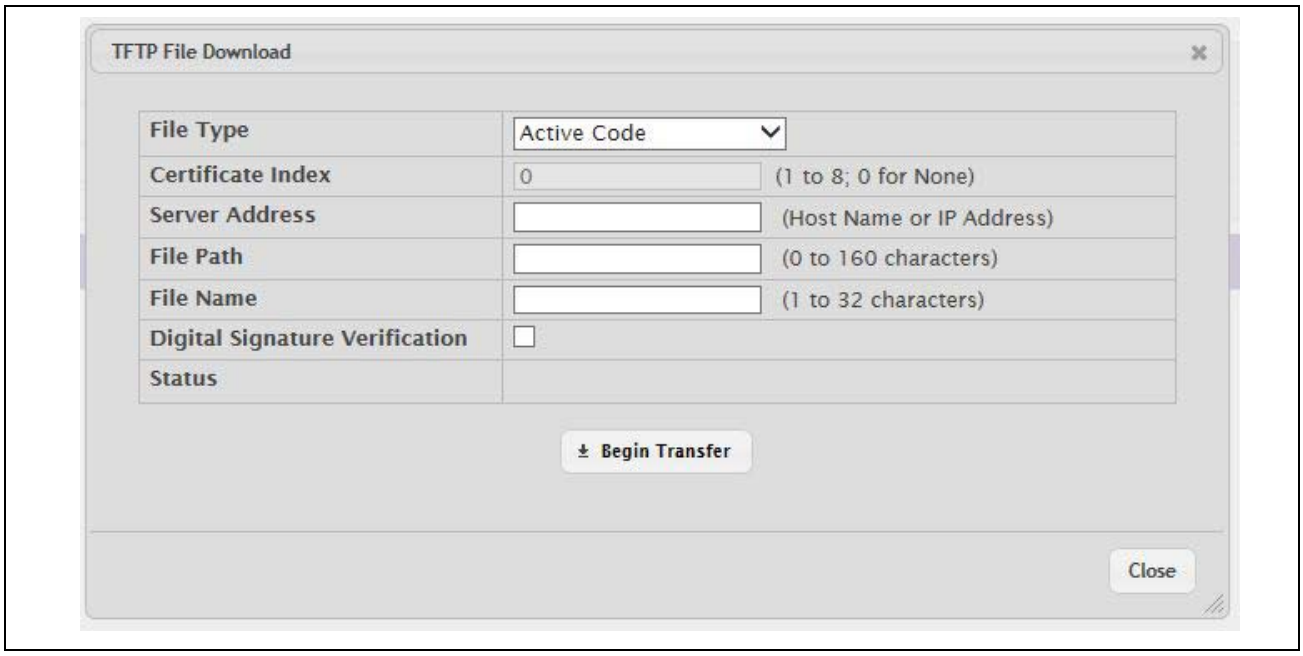
The following information describes the fields in the File Upload window for all protocols.

Table 42: File Upload Fields

Field	*Description*
File Type	Specify the type of file to transfer from the device to a remote system. • **Active Code** – Select this option to transfer an active image. • **Backup Code** – Select this option to transfer a backup image. • **Startup Configuration** – Select this option to transfer a copy of the stored startup configuration from the device to a remote system. • **Error Log** – Select this option to transfer the system error (persistent) log, which is also known as the event log, to a remote system. • **Buffered Log** – Select this option to transfer the system buffered (in-memory) log to a remote system.
Image	If the selected File Type is Code, specify whether to transfer the Active or Backup image to a remote system.
Server Address	Specify the IPv4 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 46: File Download



The following information describes the fields in the File Download window for all protocols.

Table 43: File Download Fields

Field	*Description*
File Type	Specify the type of file to transfer to the device: • **Active Code** – Select this option to transfer a new image to the device. The code file is stored as the active image. • **Backup Code** – Select this option to transfer a new image to the device. The code file is stored as the backup image. • **Startup Configuration** – Select this option to update the stored startup configuration file. If the file has errors, the update will be stopped. • • **Factory Defaults** – Select this option to transfer the factory default configuration file to a remote system. • **CA Root Certificate** – Select this option to transfer an CA certificate file to the device. This will be used as the root certificate for one of the syslog servers. Based on the index number the file will be named accordingly. • **Client Key** – Select this option to transfer an client certificate file to the device. This will be used as the client certificate for one of the syslog servers. Based on the index number the file will be named accordingly. • **Client SSL Certificate** – Select this option to transfer an client key file to the device. Based on the index number the file will be named accordingly. •
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.
Certificate Index	Index used to name a related group of certificate (PEM) or key files.

Table 43: File Download Fields (Cont.)

Field	*Description*
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.
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.
Progress	Represents the completion percentage of the file transfer. The file transfer begins after you complete the required fields and click the download icon to the right of this field.
Digital Signature Verification	For Code and Startup Configuration file types, this option, when checked, will verify the file download with the digital signature.
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 47: Core Dump

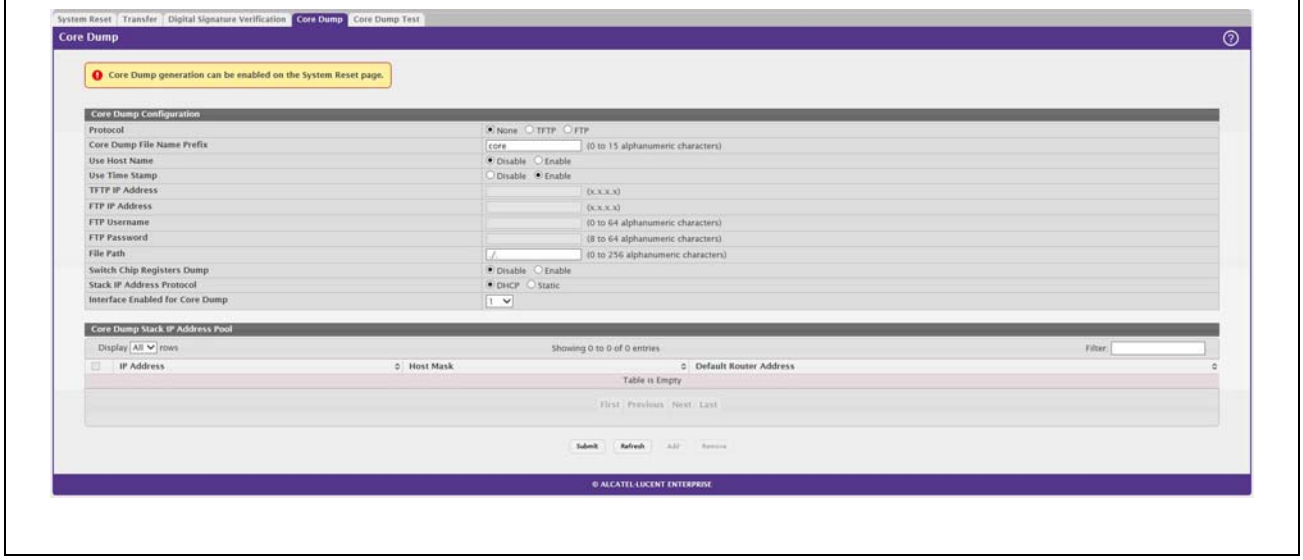


Table 44: Core Dump Configuration Fields

Field	Description
Protocol	The protocol used to store the core dump file. User can select: • **None**—Disable Core Dump. • **TFTP**—Configure protocol to upload Core Dump to the TFTP server. • **FTP**—Configure protocol to upload Core Dump to the FTP server.
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.
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, NFS mount or USB device 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.
Interface Enabled for Core Dump	Network port number which is used to upload Core Dump when swtchdrvr is down.

Table 45: 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 48: Core Dump Test

Table 46: Core Dump Test Fields

Field	*Description*
Status	Displays test status as **OK** if test passes and **Error** if test fails.
Result	Displays detailed error information with logs.

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 49: Time Range

Table 47: Time Range Configuration

Field	*Description*
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.

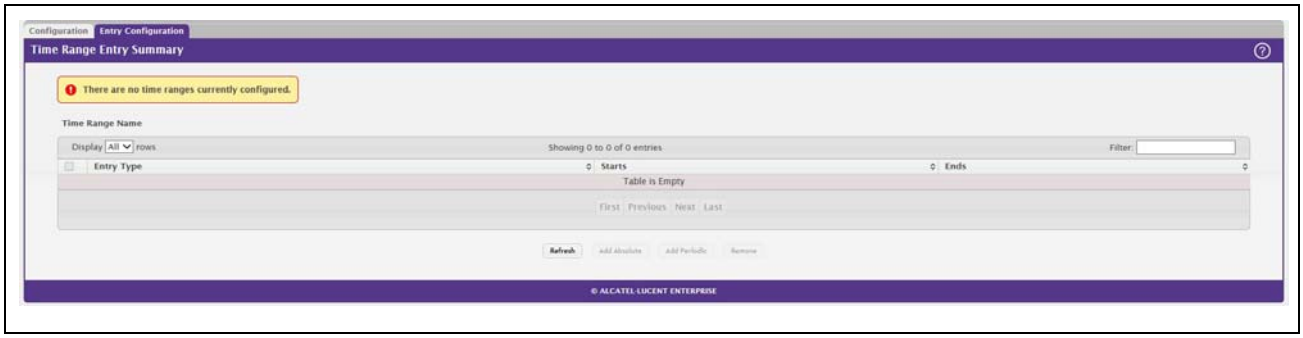
Time Range Entry Configuration

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 50: 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 48: 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 48: Time Range Entry Configuration (Cont.)

Field	*Description*
Applicable Days	Specify the day(s) when the time entry occurs: • **Daily—**Has the same start and end time every day • **Weekdays—**Has the same start and end time Monday through Friday • **Weekdays—**Has the same start and end time on Saturday and Sunday • **Days of the Week**—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.
Start Day	(Periodic Days of Week only) Select the day the time range entry starts. To select multiple days, hold the CTRL 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.
Absolute Time Range Entry	
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.

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

Configuring SNTP Settings

OS2220 Websmart 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. OS2220 Websmart software operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by Stratums. Stratums define 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 stratums:

- **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 51: SNTP Global Configuration

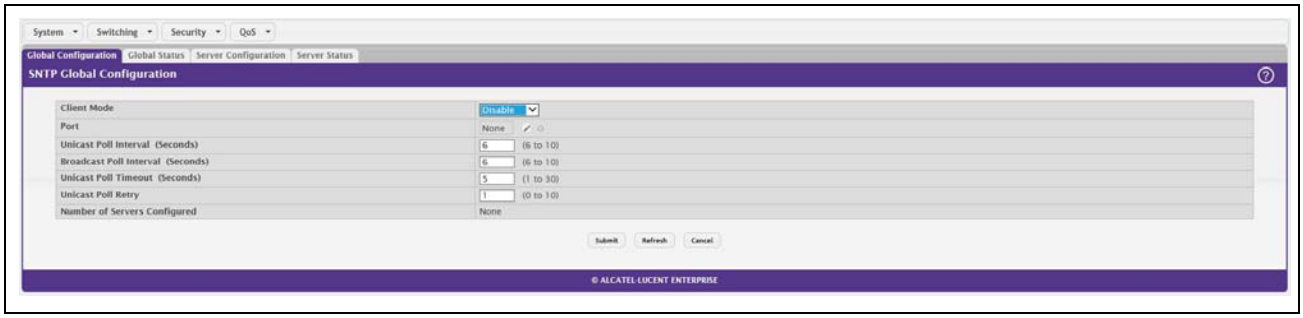


Table 49: SNTP Global Configuration Fields

Field	*Description*
Client Mode	Use drop-down list specify the SNTP client mode, which is one of the following modes: • **Disable:** SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed. • **Unicast:** 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. • **Broadcast:** 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.
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 52: Global Status

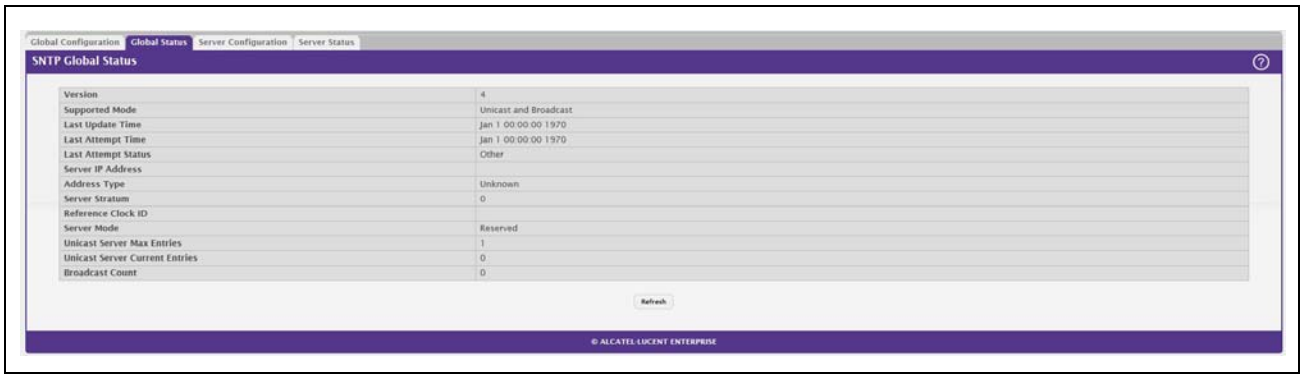


Table 50: Global Status Fields

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.

Table 50: Global Status Fields (Cont.)

Field	*Description*
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: • **Other:** None of the following enumeration values. • **Success:** The SNTP operation was successful and the system time was updated. • **Request Timed Out:** A directed SNTP request timed out without receiving a response from the SNTP server. • **Bad Date Encoded:** The time provided by the SNTP server is not valid. • **Version Not Supported:** The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized:** The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • **Server Kiss Of Death:** 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.
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 53: SNTP Server Configuration

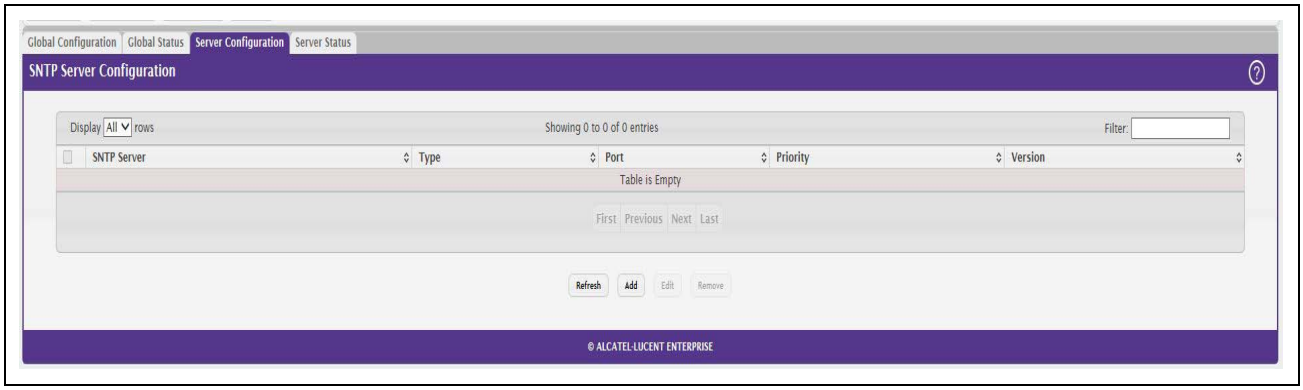


Table 51: SNTP Server Configuration Fields

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 **Add** to configure a new SNTP server. You can define up to three SNTP servers.
Type	Select **IPv4** if you entered an IPv4 address, **DNS** 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 54: SNTP Server Status

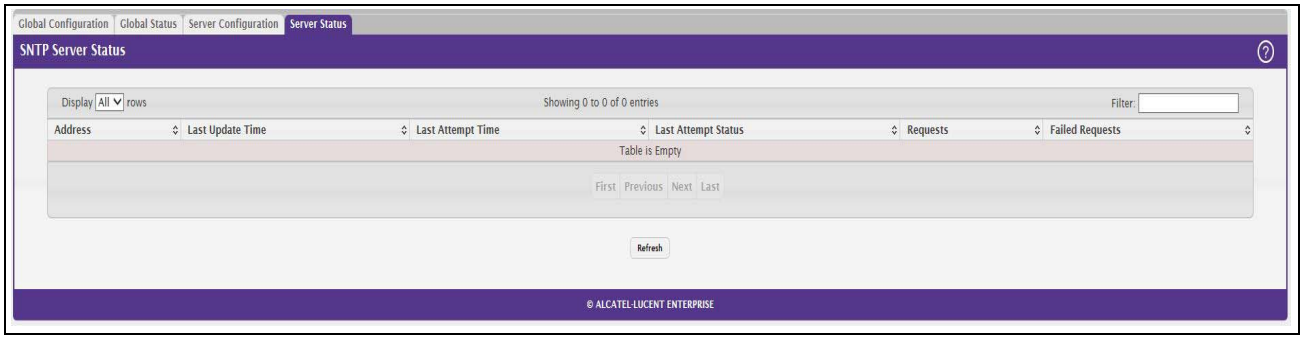


Table 52: SNTP Server Status Fields

Field	*Description*
Address	Specifies all the existing Server Addresses. If no Server configuration exists, a message saying “No SNTP server exists” 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: • **Other:** None of the following enumeration values. • **Success:** The SNTP operation was successful and the system time was updated. • **Request Timed Out:** A directed SNTP request timed out without receiving a response from the SNTP server. • **Bad Date Encoded:** The time provided by the SNTP server is not valid. • **Version Not Supported:** The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized:** The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • **Server Kiss Of Death:** 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.
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.

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 55: Time Zone Summary

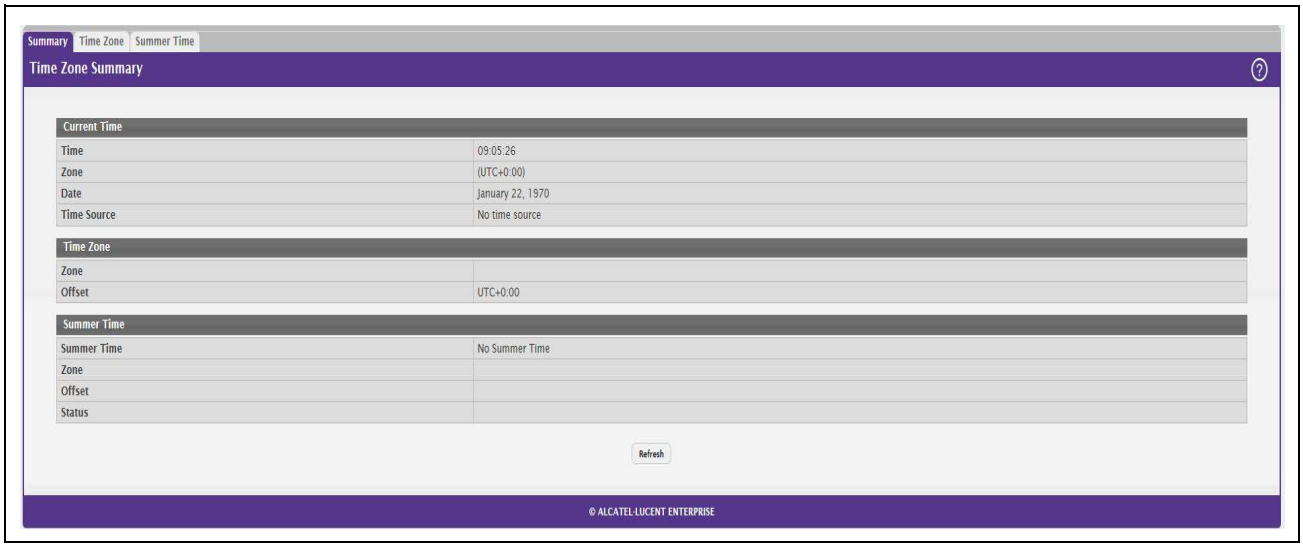


Table 53: Time Zone Summary Fields

Field	*Description*
Current Time	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. • **Time** — The current time on the system clock. This time is used to provide time stamps on log messages. • **Zone** — The acronym that represents the time zone. • **Date** — The current date on the system. • **Time Source** — The time source from which the time update is taken: – **SNTP** – The time has been acquired from an SNTP server. – **No Time Source** – The time has either been manually configured or not configured at all.
Time Zone	This section contains information about the time zone and offset. **Zone** — The acronym that represents the time zone. **Offset** — The number of hours offset from Coordinated Universal Time (UTC), which is also known as Greenwich Mean Time (GMT).

Table 53: Time Zone Summary Fields (Cont.)

Field	Description
Summer Time	The administrative status of summer time (daylight saving time). In some regions, the time shifts by one hour in the fall and spring. • **Summer Time** — The summer time mode on the system: – **Disable** — Summer time is not active, and the time does not shift based on the time of year. – **Recurring** — Summer time occurs at the same time every year. The start and end times and dates for the time shift must be manually configured. – **EU** — 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. – **USA** — 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. – **Non-Recurring** — 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. • **Zone**— The acronym that represents the time zone of the summer time. • **Offset**— The number of hours offset from Coordinated Universal Time (UTC), which is also known as Greenwich Mean Time (GMT). • **Status**— Indicates if summer time is currently active.

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 56: Time Zone Configuration

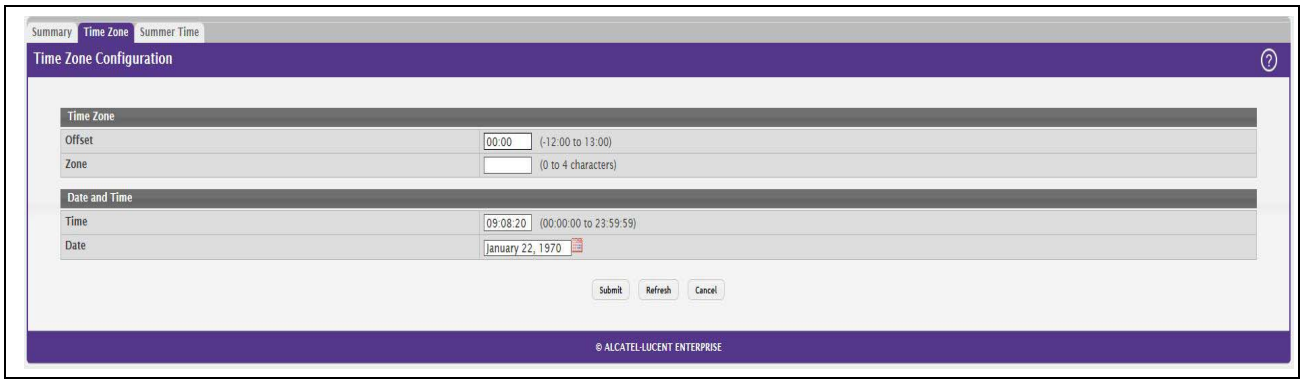


Table 54: Time Zone Configuration Fields

Field	*Description*
Time Zone	The time zone settings include the amount of time the system clock is offset from Coordinated Universal Time (UTC) and the time zone acronym. • **Offset** — The number of hours the system clock is offset from UTC, which is also known as Greenwich Mean Time (GMT). • **Zone** — The acronym that represents the time zone. This field is not validated against an official list of time zone acronyms.
Date and Time	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. • **Time** — The current time in hours, minutes, and seconds on the system clock. • **Date** — 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.

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 57: Summer Time Configuration

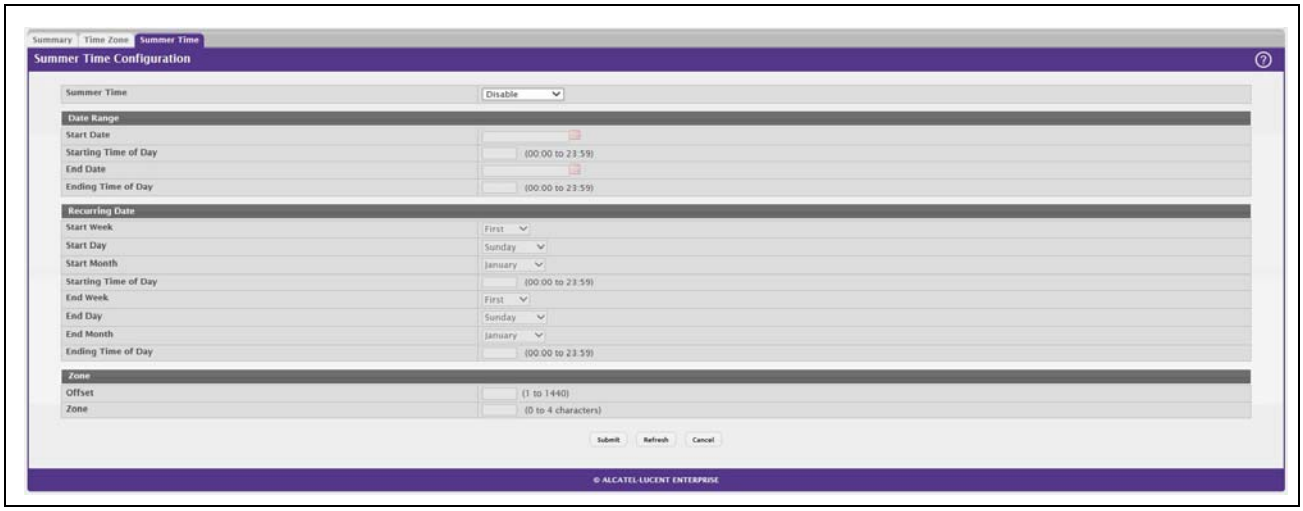


Table 55: Summer Time Configuration Fields

Field	*Description*
Summer Time	The summer time mode on the system: • **Disable** – Summer time is not active, and the time does not shift based on the time of year. • **Recurring** – Summer time occurs at the same time every year. The start and end times and dates for the time shift must be manually configured. • **EU** – 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. • **USA** – 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. • **Non-Recurring** – 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.
Date Range	The fields in this section are available only if the Non-Recurring mode is selected from the Summer Time menu. • **Start Date** — 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. • **Starting Time of Day** — The time, in hours and minutes, to start summer time on the specified day. • **End Date** — 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. • **Ending Time of Day** — The time, in hours and minutes to end summer time on the specified day.
Recurring Date	The fields in this section are available only if the Recurring mode is selected from the Summer Time menu. • **Start Week** — The week of the month within which summer time begins. • **Start Day** — The day of the week on which summer time begins. • **Start Month** — The month of the year within which summer time begins. • **Starting Time of Day** — The time, in hours and minutes, to start summer time. • **End Week** — The week of the month within which summer time ends. • **End Day** — The day of the week on which summer time ends. • **End Month** — The month of the year within which summer time ends. • **Ending Time of Day** — The time, in hours and minutes, to end summer time.
Zone	The fields in this section are available only if the Recurring or Non-Recurring modes are selected from the Summer Time menu. • **Offset** — The number of minutes to shift the summer time from the standard time. • **Zone** — The acronym associated with the time zone when summer time is in effect.

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.

Section 4: Configuring Switching Information

- Managing VLANs
- Voice VLAN Configuration
- Voice VLAN Interface
- Creating MAC Filters
- Configuring IGMP Snooping
- Creating Port Channels
- Viewing Multicast Forwarding Database Information
- Configuring Spanning Tree Protocol
- Mapping 802.1p Priority
- Configuring Port Security
- Managing LLDP
- Loop Protection

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.

To access the VLAN Status page, click **Switching > VLAN > Status** in the navigation menu.

Figure 58: VLAN Status

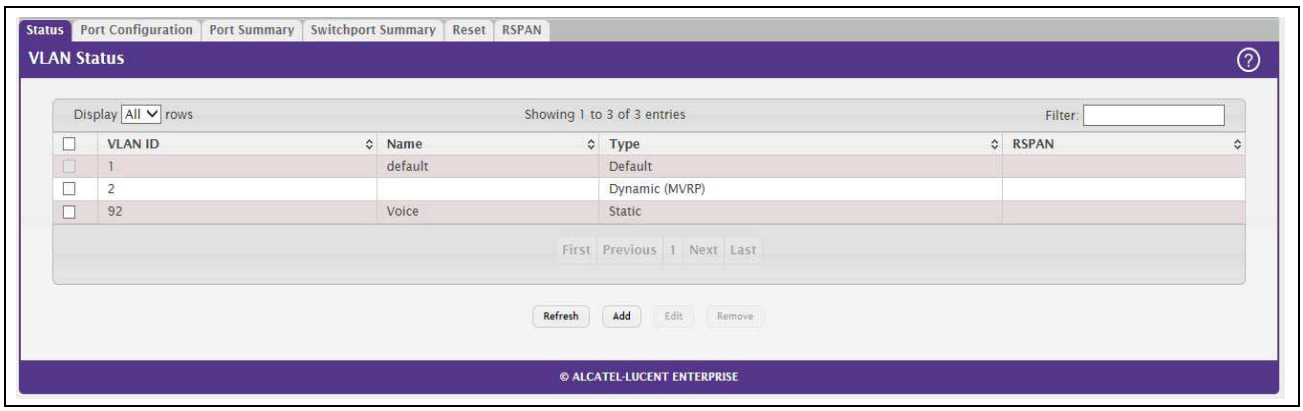


Table 56: VLAN Status Fields

Field	*Description*
VLAN ID	The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 3965.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named Default.
VLAN Type	The VLAN type, which can be one of the following: • **Default:** (VLAN ID = 1) -- always present • **Static:** A VLAN you have configured • **Dynamic:** A VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore remove

Table 56: VLAN Status Fields (Cont.)

Field	*Description*
RSPAN	List the status of RSPAN, enabled or disabled.

Use the buttons to perform the following tasks:

- To add a VLAN, click **Add** and specify a VLAN ID in the available field.
- To configure a name for a VLAN or to convert a dynamic VLAN to a static VLAN, select the entry to modify and click **Edit**. Then, configure the desired VLAN settings.
- 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.

Figure 59: Add VLAN

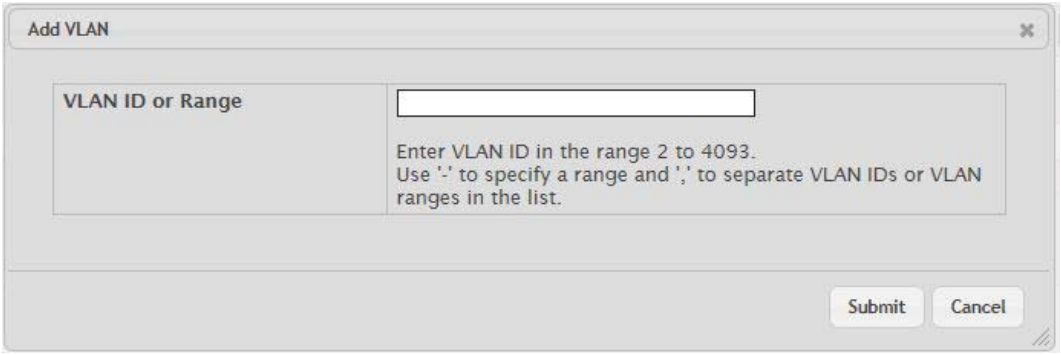


Table 57: Add VLAN Fields

Field	*Description*
VLAN ID	Edit VLAN Configuration
Name	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.
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 **Refresh** to display the latest information from the router.

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 60: VLAN Port Configuration

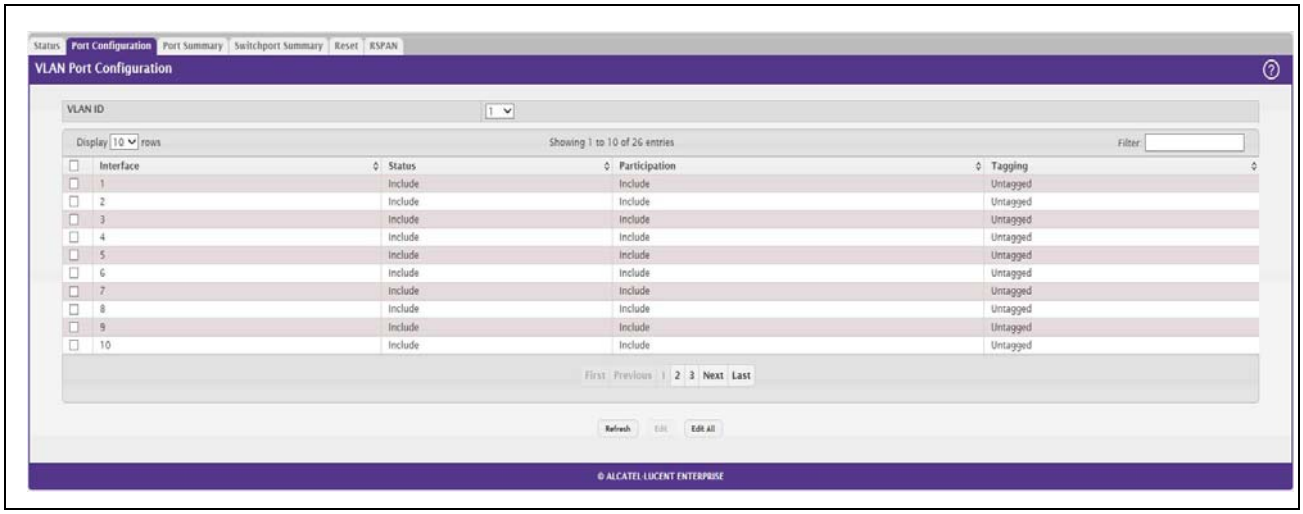


Table 58: VLAN Port Configuration Fields

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 **All** 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: • **Include** – The port is a member of the selected VLAN. • **Exclude** – The port is not a member of the selected VLAN.
Participation	The participation mode of the interface in the selected VLAN, which is one of the following: • **Include** – The port is always a member of the selected VLAN. This mode is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** – The port is never a member of the selected VLAN. This mode is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Auto Detect** – 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.

Table 58: VLAN Port Configuration Fields (Cont.)

Field	*Description*
Tagging	The tagging behavior for all the ports in this VLAN, which is one of the following: • **Tagged** – The frames transmitted in this VLAN will include a VLAN ID tag in the Ethernet header. • **Untagged** – The frames transmitted in this VLAN will be untagged.

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 61: VLAN Port Summary

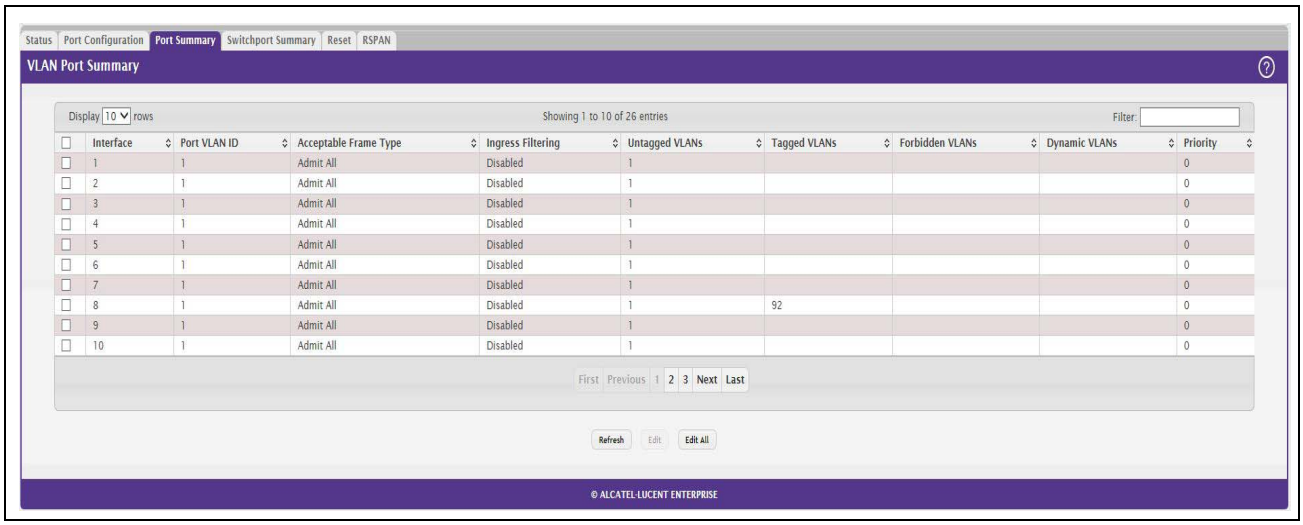


Table 59: VLAN Port Summary Fields

Field	*Description*
Interface	Identifies the physical interface associated with the rest of the data in the row.
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.
Acceptable Frame Types	Indicates how the interface handles untagged and priority tagged frames. The options include the following: • **Admit All** – Untagged and priority tagged frames received on the interface are accepted and assigned the value of the Port VLAN ID for this interface. • **Only Tagged** – The interface discards any untagged or priority tagged frames it receives. • **Only Untagged** – The interface discards any tagged frames it receives. 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. • **Enable:** A tagged frame is discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. • **Disable:** All tagged frames are accepted, which is the factory default.
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.

Table 59: VLAN Port Summary Fields (Cont.)

Field	*Description*
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 62: VLAN Switchport Summary

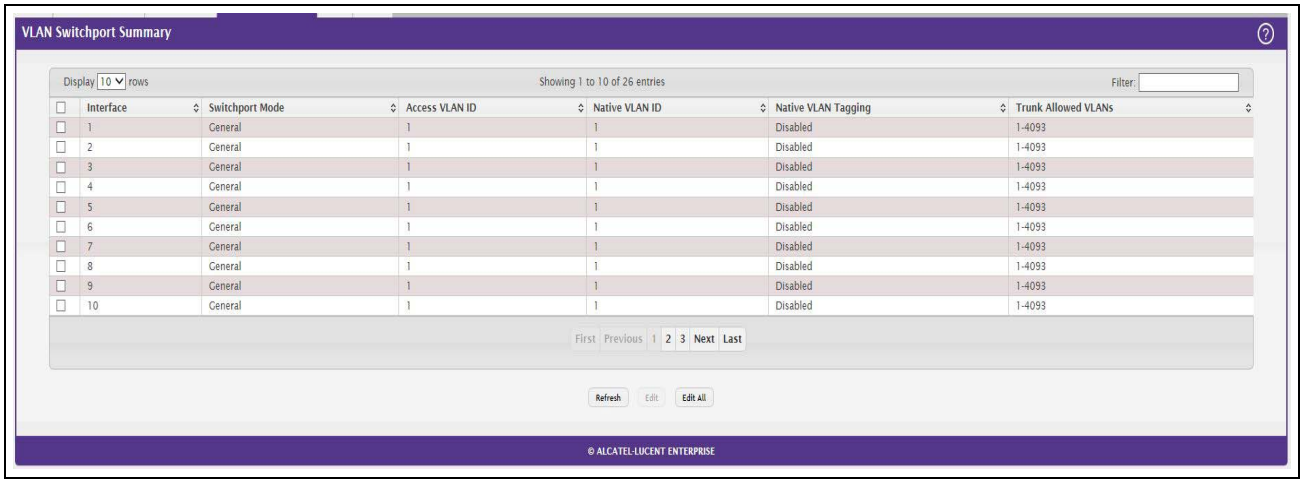


Table 60: VLAN Switchport Summary Fields

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: • **Access—**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. • **Trunk—**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. • **General** —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.
Access VLAN ID	The access VLAN for the port, which is valid only when the port switchport mode is Access.
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**.

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 63: 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 64: RSPAN VLAN Configuration

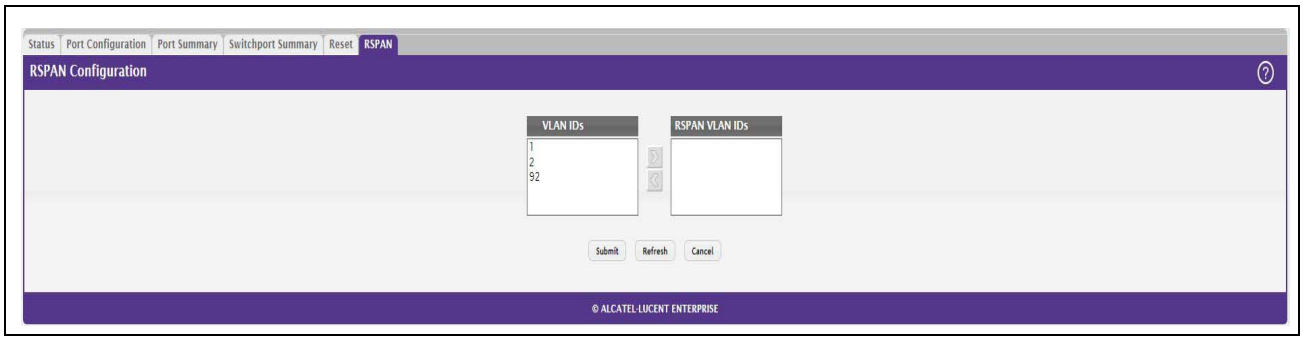


Table 61: RSPAN VLAN Configuration Fields

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 CTRL + click to select multiple VLAN IDs). Then, click the appropriate arrow to move the selected VLAN or VLANs to the RSPAN VLAN IDs window.

Table 61: RSPAN VLAN Configuration Fields (Cont.)

Field	Description
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 CTRL + 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.

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 65: Voice VLAN Configuration

Table 62: Voice VLAN Configuration Fields

Field	Description
Voice VLAN Admin Mode	Click **Enable** or **Disable** 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 66: Voice VLAN Interface

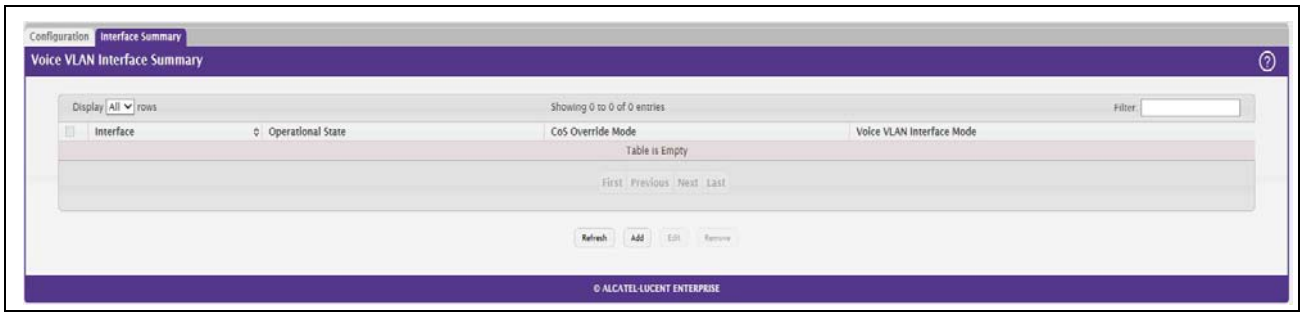


Table 63: Voice VLAN Interface Fields

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: • **Enabled** – The port ignores the 802.1p priority value in the Ethernet frames it receives from connected devices. • **Disabled** – The port trusts the priority value in the received frame.

Table 63: Voice VLAN Interface Fields (Cont.)

Field	Description
Voice VLAN Interface Mode	Indicates how an IP phone connected to the port should send voice traffic: • **LAN ID** – Forward voice traffic in the specified voice VLAN. • **Dot1p** – Tag voice traffic with the specified 802.1p priority value. • **None** – Use the settings configured on the IP phone to send untagged voice traffic. • **Untagged** – Send untagged voice traffic. • **Disable** – Operationally disables the Voice VLAN feature on the interface.
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.

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 67: MAC Filter Configuration

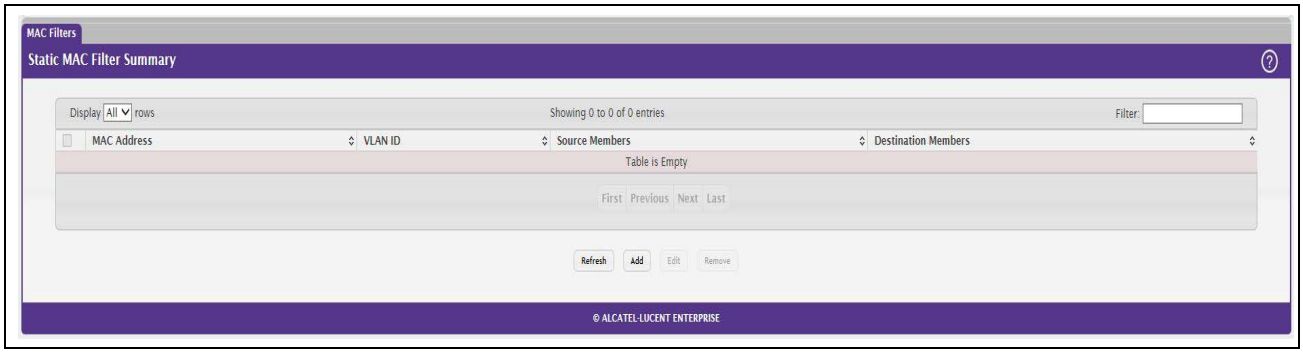


Table 64: MAC Filter Configuration Fields

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: • 00:00:00:00:00:00 • 01:80:C2:00:00:00 to 01:80:C2:00:00:0F • 01:80:C2:00:00:20 to 01:80:C2:00:00:21 • FF:FF:FF:FF:FF:FF
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 (CTRL + click to select multiple ports). Then, use the appropriate arrow icon to move the selected ports to the Source Members field.
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 (CTRL + 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 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 68: IGMP Snooping Global Configuration and Status

Table 65: 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 “Interface Configuration” on page 108.
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 69: IGMP Snooping Interface Configuration

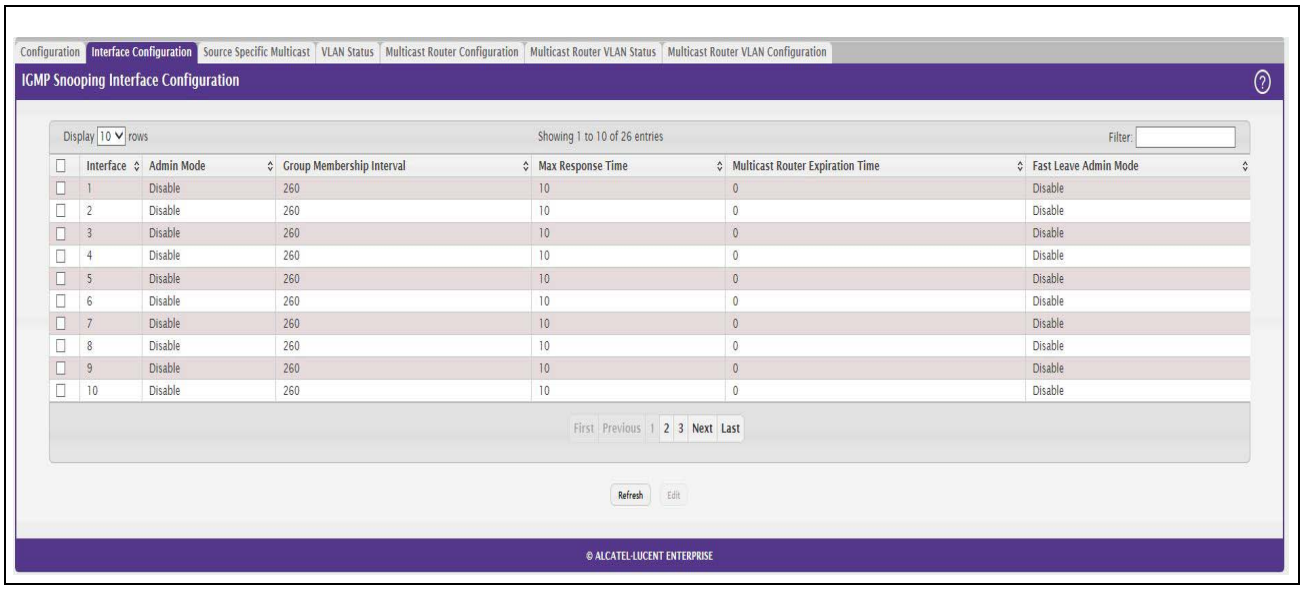


Table 66: IGMP Snooping Interface Configuration Fields

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.
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 **Disable**.

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 70: IGMP Snooping Source Specific Multicast

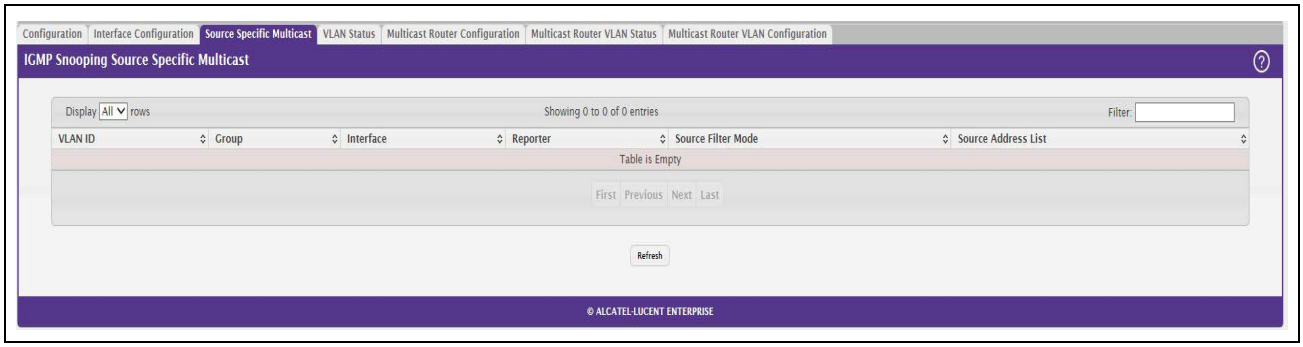


Table 67: IGMP Snooping Source Specific Multicast Fields

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.
Source Address List	List of source IP addresses for which source filtering is requested.

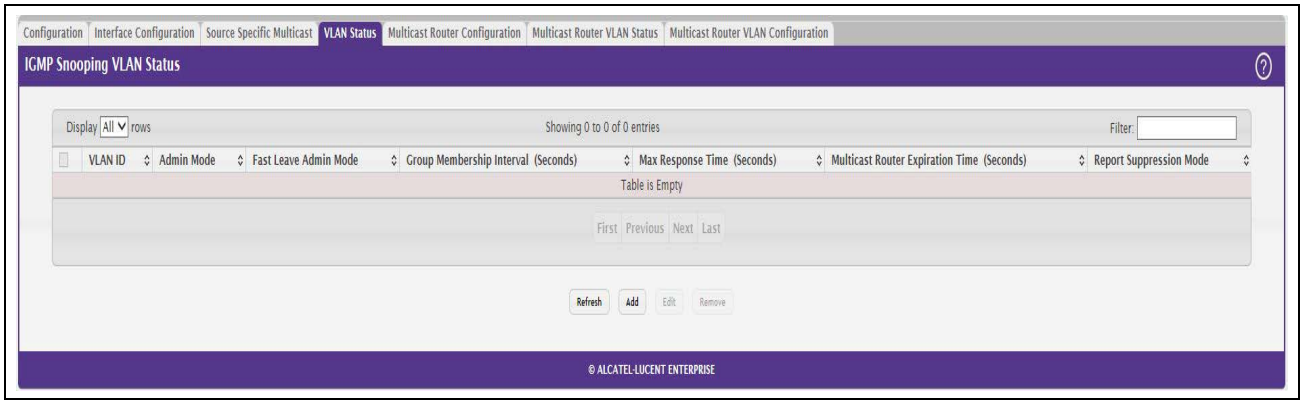
Click **Refresh** to refresh the page with the most current data from the switch.

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 71: 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 68: 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.
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 to wait for a report for a particular group on the VLAN before the IGMP snooping feature deletes the VLAN from the group.

Table 68: IGMP Snooping VLAN Status Fields (Cont.)

Field	*Description*
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: • **Enabled** – Only the first IGMP report from all hosts for a group IGMP report is forwarded to the multicast routers. • **Disabled** – The device forwards all IGMP reports from all hosts in a multicast group to the multicast routers.

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 72: Multicast Router Configuration

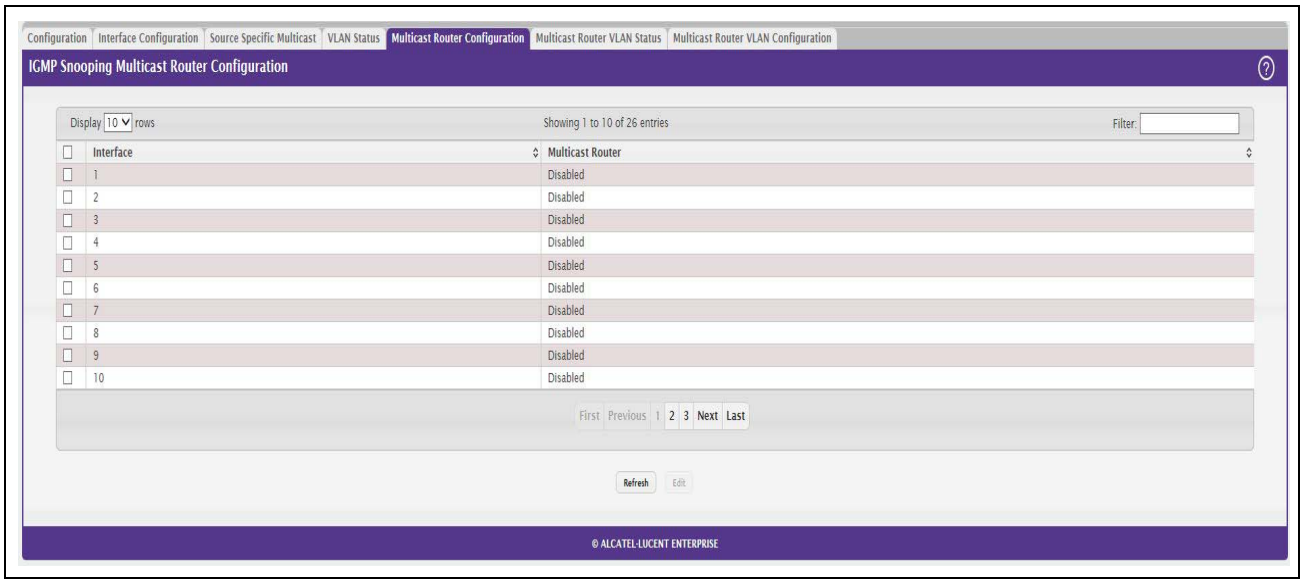


Table 69: Multicast Router Configuration Fields

Field	*Description*
Interface	Select the physical or LAG interface to display.
Multicast Router	Set the multicast router status: • **Enabled:** The port is a multicast router interface. • **Disabled:** The port does not have a multicast router configured.

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 73: IGMP Snooping Multicast Router VLAN Status

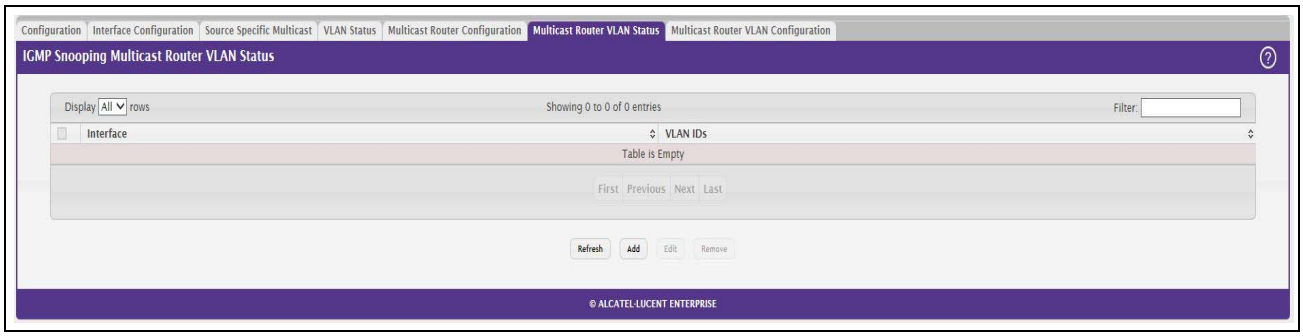


Table 70: IGMP Snooping Multicast Router VLAN Status Fields

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 74: IGMP Snooping Multicast Router VLAN Configuration

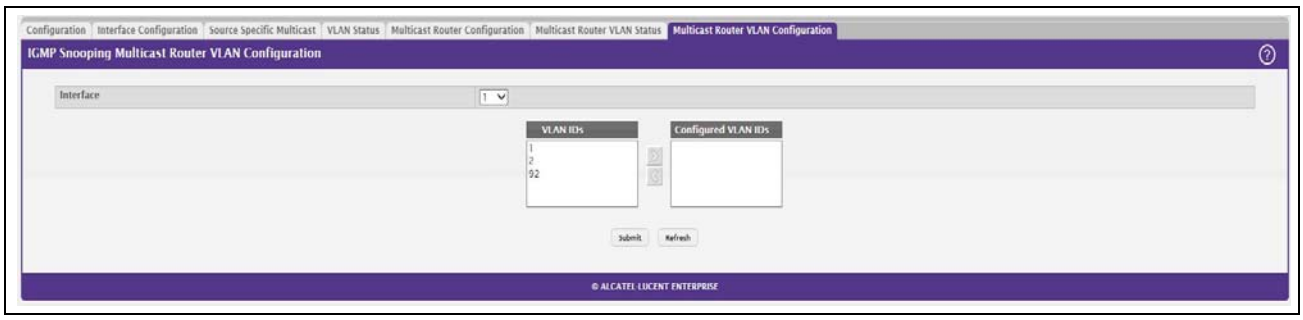


Table 71: IGMP Snooping Multicast Router VLAN Configuration Fields

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 CTRL + 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 CTRL + 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.

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 LACPDUs.

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 75: Port Channel Summary

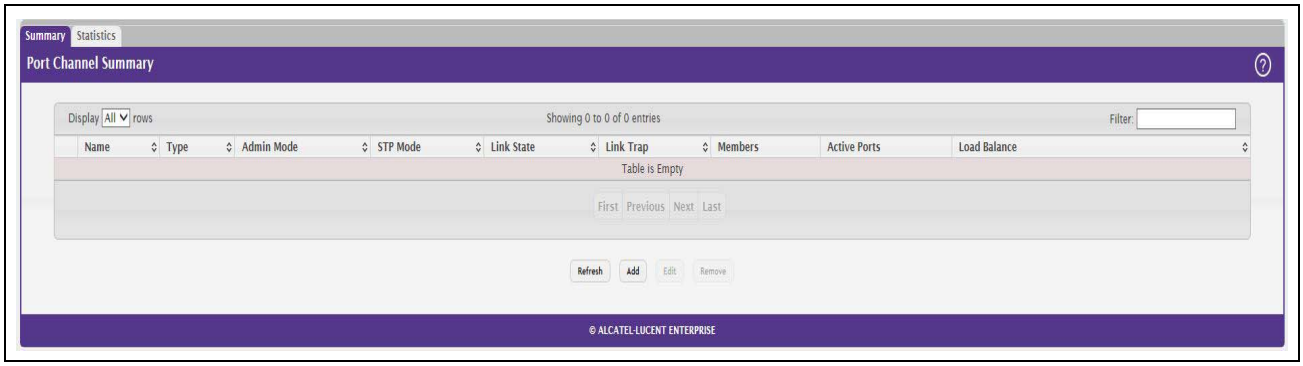


Table 72: Port Channel Summary Fields

Field	*Description*
Name	Identifies the user-configured text name of the port channel.
Type	The type of port channel: • **Dynamic** – 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. • **Static** – 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. 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.
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.
Members	Lists the ports that are members of the Port Channel. There can be a maximum of 4 ports assigned to a Port Channel.
Active Ports	Lists the ports that are actively participating members of this Port Channel.

Table 72: Port Channel Summary Fields (Cont.)

Field	*Description*
Load Balance	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: • Source MAC, VLAN, EtherType, Incoming Port • Destination MAC, VLAN, EtherType, Incoming Port • Source/Destination MAC, VLAN, EtherType, Incoming Port • Source IP and Source TCP/UDP Port Fields • Destination IP and Destination TCP/UDP Port Fields • Source/Destination IP and TCP/UDP Port Fields • Enhanced Hashing Mode

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 76: Port Channel Configuration

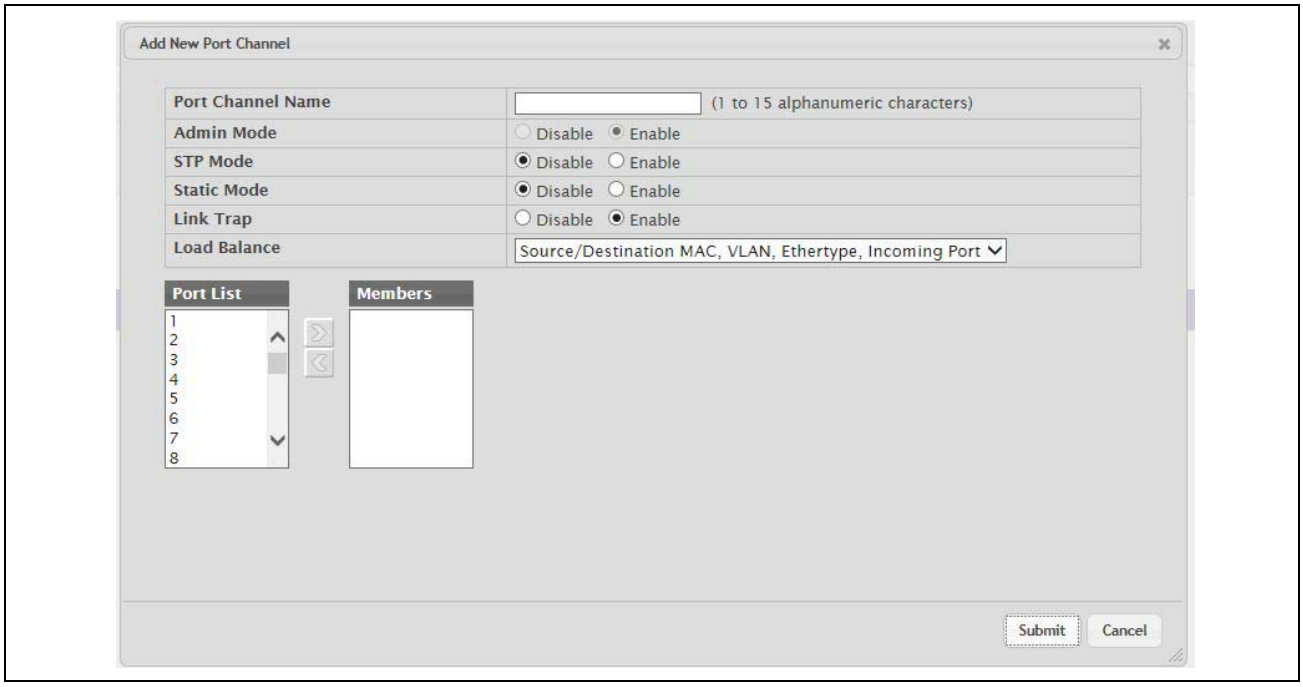


Table 73: Port Channel Configuration Fields

Field	*Description*
Port Channel Interface	Select the port channel to configure. The port channel follows a lag <number> interface naming convention.
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 LACPDUs 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: • **Disable:** Spanning tree is disabled for this Port Channel. • **Enable:** Spanning tree is enabled for this Port Channel.
Static Mode	Select enable or disable from the pull-down menu. The factory default is Disable. • **Enable:** 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 LAGPDUs it may receive are dropped. A static port-channel interface does not require a partner system to be able to aggregate its member ports. • **Disable:** The port channel is dynamically maintained. The interface transmits and processes LAGPDUs and requires a partner system.
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: • Source MAC, VLAN, EtherType, and source port • Destination MAC, VLAN, EtherType and source port • Source/Destination MAC, VLAN, EtherType, and source port • Source IP and Source TCP/UDP Port • Destination IP and Destination TCP/UDP Port • Source/Destination IP and source/destination TCP/UDP Port • Enhanced hashing mode
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.
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. • **Include:** The port participates in the port channel. • **Exclude:** The port does not participate in the port channel, which is the default.

Table 73: Port Channel Configuration Fields (Cont.)

Field	Description
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 77: Port Channel Statistics

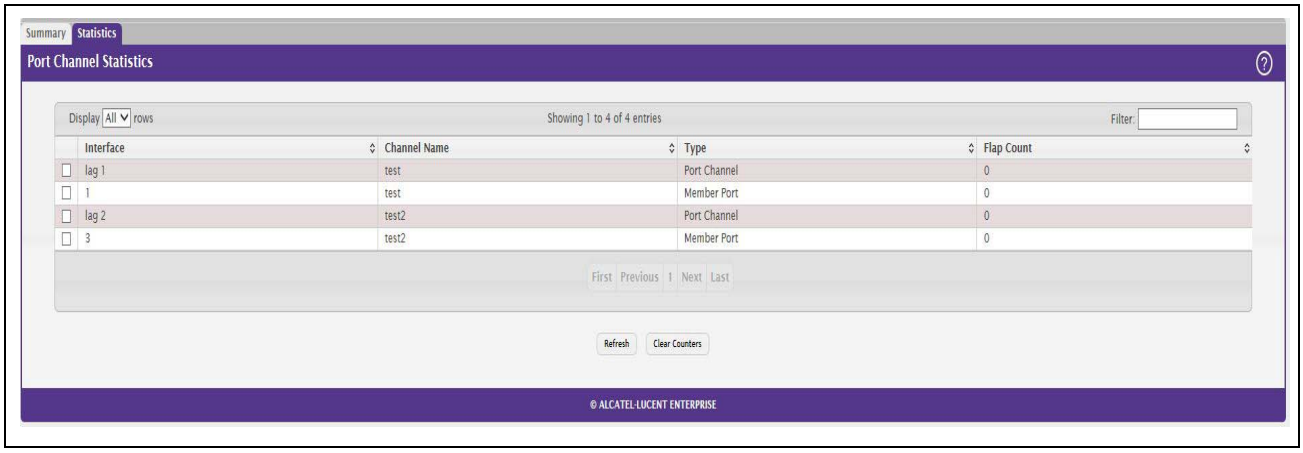


Table 74: Port Channel Statistics Fields

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).

Table 74: Port Channel Statistics Fields (Cont.)

Field	Description
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 78: MFDB Table

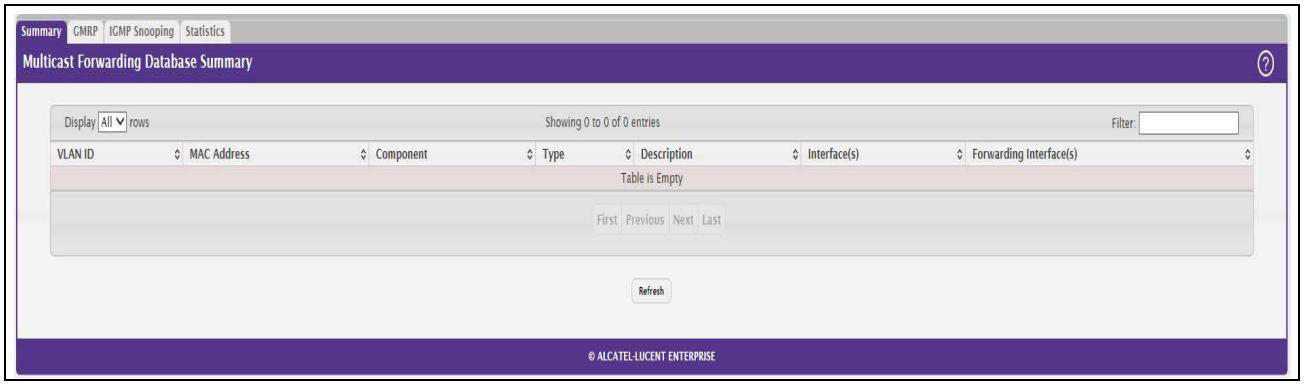


Table 75: MFDB Summary Fields

Field	*Description*
VLAN ID	The VLAN ID associated with the entry in the MFDB.
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: • **IGMP Snooping** – 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. • **MLD Snooping** – 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. • **GMRP** – Generic Address Resolution Protocol (GARP) Multicast Registration Protocol, which helps help control the flooding of multicast traffic by keeping track of group membership information. • **Static Filtering** – A static MAC filter that was manually added to the address table by an administrator.
Type	The type of entry, which is one of the following: • **Static** – The entry has been manually added to the MFDB by an administrator. • **Dynamic** – The entry has been added to the MFDB as a result of a learning process or protocol.
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 79: GMRP Table

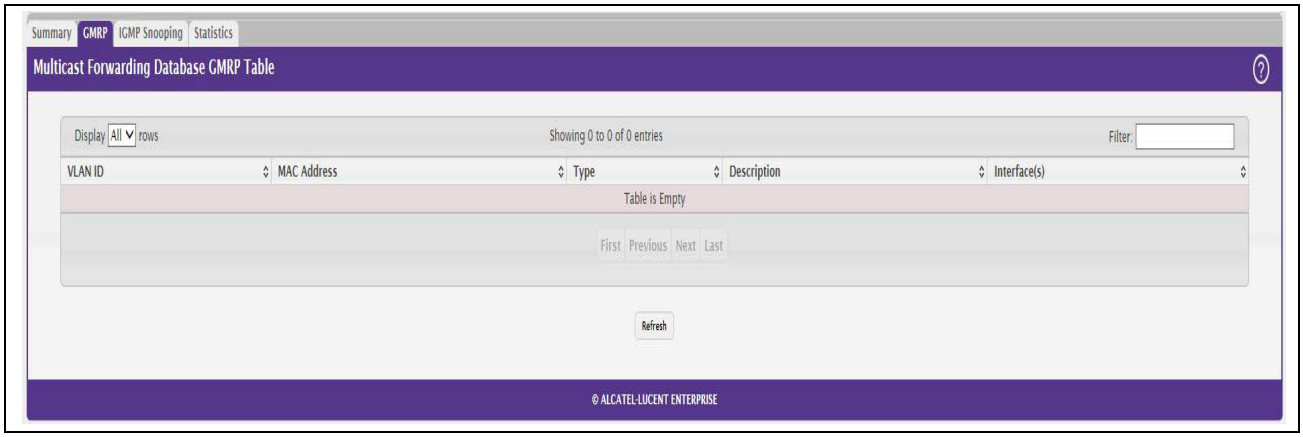


Table 76: GMRP Fields

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: • **Static** – The entry has been manually added to the MFDB by an administrator. • **Dynamic** – 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.
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 80: IGMP Snooping Table

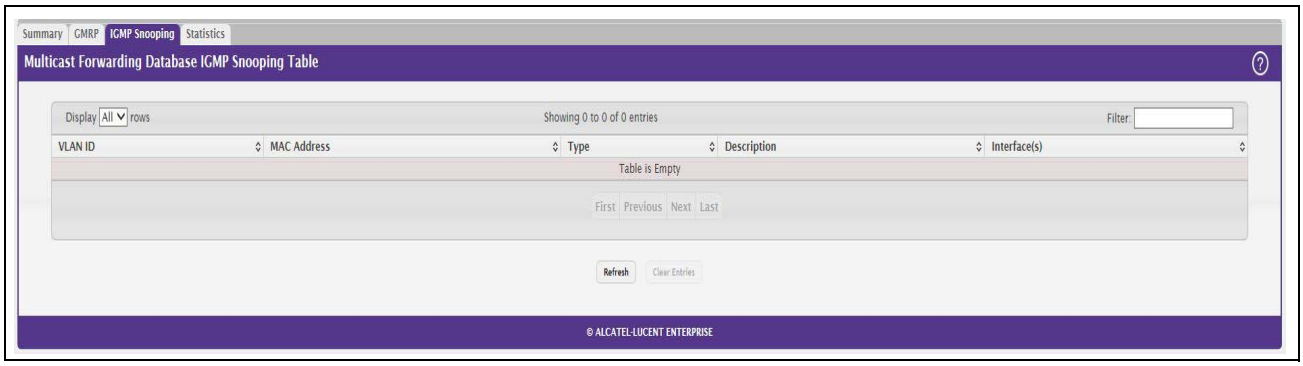


Table 77: IGMP Snooping Fields

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: • **Static** – The entry has been manually added to the MFDB by an administrator. • **Dynamic** – 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.
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.
- Click **Clear Entries** to remove all IGMP snooping entries from the MFDB table. The table is repopulated as new addresses are discovered by the IGMP snooping feature.

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 81: Multicast Forwarding Database Statistics

Table 78: 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.

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 128.

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 82: Spanning Tree Switch Configuration

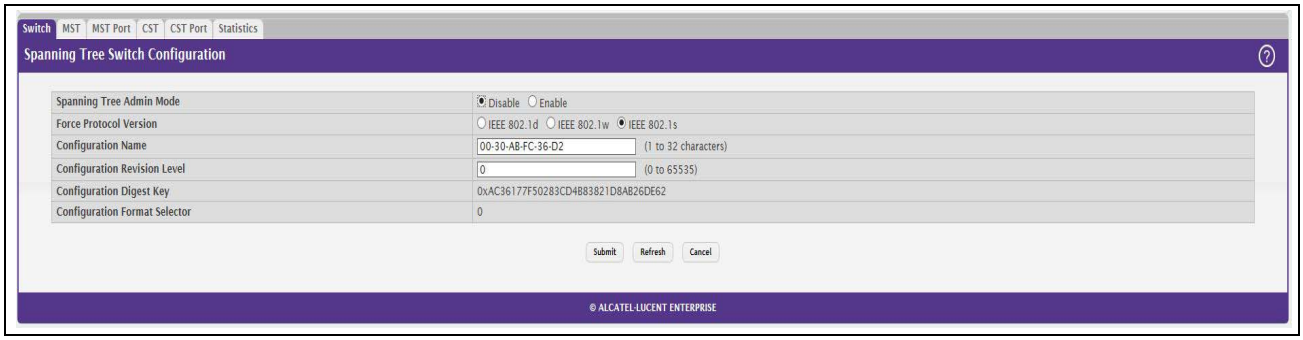


Table 79: Spanning Tree Switch Configuration Fields

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: • **IEEE 802.1d** – Classic STP provides a single path between end stations, avoiding and eliminating loops. • **IEEE 802.1w** – 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. • **IEEE 802.1s** – 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.
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 83: Spanning Tree CST

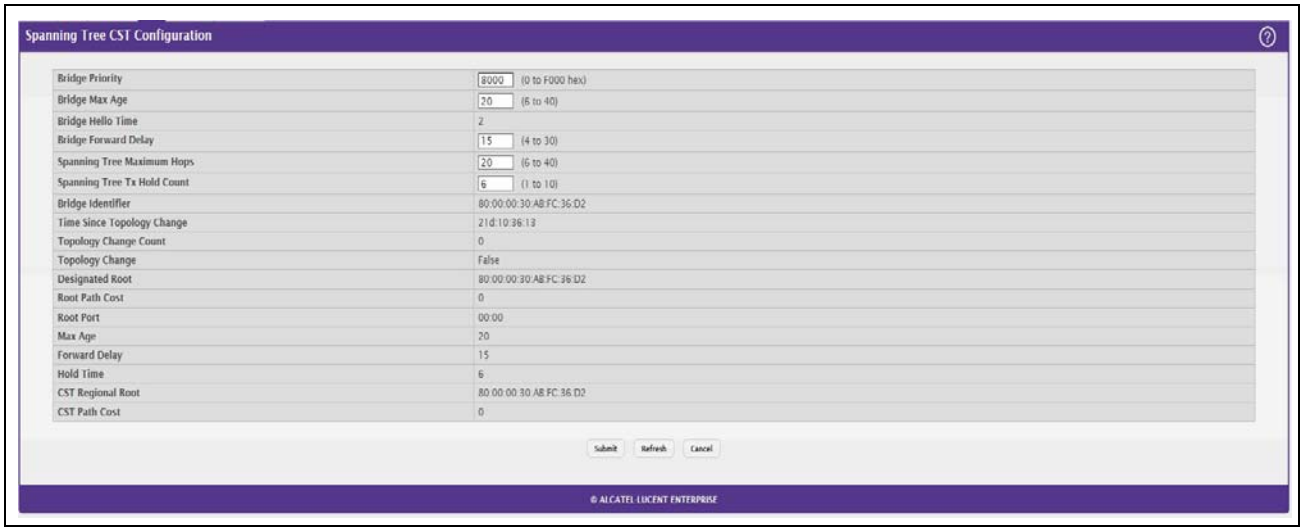


Table 80: Spanning Tree CST Fields

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.

Table 80: Spanning Tree CST Fields (Cont.)

Field	*Description*
Spanning Tree Tx Hold Count	The maximum number of BPDUs that a bridge is allowed to send within a hello time window.
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 84: Spanning Tree CST Port

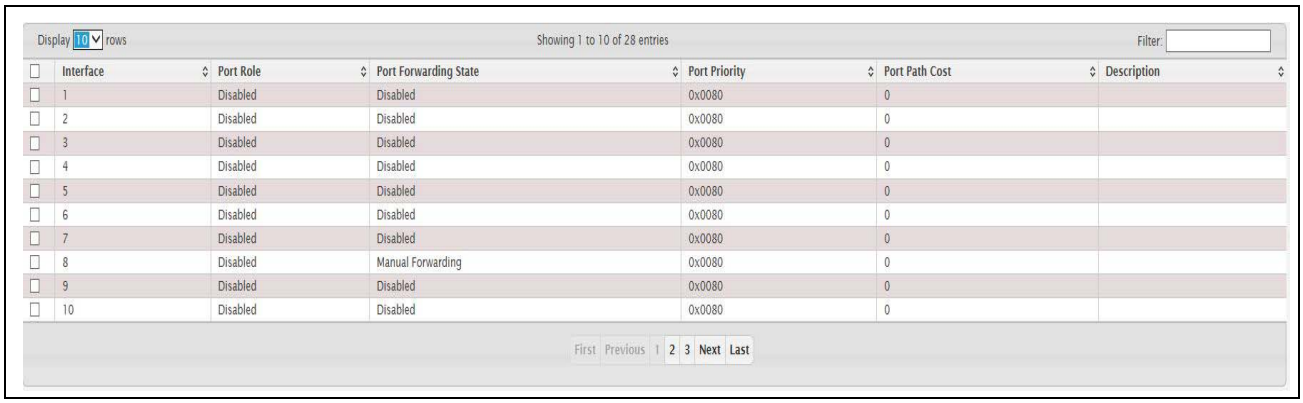


Table 81: Spanning Tree CST Port Fields

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: • **Root** – A port on the non-root bridge that has the least-cost path to the root bridge. • **Designated** – A port that has the least-cost path to the root bridge on its segment. • **Alternate** – A blocked port that has an alternate path to the root bridge. • **Backup** – A blocked port that has a redundant path to the same network segment as another port on the bridge. • **Master** – The port on a bridge within an MST instance that links the MST instance to other STP regions. • **Disabled** – The port is administratively disabled and is not part of the spanning tree.

Table 81: Spanning Tree CST Port Fields (Cont.)

Field	*Description*
Port Forwarding State	• **Blocking** – 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. • **Listening** – 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. • **Learning** – 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. • **Forwarding** – The port sends and receives user traffic. • **Disabled** – The port is administratively disabled and is not part of the spanning tree.
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 **Edit**, 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.

Table 81: Spanning Tree CST Port Fields (Cont.)

Field	*Description*
Designated Root	The bridge ID of the root bridge for the CST.
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 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 **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 85: Spanning Tree MST Summary

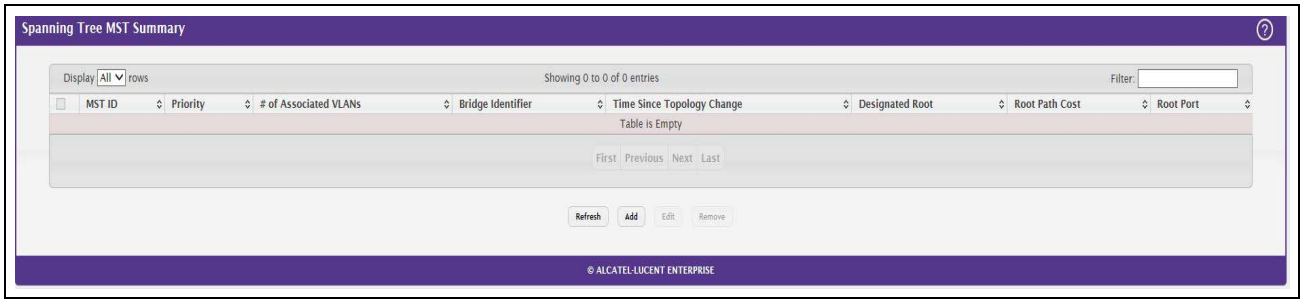


Table 82: Spanning Tree MST Summary Fields

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.

Table 82: Spanning Tree MST Summary Fields (Cont.)

Field	Description
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 86.

Figure 86: Spanning Tree MST Port Configuration

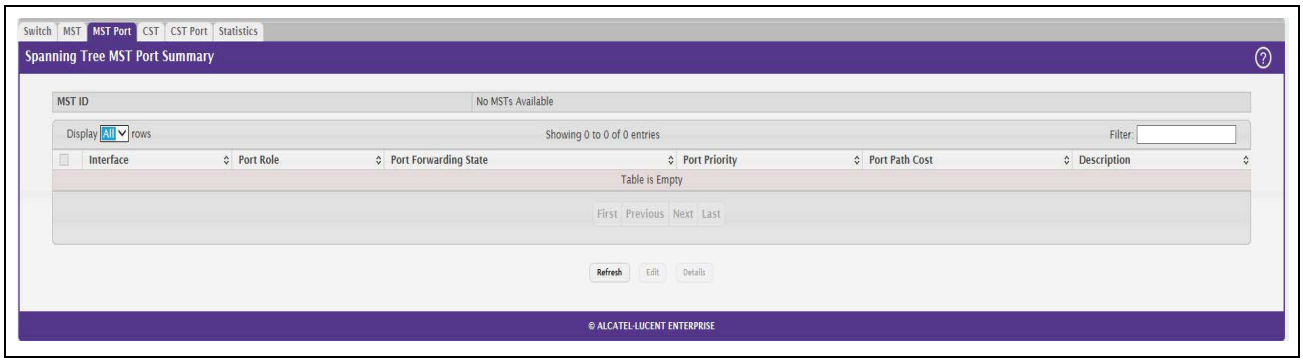


Table 83: Spanning Tree MST Port Configuration Fields

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 83: Spanning Tree MST Port Configuration Fields (Cont.)

Field	*Description*
Port Role	The role of the port within the MST, which is one of the following: • **Root** – A port on the non-root bridge that has the least-cost path to the root bridge. • **Designated** – A port that has the least-cost path to the root bridge on its segment. • **Alternate** – A blocked port that has an alternate path to the root bridge. • **Backup** – A blocked port that has a redundant path to the same network segment as another port on the bridge. • **Master** – The port on a bridge within an MST instance that links the MST instance to other STP regions. • **Disabled** – The port is administratively disabled and is not part of the spanning tree.
Port Forwarding State	• **Blocking** – 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. • **Listening** – 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. • **Learning** – 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. • **Forwarding** – The port sends and receives user traffic. • **Disabled** – The port is administratively disabled and is not part of the spanning tree.
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 **Edit**, 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.

Table 83: Spanning Tree MST Port Configuration Fields (Cont.)

Field	Description
Designated Port	The port ID of the designated port.
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 87: Spanning Tree Statistics

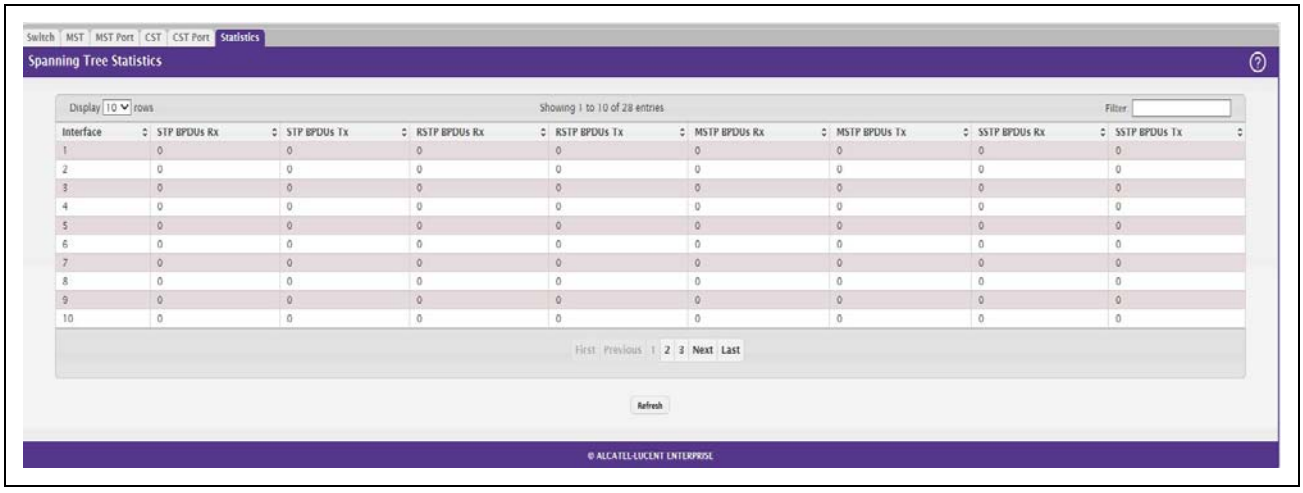


Table 84: Spanning Tree Statistics Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row.
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.

Table 84: Spanning Tree Statistics Fields (Cont.)

Field	Description
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.

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 88: 802.1p Priority Mapping

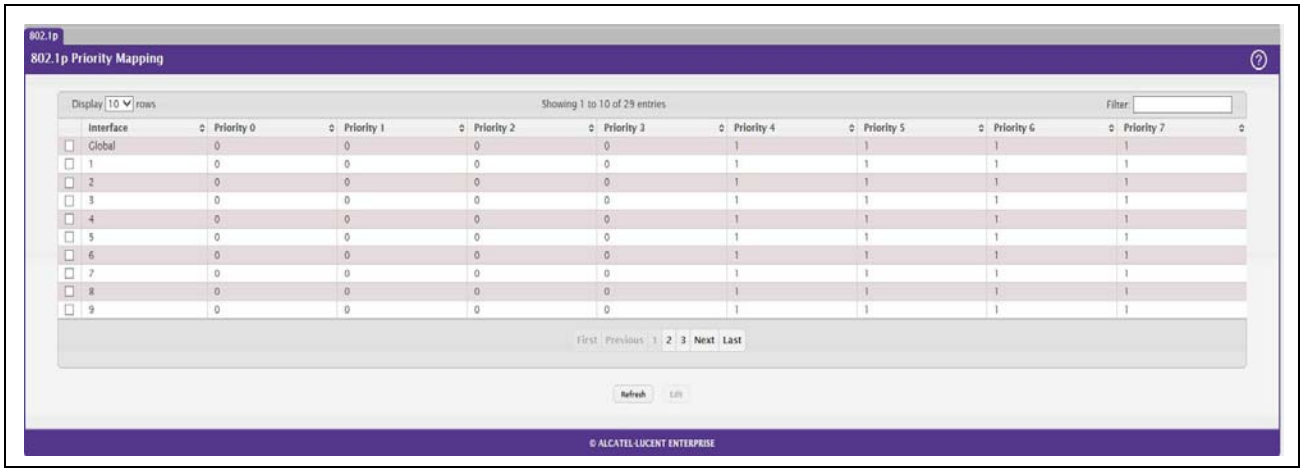


Table 85: 802.1p Priority Mapping

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.

Table 85: 802.1p Priority Mapping (Cont.)

Field	*Description*
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.
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 that 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 “Configuring and Searching the Forwarding Database” on page 38.

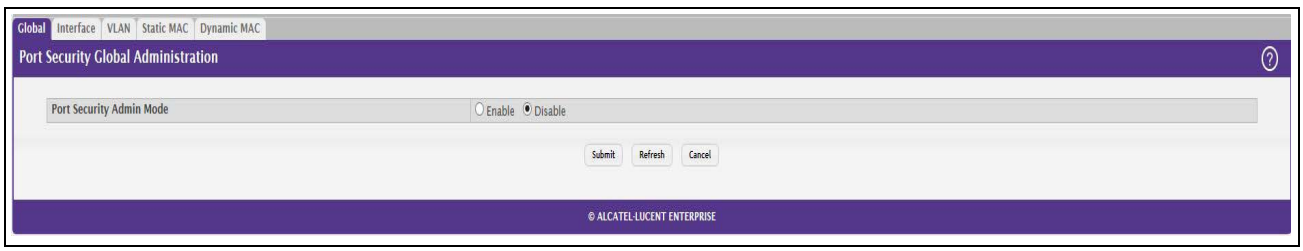
Disabled ports can only be activated from the **Configuring Ports** page.

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 89: Port Security Administration



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 90: Port Security Interface Configuration

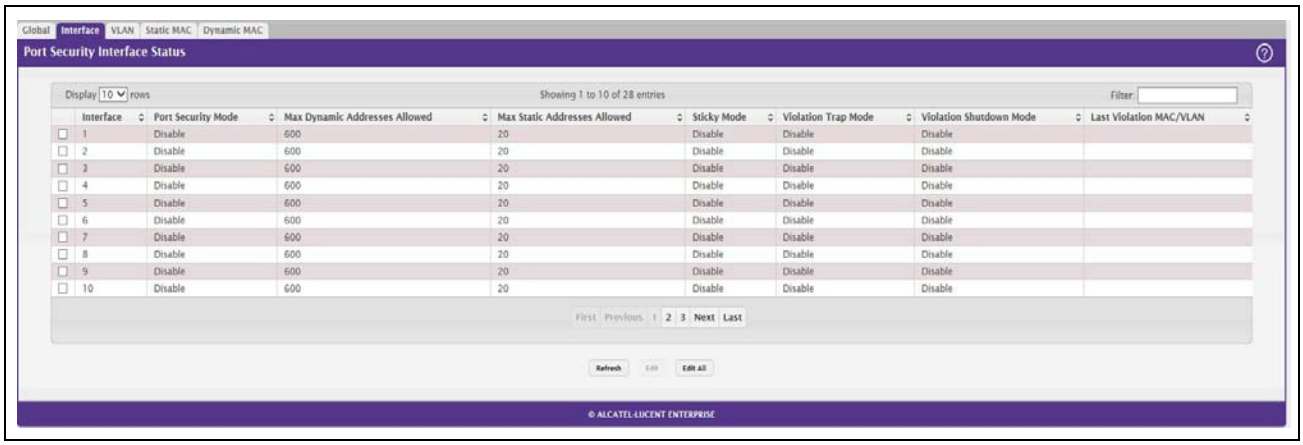


Table 86: Port Security Interface Configuration Fields

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. • **Enable:** Locks the port so that only packets with allowable source MAC addresses can be forwarded. All other packets are discarded. • **Disable:** The port is not locked, so no port security restrictions are applied.
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.

Table 86: Port Security Interface Configuration Fields (Cont.)

Field	Description
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.
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 91: VLAN MAC Locking Status Configuration

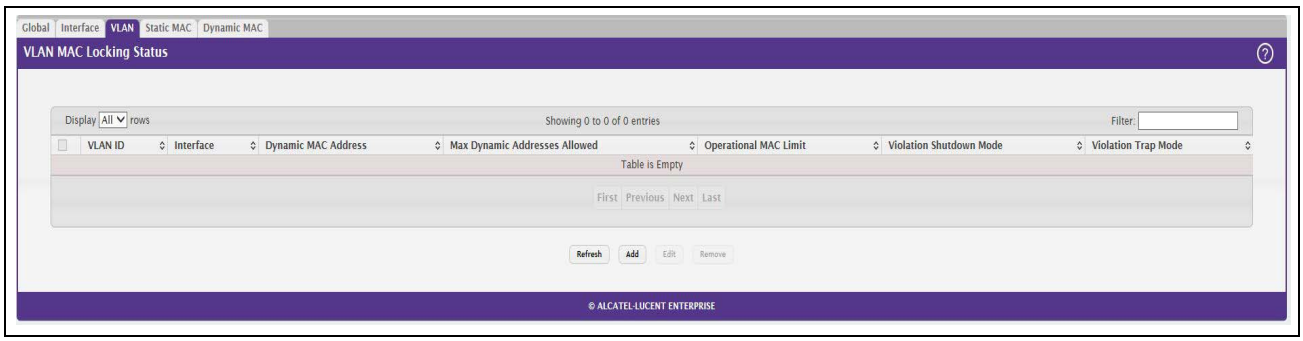


Table 87: Port Security Interface Configuration Fields

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 87: Port Security Interface Configuration Fields (Cont.)

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 92: Port Security Statically Configured MAC Addresses

Table 88: Port Security Statically Configured MAC Address Fields

Field	Description
Interface	Select the physical interface or the LAG on which to view the dynamically learned MAC addresses.

Table 88: Port Security Statically Configured MAC Address Fields (Cont.)

Field	Description
MAC Address	This column lists the static MAC addresses, if any, configured on the selected port.
VLAN ID	Displays the VLAN ID corresponding to the statically configured MAC address.
Delete a static MAC Address	Enter the address of the statically configured MAC address to delete. All MAC addresses that are available to be deleted appear in the MAC Address – VLAN ID table.
VLAN ID	Enter the VLAN ID that corresponds to the statically configured MAC address to delete.

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 93: Port Security Dynamic MAC Address

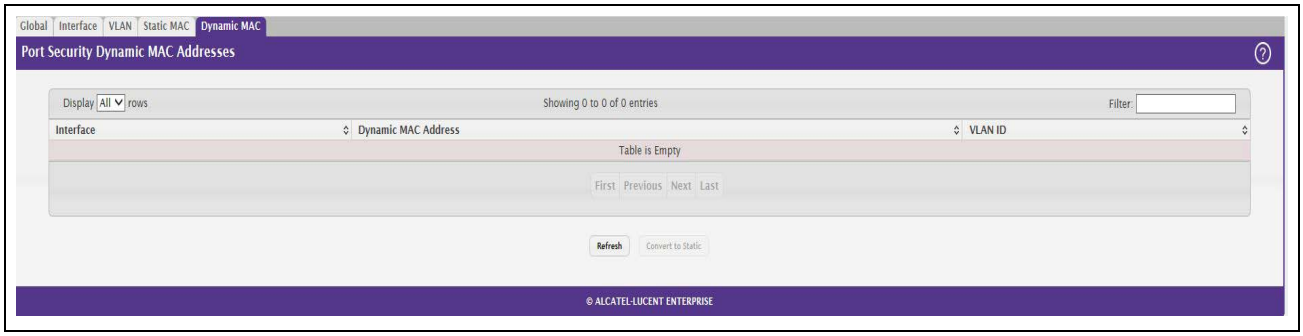


Table 89: Port Security Dynamic Fields

Field	Description
Interface	Select the physical interface or the LAG on which to view the dynamically learned MAC addresses.
MAC Address	This column lists the dynamically learned MAC addresses, if any, on the selected port.
VLAN ID	Displays the VLAN ID corresponding to the dynamically learned MAC address.

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.

OS2220 Websmart 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 94: LLDP Global Configuration

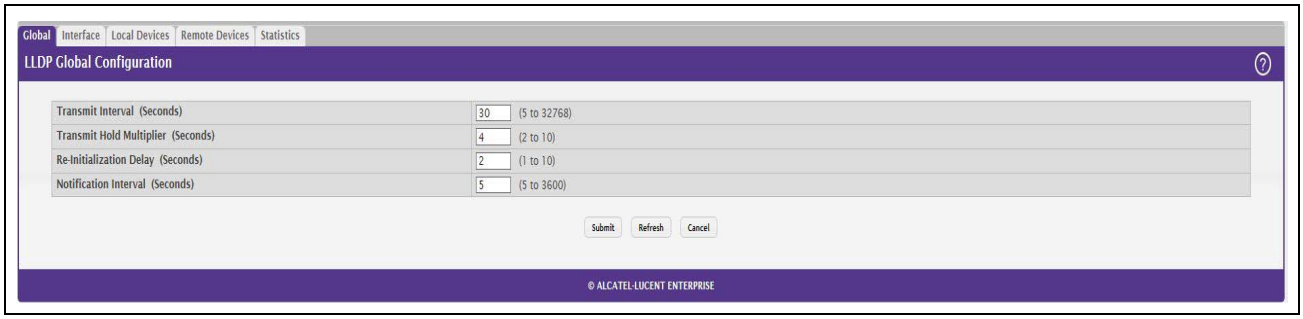


Table 90: LLDP Global Configuration Fields

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.
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.

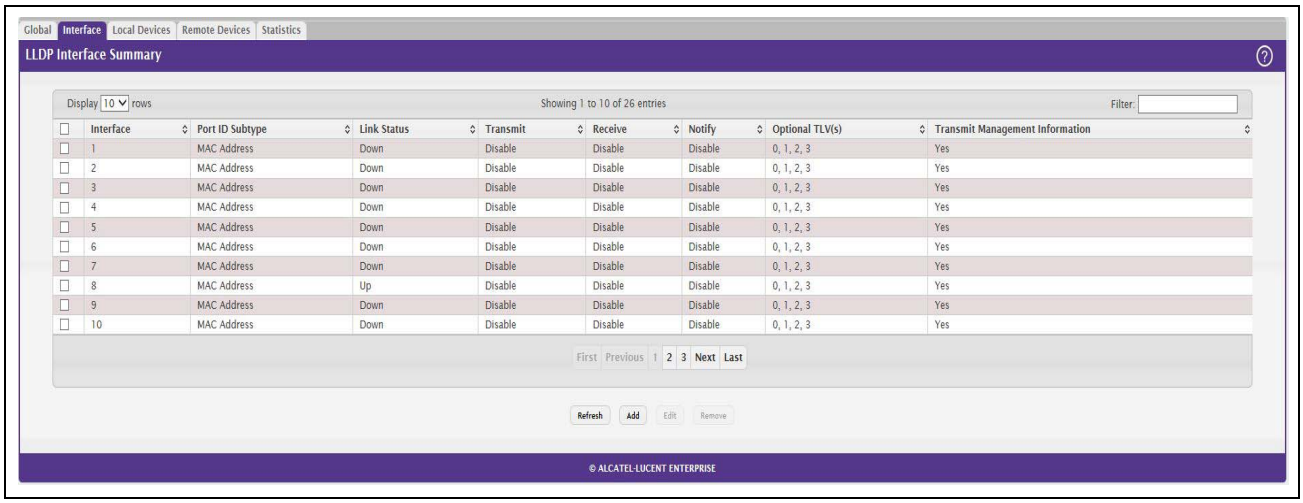
If you make any changes to the page, click **Submit** to apply the new settings to the system.

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 95: 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 91: 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.
Receive	The LLDP receive mode on the interface. If the receive mode is enabled, the device can receive LLDPDUs from other devices.

Table 91: LLDP Interface Summary Fields (Cont.)

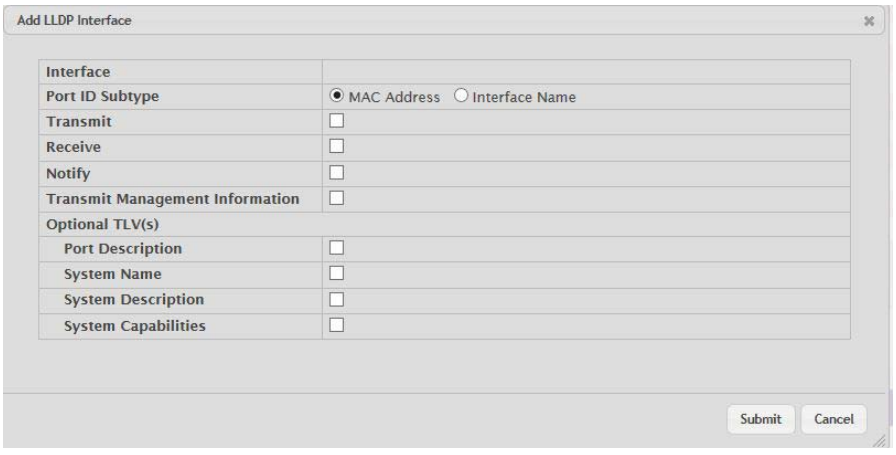
Field	*Description*
Notify	The LLDP remote data change notification status on the interface. If the notify mode is enabled, the interface sends SNMP notifications when a link partner device is added or removed.
Optional TLV(s)	Select each check box next to the type-length value (TLV) information to transmit. Choices include: • **System Name**. To include system name TLV in LLDP frames. To configure the System Name, see "System Description" on page 26. • **System Description**. To include system description TLV in LLDP frames. • **System Capabilities**. To include system capability TLV in LLDP frames. • **Port Description**. To include port description TLV in LLDP frames. To configure the Port Description, see "Port Description" on page 55.
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 96: LLDP Interface Add



In addition to some of the fields that Table 91 describes, Table 92 shows the additional fields available on the Add LLDP Interface window.

Table 92: 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 97: LLDP Local Devices

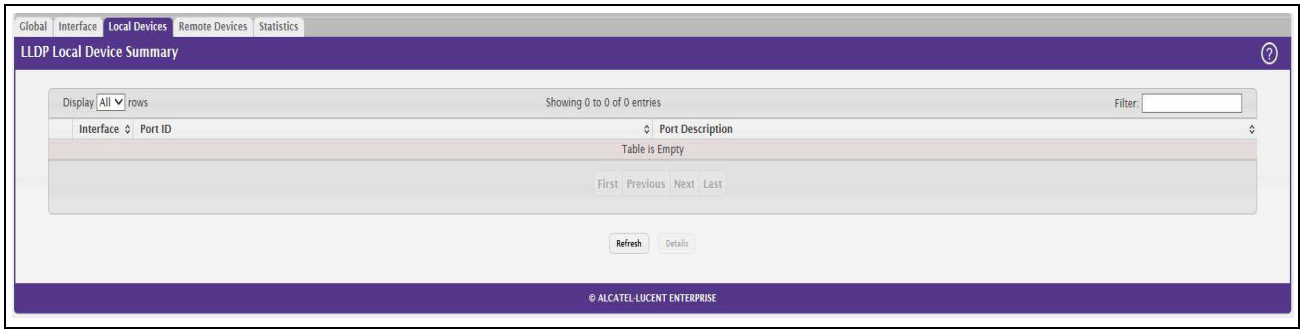


Table 93: LLDP Local Devices Columns

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 94: 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.

Table 94: LLDP Local Devices Details

Field	Description
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 98: LLDP Remote Device Summary

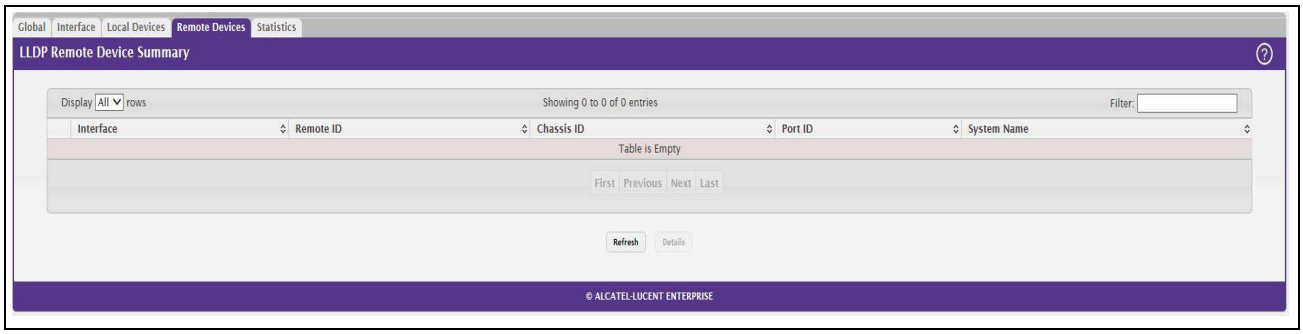


Table 95: LLDP Remote Device Summary Columns

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 96: 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.
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 99: LLDP Statistics

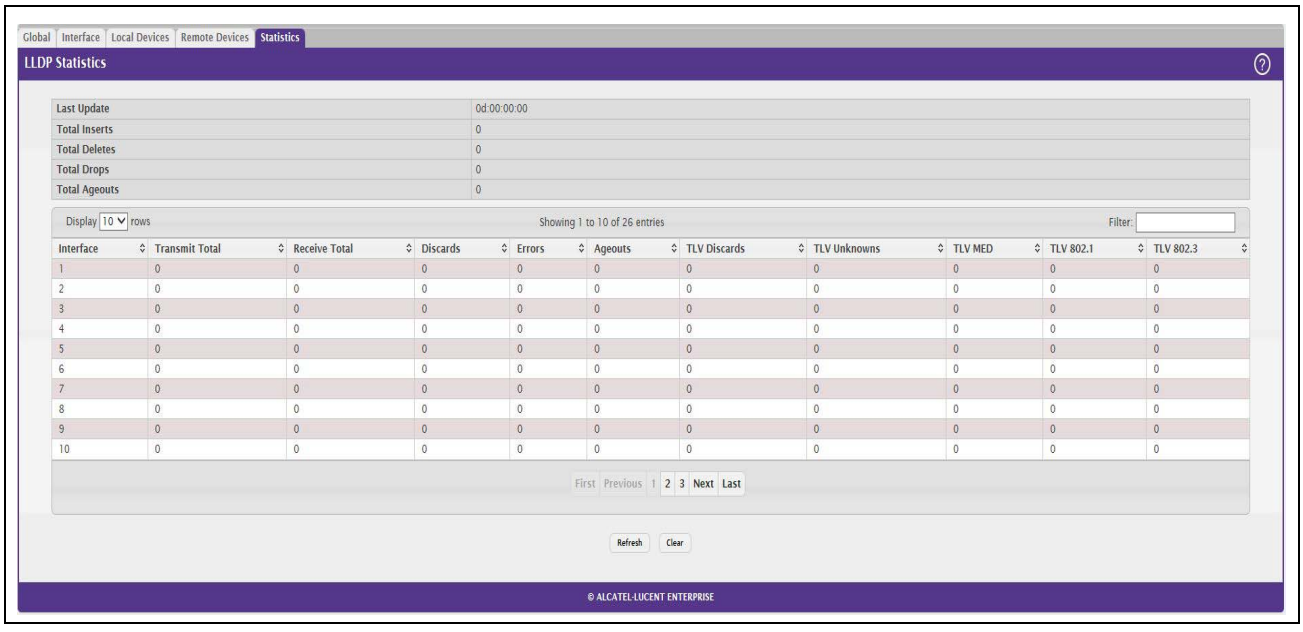


Table 97: LLDP Statistics Fields

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.
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 and Layer 2 Priority 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 100: LLDP-MED Global Configuration

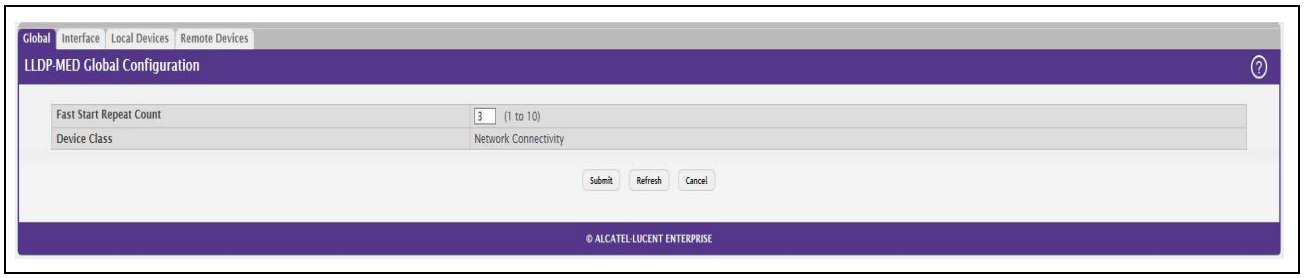


Table 98: LLDP Global Configuration Fields

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 s 3.
Device Class	Specifies local device's MED Classification. The following three represent the actual endpoints: • Class I Generic [IP Communication Controller etc.] • Class II Media [Conference Bridge etc.] • Class III Communication [IP Telephone etc.]) 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 updated 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 101: LLDP-MED Interface Summary

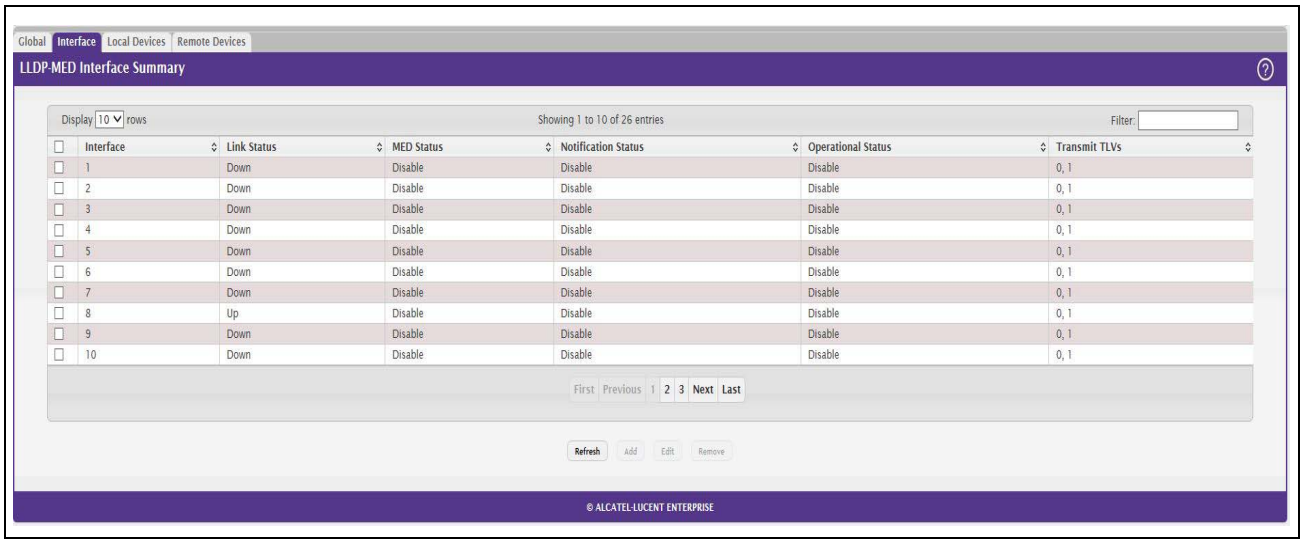


Table 99: LLDP-MED Interface Configuration Fields

Field	*Description*
Interface	Selects the port that you want to configure LLDP-MED—802.1AB on. You can select **All** 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 checkboxes 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: • MED Capabilities: 0 • Network Policy: 1

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 LLPD-MED information advertised on the selected local interface. To display this page, click **Switching > LLDP-MED > Local Devices** in the navigation menu.

Figure 102: LLPD-MED Local Device Summary

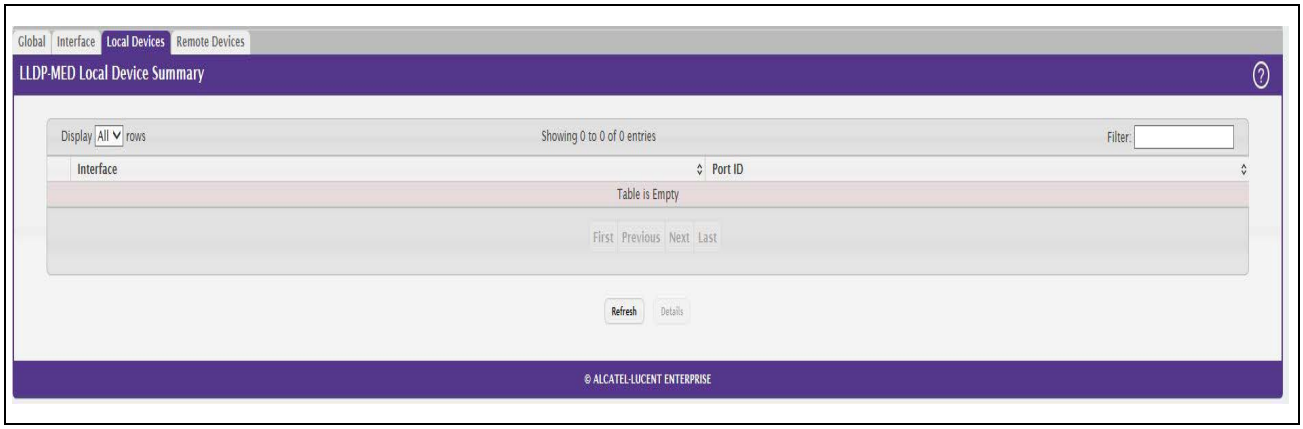


Table 100: LLPD-MED Local Device Information Fields

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 **Details**, 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, streammingvideo, 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.

Table 100: LLPD-MED Local Device Information Fields (Cont.)

Field	Description
Tagged Bit Status	Identifies whether the network policy is defined for tagged or untagged VLANs.
Location Information	
Sub Type	The type of location information: • **Coordinate Based** – The location map coordinates (latitude, longitude and altitude) of the device. • **Civic Address** – The civic or street address location of the device. • **ELIN** – The Emergency Call Service (ECS) Emergency Location Identification Number (ELIN) of the device.
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 103: LLDP Remote Device Summary

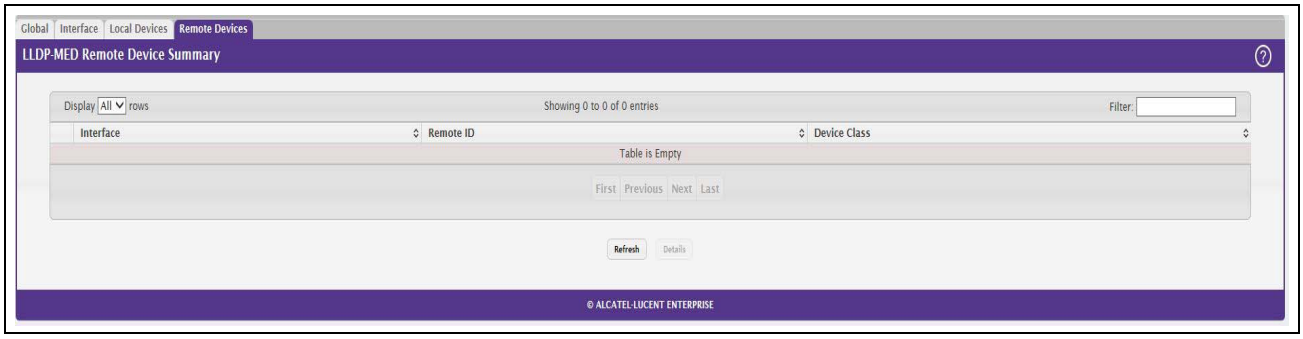


Table 101: LLPD-MED Remote Device Information Fields

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.
Enabled Capabilities	The supported capabilities on the remote device that are also enabled.

Table 101: LLPD-MED Remote Device Information Fields (Cont.)

Field	*Description*
Device Class	The MED Classification advertised by the TLV from the remote device. The following three classifications represent the actual endpoints: • Class I Generic (for example, IP Communication Controller) • Class II Media (for example, Conference Bridge) • Class III Communication (for example, IP Telephone) 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, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, 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 subtype.
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 104: Loop Protection Configuration

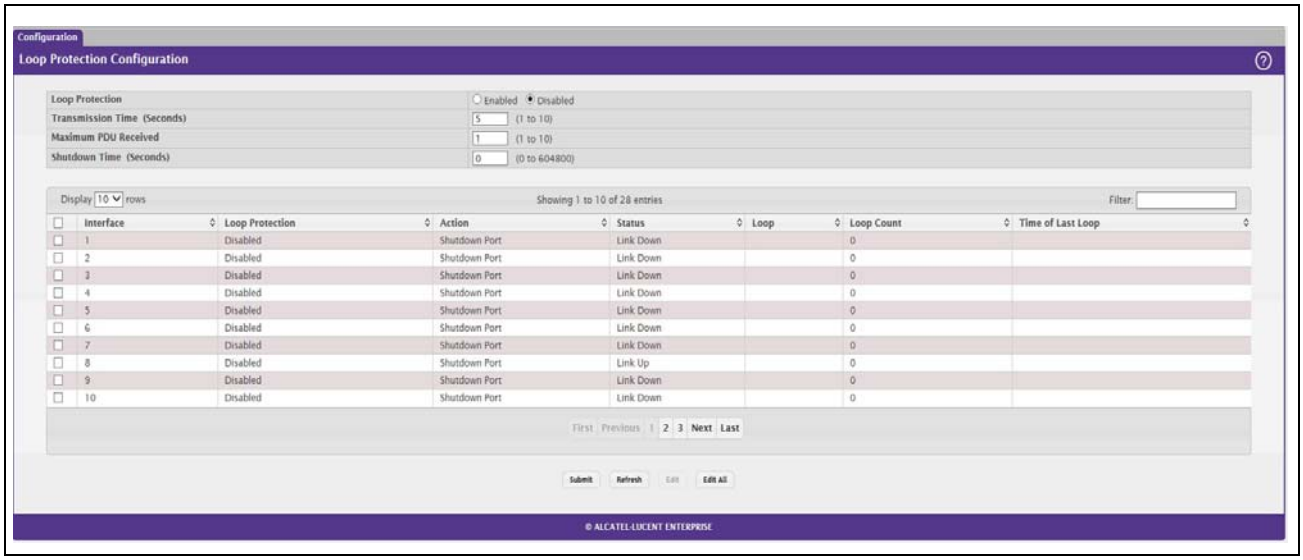
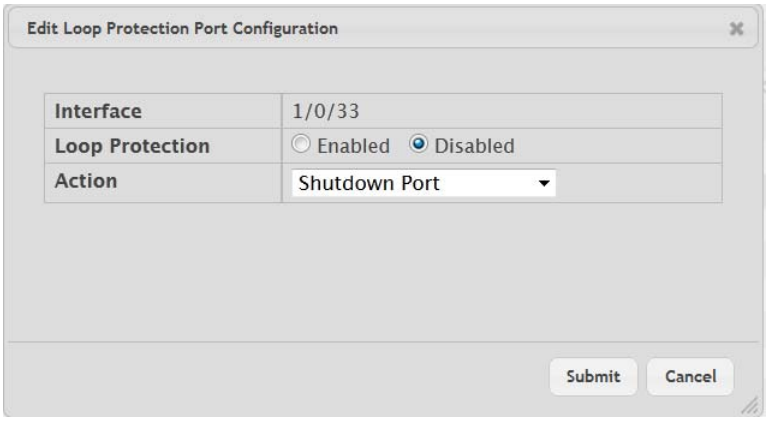


Table 102: Loop Protection Configuration Fields

Field	*Description*
Loop Protection	Enables or disables the loop protection feature globally on the switch. ***Note:*** 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.

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.



Action	The action to be taken when a loop is detected on the port: • **Shutdown Port**: Shut down the port for the configured **Transmission Time**. • **Shutdown Port and Log**: Shut down the port for the configured **Transmission Time** and send a message to the system log. • **Log Only**: Send a message to the system log but do not shut down the port.
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.
Time of Last Loop	The date and time the most recent loop was detected.

Click **Submit** to updated the switch. The changes take effect but will not be retained across a power cycle unless a save is performed.

Section 5: 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. The Security folder contains links to the following features:

- Port Access Control
- RADIUS Settings

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 105: Port Access Control—Port Configuration

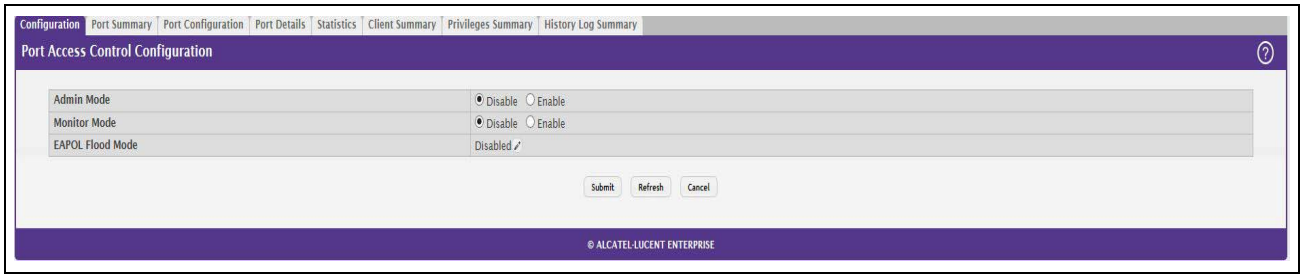


Table 103: Port Access Control—Port Configuration Fields

Field	*Description*
Administrative Mode	Select **Enable** or **Disable** 802.1x mode on the switch. The default is Disable. This feature permits port-based authentication on the switch.
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.

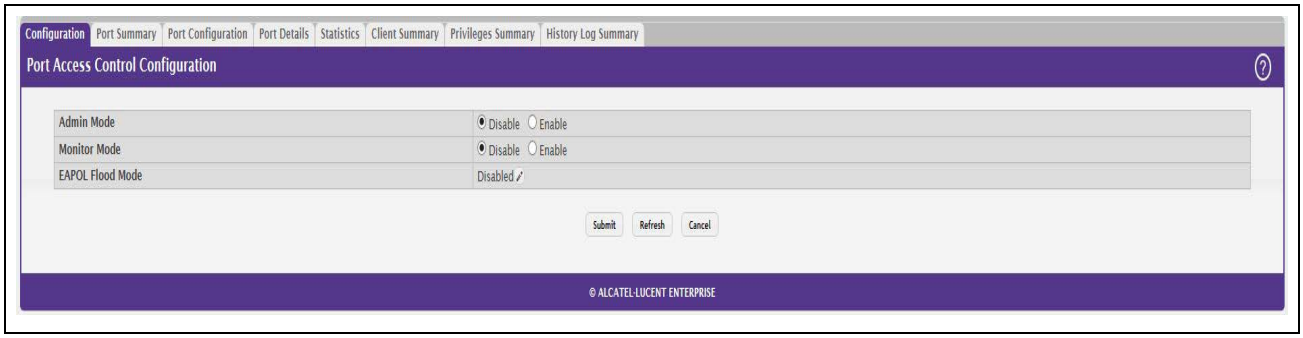
If you change the mode, click **Submit** to apply the new settings to the system.

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 106: Port Access Control—Port Summary



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.
- 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.

Table 104: Port Access Control—Port Summary Fields

Field	*Description*
Interface	The interface associated with the rest of the data in the row.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: • **Authenticator** – 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. • **Supplicant** – The port must be granted permission by the authentication server before it can access the remote authenticator port.
Control Mode	The port-based access control mode configured on the port, which is one of the following: • **Auto** – The port is unauthorized until a successful authentication exchange has taken place. • **Force Unauthorized** – The port ignores supplicant authentication attempts and does not provide authentication services to the client. • **Force Authorized** – The port sends and receives normal traffic without client port-based authentication. • **MAC-Based** – This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses.

Table 104: Port Access Control—Port Summary Fields (Cont.)

Field	*Description*
Operating Control Mode	The control mode under which the port is actually operating, which is one of the following: • **Auto** • **Force Unauthorized** • **Force Authorized** • **MAC-Based** • **N/A** If the mode is N/A, port-based access control is not applicable to the port. If the port is in detached state it cannot participate in port access control. Additionally, if port-based access control is globally disabled, the status for all ports is N/A.
PAE State	The current state of the authenticator PAE state machine, which is the 802.1X process that controls access to the port. The state can be one of the following: • **Initialize** • **Disconnected** • **Connecting** • **Authenticating** • **Authenticated** • **Aborting** • **Held** • **ForceAuthorized** • **ForceUnauthorized**
Backend State	The current state of the back-end authentication state machine, which is the 802.1X process that controls the interaction between the 802.1X client on the local system and the remote authentication server. The state can be one of the following: • **Request** • **Response** • **Success** • **Fail** • **Timeout** • **Initialize** • **Idle**
Initialize (Icon)	Click the Initialize icon to reset the 802.1X state machine on the associated interface to the initialization state. Traffic sent to and from the port is blocked during the authentication process. This icon can be clicked only when the port is an authenticator and the operating control mode is Auto.
Re-Authenticate (Icon)	Click the Re-Authenticate icon to force the associated interface to restart the authentication process.

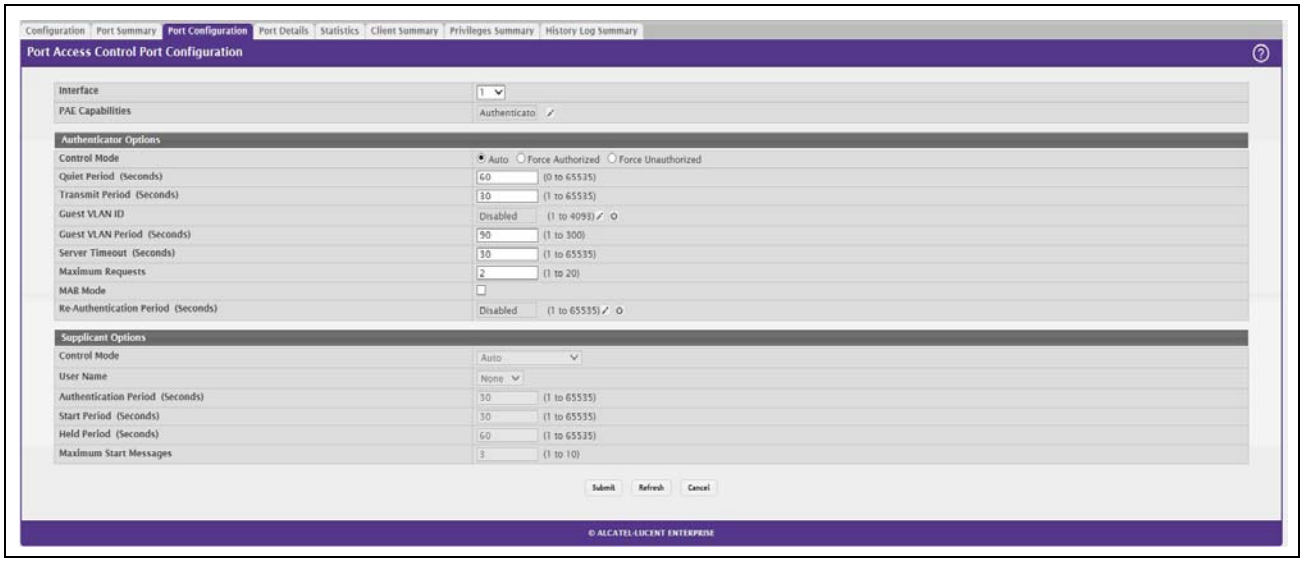
If you change the mode, click **Submit** to apply the new settings to the system.

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 107: Port Access Control Port Configuration



Use the buttons to perform the following tasks:

- To configure the port-based access control settings for one or more ports, select each port to configure and click **Edit**. The same settings are applied to all selected ports.
- 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**.

Table 105: 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.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: • **Authenticator** – 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. • **Supplicant** – 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. To change the PAE capabilities of a port, click the **Edit** icon associated with the field and select the desired setting from the menu in the Set PAE Capabilities window.

Table 105: Port Access Control Port Configuration Fields (Cont.)

Field	*Description*
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).
• **Control Mode**	The port-based access control mode on the port, which is one of the following: • **Auto** – The port is unauthorized until a successful authentication exchange has taken place. • **Force Unauthorized** – The port ignores supplicant authentication attempts and does not provide authentication services to the client. • **Force Authorized** – The port sends and receives normal traffic without client **port-based authentication.**
• **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.
• **Guest VLAN ID**	The value, in seconds, of the timer used for guest VLAN authentication.
• **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.
• **Re-Authentication Period**	The amount of time that clients can be connected to the port without being reauthenticated. If this field is disabled, connected clients are not forced to reauthenticate periodically. To change the value, click the **Edit** icon associated with the field and specify a value in the available field. To reset the reauthentication period to the default value, click the Reset icon associated with the field and confirm the action.
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: • **Auto** – The port is in an unauthorized state until a successful authentication exchange has taken place between the supplicant port, the authenticator port, and the authentication server. • **Force Unauthorized** – The port is placed into an unauthorized state and is automatically denied system access. • **Force Authorized** – The port is placed into an authorized state and does not require client port-based authentication to be able to send and receive traffic.
• **User Name**	The name the port uses to identify itself as a supplicant to the authenticator port. The menu includes the users that are configured for system management. When authenticating, the supplicant provides the password associated with the selected User Name.
• **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.

Table 105: Port Access Control Port Configuration Fields (Cont.)

Field	Description
• **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.

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 108: Port Access Control Port Details

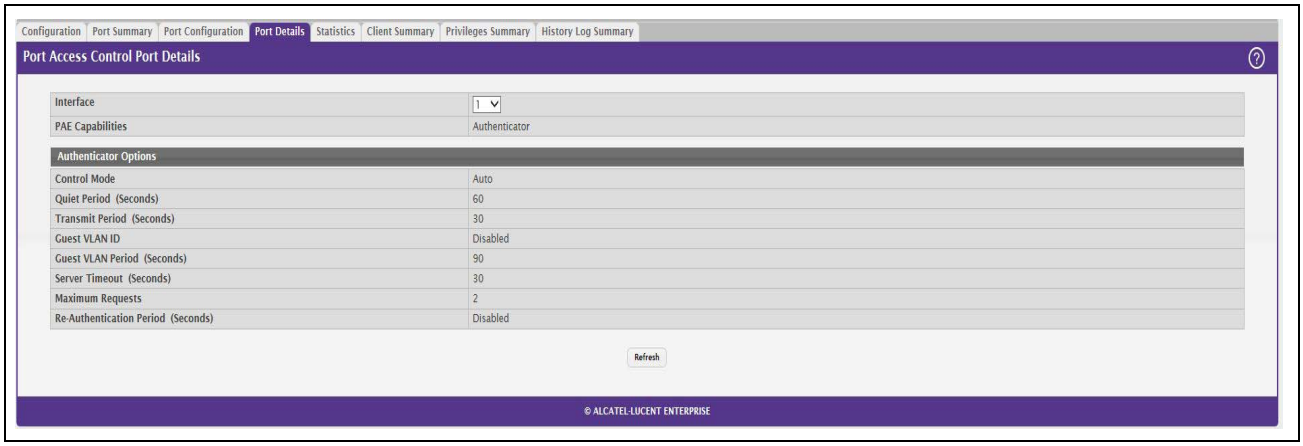


Table 106: Port Access Control Port Details Fields

Field	Description
Interface	The interface associated with the rest of the data on the page.

Table 106: Port Access Control Port Details Fields (Cont.)

Field	*Description*
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: • **Authenticator** – 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. • **Supplicant** – 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.
Authenticator Options	The fields in this section provide information about the settings that apply to the port when it is configured as an 802.1X authenticator.
• **Control Mode**	The port-based access control mode on the port, which is one of the following: • **Auto** – The port is unauthorized until a successful authentication exchange has taken place. • **Force Unauthorized** – The port ignores supplicant authentication attempts and does not provide authentication services to the client. • **Force Authorized** – The port sends and receives normal traffic without client port-based authentication.
• **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.
• **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.
• **Guest VLAN Period**	The value, in seconds, of the timer used for guest VLAN authentication.
• **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.
• **Re-Authentication Period**	The amount of time that clients can be connected to the port without being reauthenticated. If this field is disabled, connected clients are not forced to reauthenticate periodically.
• **Logical Port**	The logical port number associated with the supplicant that is connected to the port.
• **Supplicant MAC Address**	The MAC address of the supplicant that is connected to the port.
• **Authenticator PAE State**	The current state of the authenticator PAE state machine, which is the 802.1X process that controls access to the port. The state can be one of the following: • **Initialize** • **Disconnected** • **Connecting** • **Authenticating** • **Authenticated** • **Aborting** • **Held** • **ForceAuthorized** • **ForceUnauthorized**

Table 106: Port Access Control Port Details Fields (Cont.)

Field	*Description*
• **Backend Authentication State**	The current state of the backend authentication state machine, which is the 802.1X process that controls the interaction between the 802.1X client on the local system and the remote authentication server. The state can be one of the following: • **Request** • **Response** • **Success** • **Fail** • **Timeout** • **Initialize** • **Idle**
• **VLAN Assigned**	The ID of the VLAN the supplicant was placed in as a result of the authentication process.
• **VLAN Assigned Reason**	The reason why the authenticator placed the supplicant in the VLAN. Possible values are: • **RADIUS** • **Default** • **Not Assigned**
Supplicant Options	The fields in this section provide information about the settings that apply to the port when it is configured as an 802.1X supplicant.
• **Control Mode**	The port-based access control mode on the port, which is one of the following: • **Auto** – The port is in an unauthorized state until a successful authentication exchange has taken place between the supplicant port, the authenticator port, and the authentication server. • **Force Unauthorized** – The port is placed into an unauthorized state and is automatically denied system access. • **Force Authorized** – The port is placed into an authorized state and does not require client port-based authentication to be able to send and receive traffic.
• **User Name**	The name the port uses to identify itself as a supplicant to the authenticator port. The menu includes the users that are configured for system management. When authenticating, the supplicant provides the password associated with the selected User Name.
• **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 109: Port Access Control Statistics

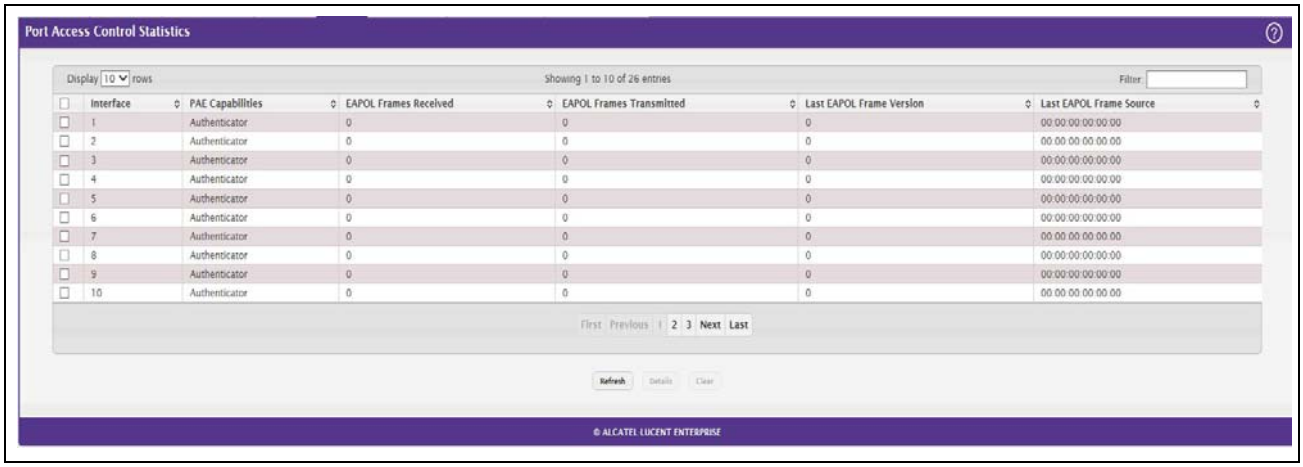


Table 107: Port Access Control Statistics Fields

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: • **Authenticator** – 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. • **Supplicant** – The port must be granted permission by the authentication server before it can access the remote authenticator port.
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	
After you click **Details**, 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 107: Port Access Control Statistics Fields (Cont.)

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.

Client Summary

This page displays information about supplicant devices that are connected to the local authenticator ports. If there are no active 802.1X sessions, the table is empty. To view additional information about a supplicant, select the interface it is connected to and click **Details**.

To access the Port Access Control Client Summary page, click **Security > Port Access Control > Client Summary** in the navigation menu.

Figure 110: Port Access Control Client Summary

Table 108: Port Access Control Client Summary Fields

Field	*Description*
Interface	The local 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.
Logical Interface	The logical port number associated with the supplicant that is connected to the port.
User Name	The name the client uses to identify itself as a supplicant to the authentication server.
Supp MAC Address	The MAC address of the supplicant that is connected to the port.
Session Time	The amount of time that has passed since the connected supplicant was granted access to the network through the authenticator port.
Filter ID	The policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID	The ID of the VLAN the supplicant was placed in as a result of the authentication process.
After you click Details, a window opens and displays additional information about the client. The following information describes the additional fields that appear in the window.	
Session Timeout	The reauthentication timeout period set by the RADIUS server to the supplicant device.
Session Termination Action	The termination action set by the RADIUS server that indicates the action that will take place once the supplicant reaches the session timeout value.

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 111: Port Access Control Privileges Summary

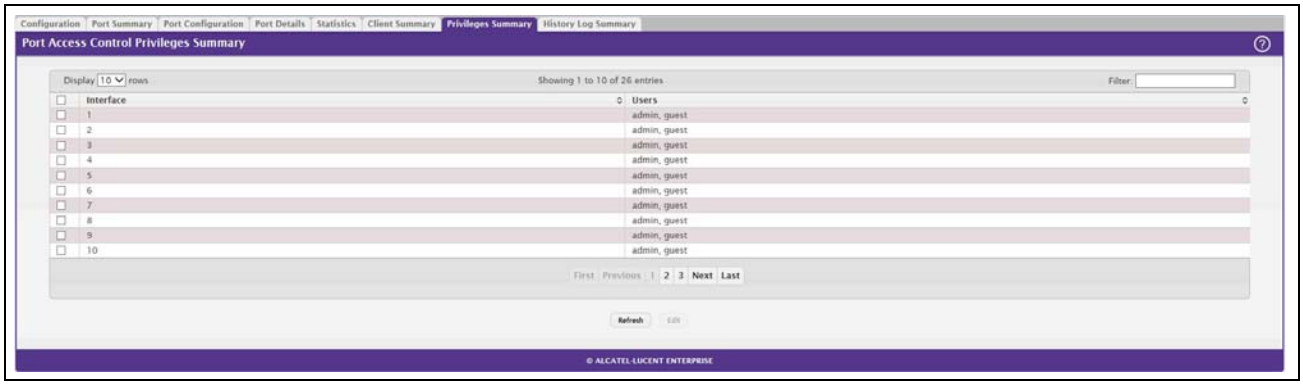


Table 109: Port Access Control Privileges Summary Fields

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.

History Log 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 History Log Summary page, click **Security > Port Access Control > History Log Summary** in the navigation menu.

Figure 112: Port Access Control History Log Summary

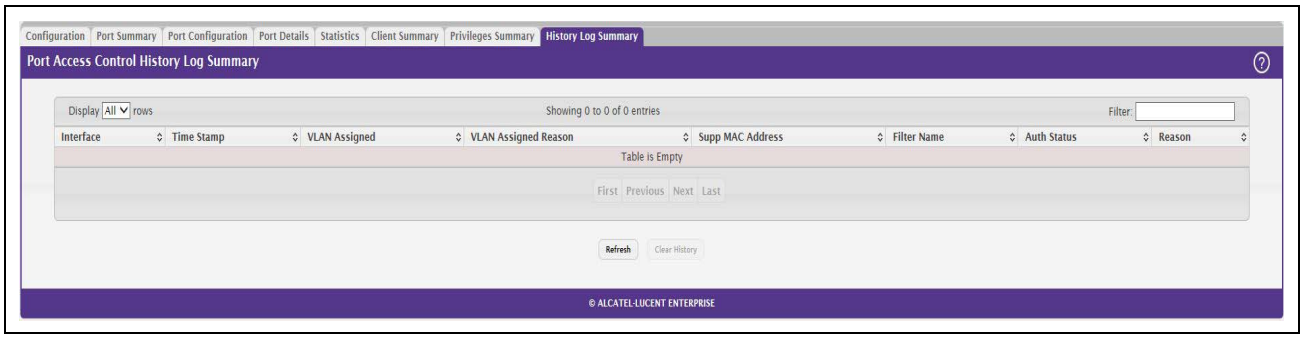


Table 110: Port Access Control History Log Summary Fields

Field	*Description*
Interface	The interface associated with the rest of the data in the row. Only interfaces that have entries in the log history are listed.
Time Stamp	The absolute time when the authentication event took place.
VLAN Assigned	The ID of the VLAN the supplicant was placed in as a result of the authentication process.
VLAN Assigned Reason	The reason why the authenticator placed the supplicant in the VLAN. Possible values are: • **RADIUS** • **Default** • **Not Assigned**
Supp MAC Address	The MAC address of the supplicant that is connected to the port.
Filter Name	The policy filter ID assigned by the authenticator to the supplicant device.
Auth Status	The authentication status of the client or port.
Reason	The reason for the successful or unsuccessful authentication.

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:

- Web 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 113: RADIUS Configuration

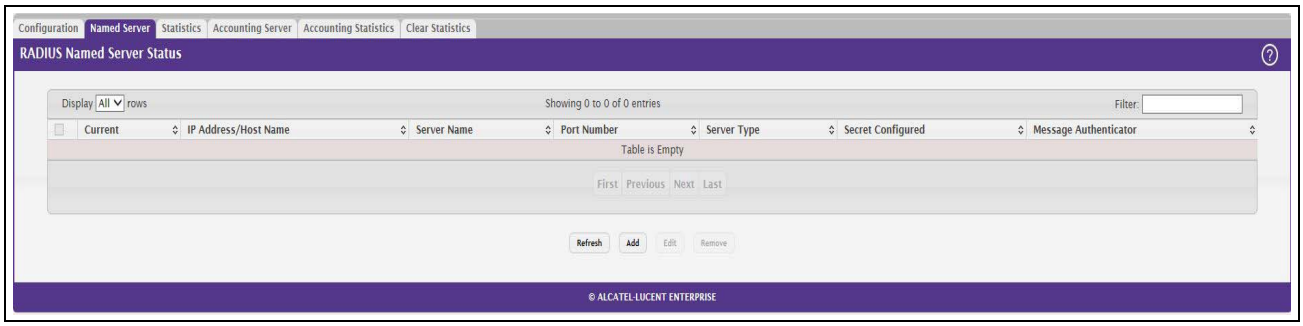


Table 111: RADIUS Configuration Fields

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.

Table 111: RADIUS Configuration Fields (Cont.)

Field	*Description*
NAS-IP Address	The network access server (NAS) IP address for the RADIUS server. To specify an address, click the **Edit** 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.

Use the buttons at the bottom of the page to perform the following actions:

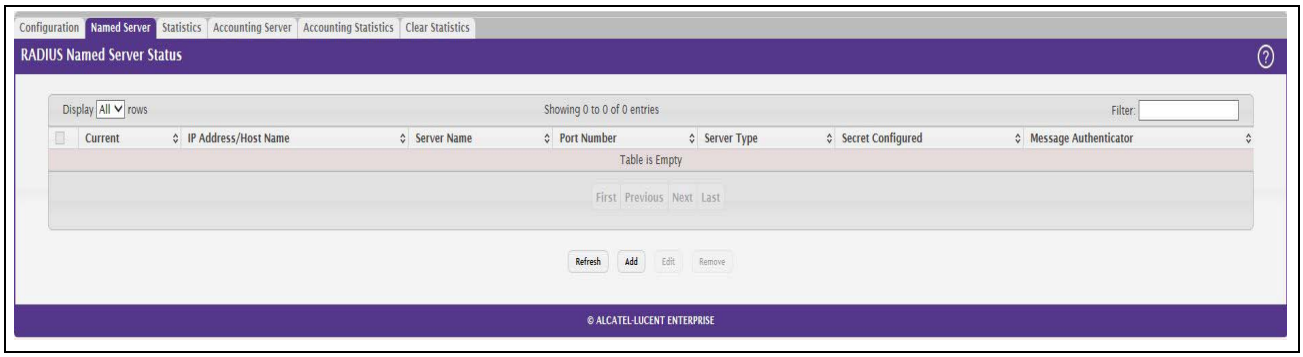
- Click **Refresh** to update the page with the most current information.
- If you make changes to the page, click **Submit** to apply the changes to the system.

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 114: 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 112: 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 115: RADIUS Server Statistics

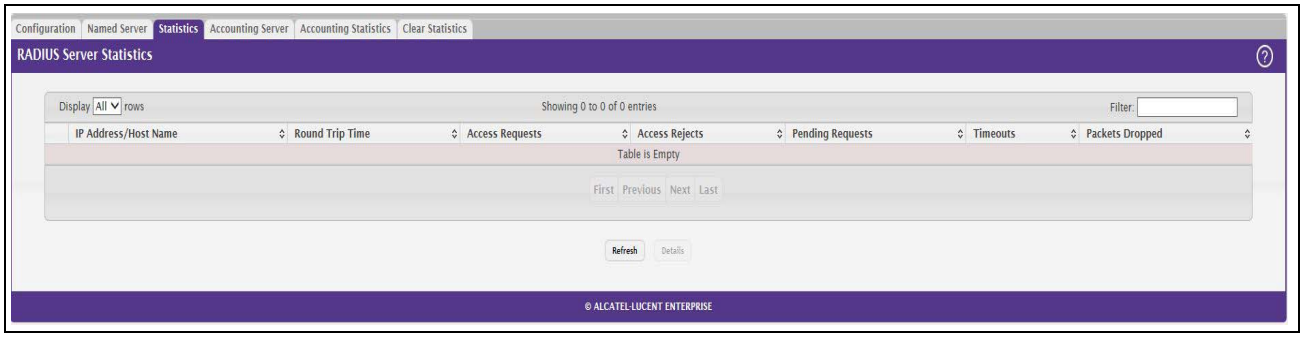


Table 113: RADIUS Server Statistics Fields

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.
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.

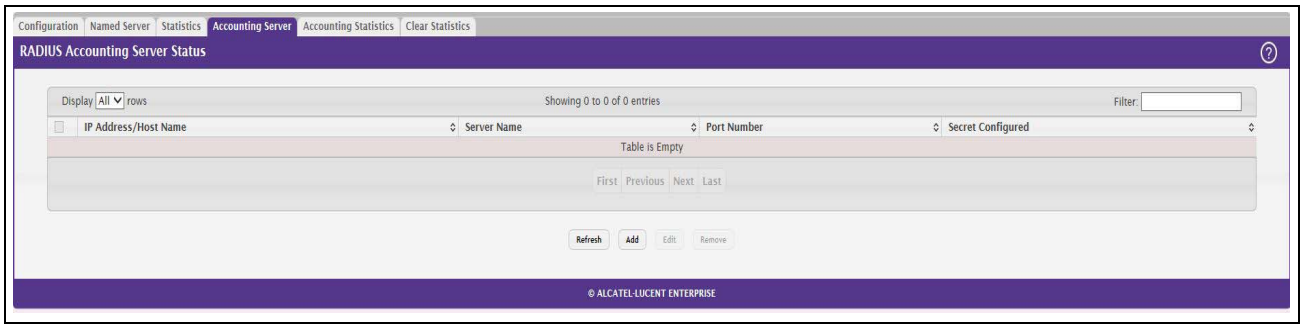
Click **Refresh** to update the page with the most current information.

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 116: 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 114: 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 RAIDUS 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 117: RADIUS Accounting Statistics

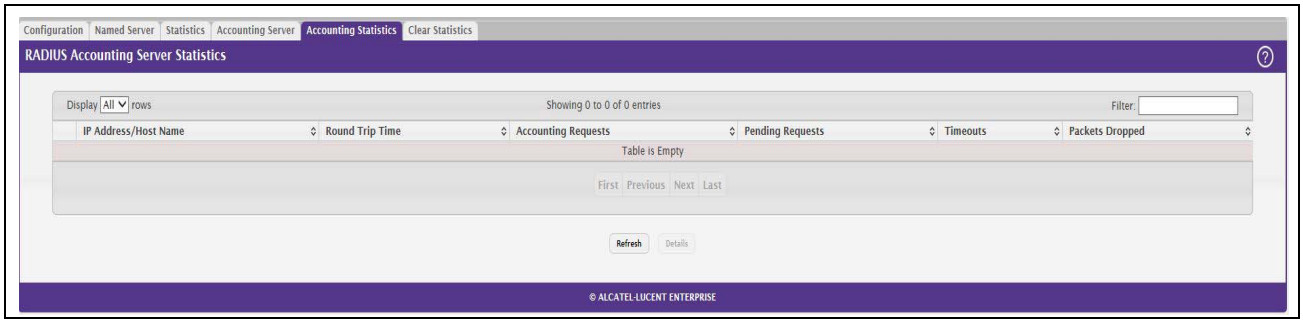


Table 115: RADIUS Accounting Statistics Fields

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.
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.

Table 115: RADIUS Accounting Statistics Fields (Cont.)

Field	Description
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 118: 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.

Section 6: 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. This section contains the following subsections:

- Configuring Access Control Lists
- Configuring Class of Service
- Configuring Auto VoIP

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 FATPATH 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. OS2220 Websmart software supports IPv4 and MAC ACLs. The total number of MAC and IP ACLs supported by OS2220 Websmart software is platform-specific.

You first create an IPv4-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:

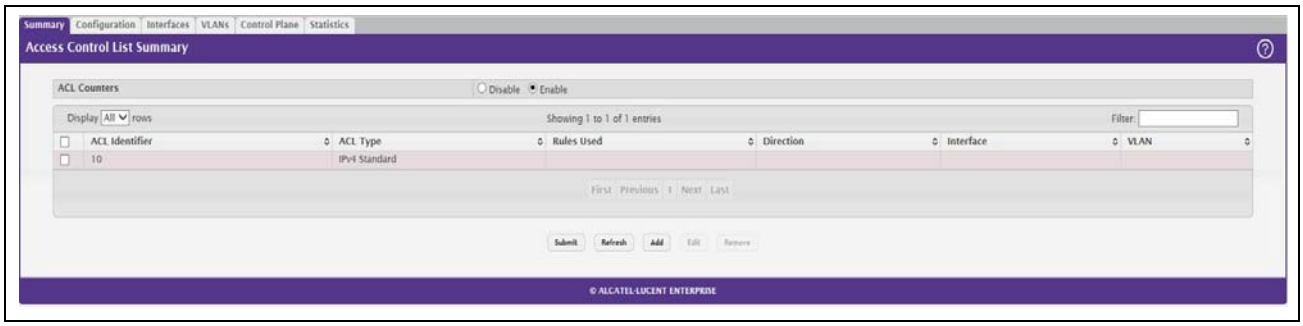
1. Use the “IP ACL Configuration” on page 180 page to define the IP ACL type and assign an ID to it.
2. Use the “Access Control List Interface Summary” on page 190 page to create rules for the ACL.
3. Use the “Access Control List Configuration” on page 181 page to view the configuration.

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 “Access Control List Interface Summary” on page 190 page.

To display the Access List Summary page, click **QoS > Access Control Lists > Summary** in the navigation menu.

Figure 119: 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 116: 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.

Table 116: Access List Summary Fields (Cont.)

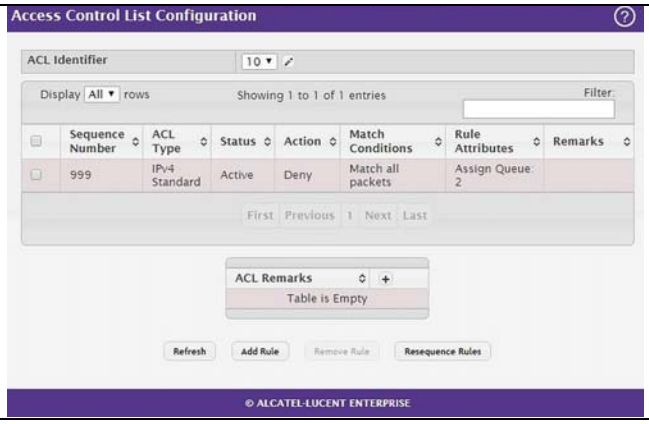
Field	*Description*
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows: • **IPv4 Standard** – Match criteria is based on the source address of IPv4 packets. • **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. • **IPv4 Named** – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number. • **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.
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 120: 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**.

Table 117: IP ACL Summary Fields

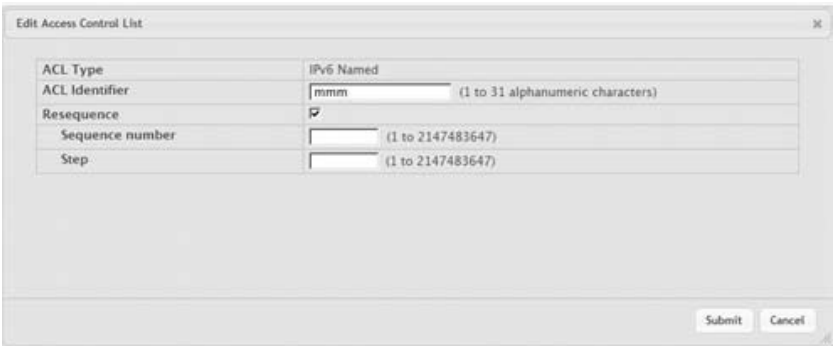
Field	*Description*
ACL Identifier	The menu contains the ID for each ACL that exists on the system. Before you add or remove a rule, you must select the ID of the ACL from the menu. For ACLs with alphanumeric names, click the **Edit** icon to change the ACL ID.  The ID of a Named IPv4 ACL must begin with a letter, and not a number. The ACL identifier for IPv4 Standard and IPv4 Extended ACLs cannot be changed.
Sequence Number	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.

Table 117: IP ACL Summary Fields (Cont.)

Field	*Description*
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: • **IPv4 Standard** – Match criteria is based on the source address of IPv4 packets. • **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. • **IPv4 Named** – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number. • **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. • **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.
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: • **Permit** – The packet or frame is forwarded. • **Deny** – The packet or frame is dropped. ***Note:*** 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.	
ACL Remarks	Lists the configured remarks for the selected ACL. All remarks present in this table are applied to the next rule created with the **Add Rule** button.

Table 117: IP ACL Summary Fields (Cont.)

Field	*Description*

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.

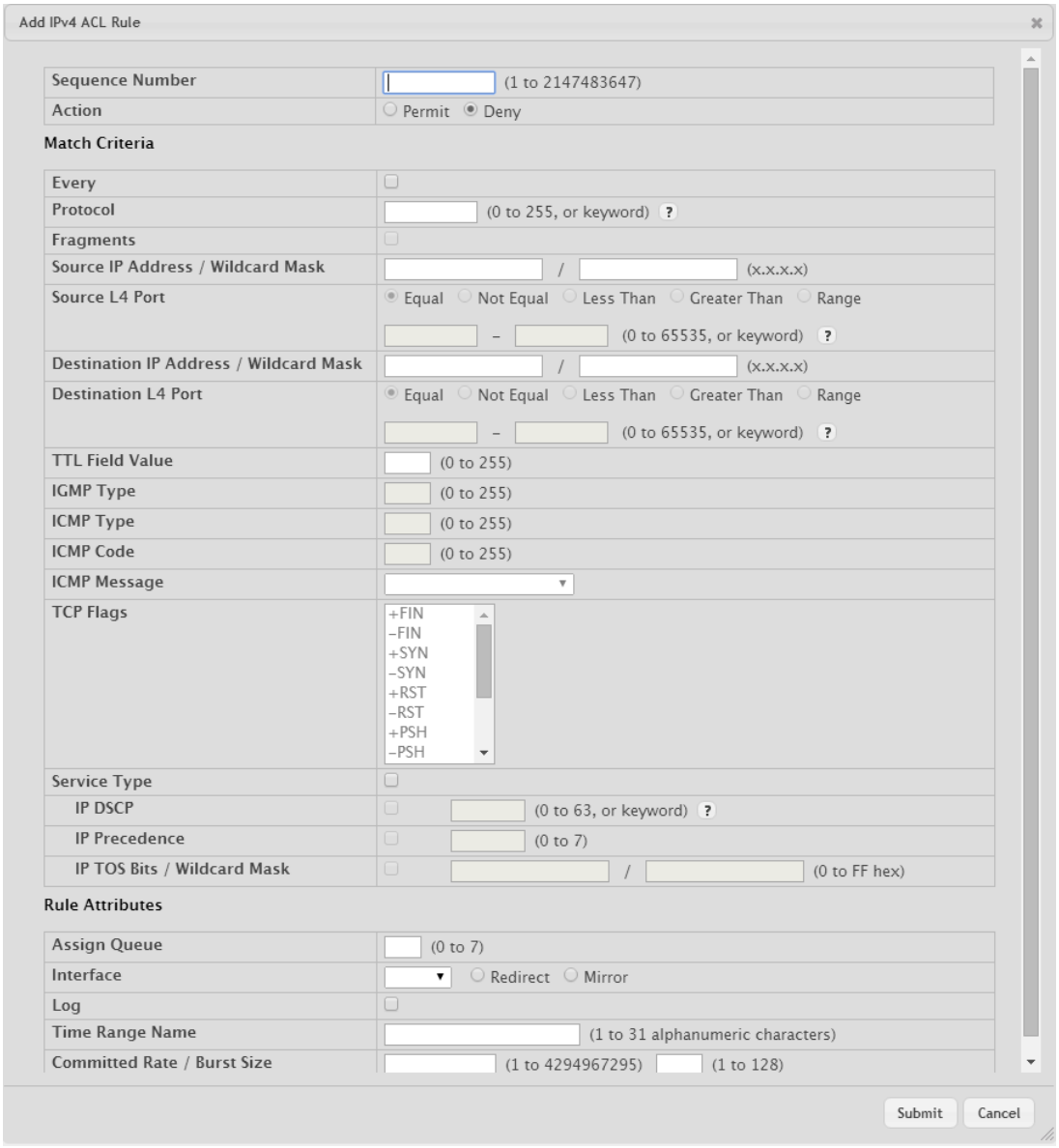


Table 117: IP ACL Summary Fields (Cont.)

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.
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: BGP, 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.

Table 117: IP ACL Summary Fields (Cont.)

Field	*Description*
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: BGP, 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.
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.

Table 117: IP ACL Summary Fields (Cont.)

Field	*Description*
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: • **IP DSCP** – 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. • **IP Precedence** – 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. • **IP TOS Bits** – 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. – TOS Bits – Requires the bits in a packet's TOS field to match the two-digit hexadecimal number entered in this field. – TOS Mask – The bit positions that are used for comparison against the IP TOS field in a packet.
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.
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 BGP, 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.

Table 117: IP ACL Summary Fields (Cont.)

Field	*Description*
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 BGP, 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 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.
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.
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_bb_xx_xx_xx_xx result in a match (where x is any hexadecimal number).

Table 117: IP ACL Summary Fields (Cont.)

Field	*Description*
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_cc_dd_ee_ff, and the mask is 00_00_ff_ff_ff_ff, all MAC addresses with aa_bb_xx_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: • **Redirect** – 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. • **Mirror** – 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.
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.
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.	
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.

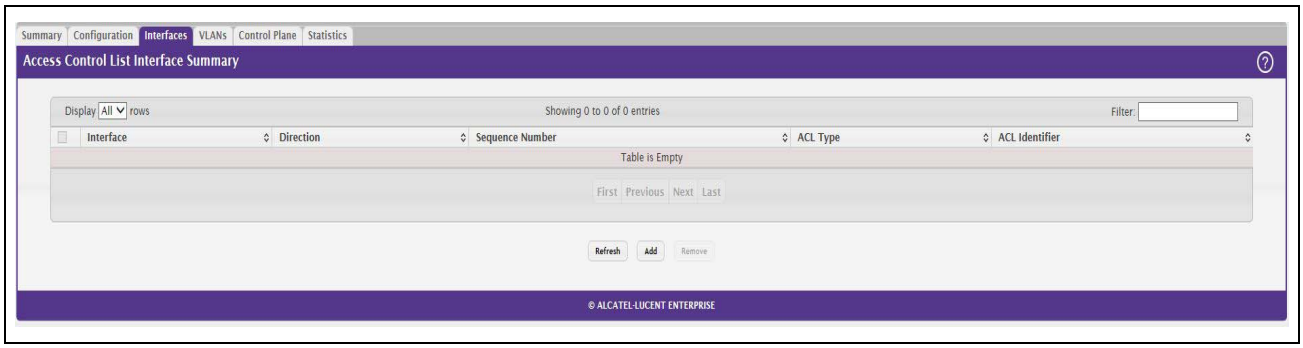
Figure 121: Add ACL Remark

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 122: 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 118: 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).

Table 118: Access Control List Interface Summary Fields (Cont.)

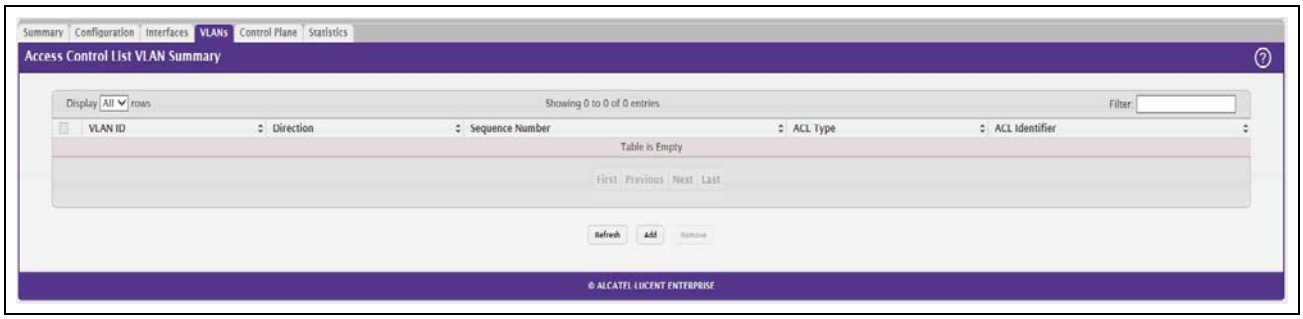
Field	*Description*
Sequence Number	The order the ACL is applied to traffic on the interface relative to other ACLs associated with the interface in the same direction. When multiple ACLs are applied to the same interface in the same direction, the ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.
ACL Type	The type of ACL, which is either IPv4, IPv6, or MAC.
ACL Identifier	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.

Access Control List VLAN Summary

Use this page to associate one or more ACLs with one or more VLANs on the device.

To display the Access Control List VLAN Summary page, click **QoS > Access Control Lists > VLANs** in the navigation menu.

Figure 123: 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 119: **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.

Table 119:* Access Control List VLAN Summary *Fields (Cont.)

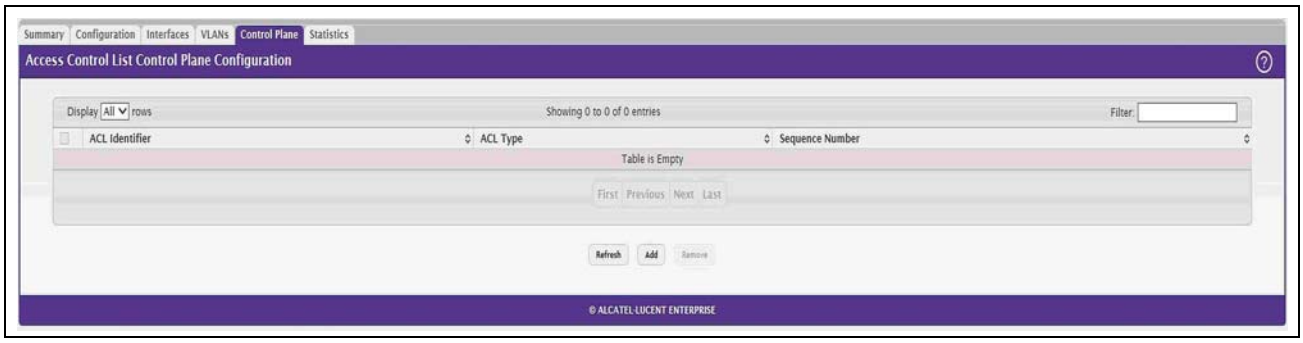
Field	*Description*
ACL Type	The type of ACL, which is either IPv4, IPv6, or MAC.
ACL Identifier	The name or number that identifies the ACL. The permitted identifier depends on the ACL type. Standard and Extended IPv4 ACLs use numbers within a set range, and Named IPv4, IPV6, and MAC ACLs use alphanumeric 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 124: 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 120: Access Control List Control Plane Configuration Fields

Field	*Description*
ACL Identifier	The name or number that identifies the ACL.

Table 120: Access Control List Control Plane Configuration Fields (Cont.)

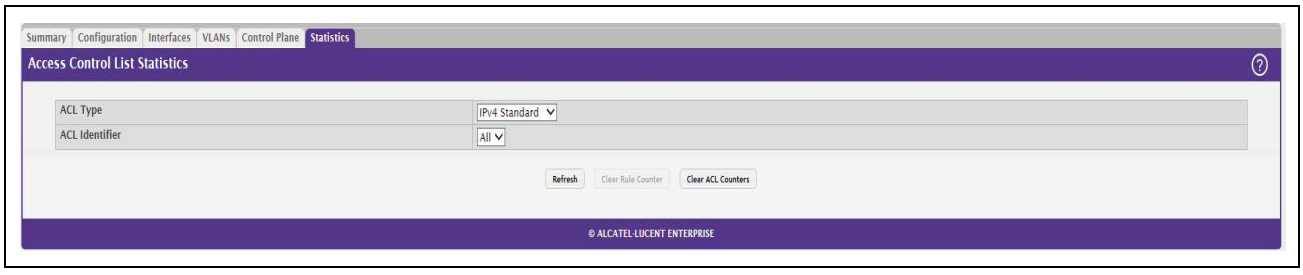
Field	Description
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows: • **IPv4 Standard** – Match criteria is based on the source address of IPv4 packets. • **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. • **IPv4 Named** – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number. • **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.
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.

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 125: 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 121: Access Control List Statistics Fields

Field	*Description*
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: • **IPv4 Standard** – Match criteria is based on the source address of the IPv4 packets. • **IPv4 Extended** – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of the IPv4 packets. • **IPv4 Named** – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number. • **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 the IPv6 packets. • **Extended MAC** – 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.
ACL Identifier	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 **All** is selected. Option **All** lets you clear the hit count for an ACL type.
Sequence Number	The number that indicates the position of a rule within the ACL.
Action	The action to take when a packet or frame matches the criteria in the rule: • **Permit** – The packet or frame is forwarded. • **Deny** – The packet or frame is dropped.
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.
Hit Count	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.

Configuring Auto VoIP

Voice over Internet Protocol (VoIP) allows you to make telephone calls using a computer network over a data network like the Internet. With the increased prominence of delay-sensitive applications (voice, video, and other multimedia applications) deployed in networks today, proper QoS configuration will ensure high-quality application performance. The Auto VoIP feature is intended to provide an easy classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better QoS.

The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class of service than ordinary traffic. If you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

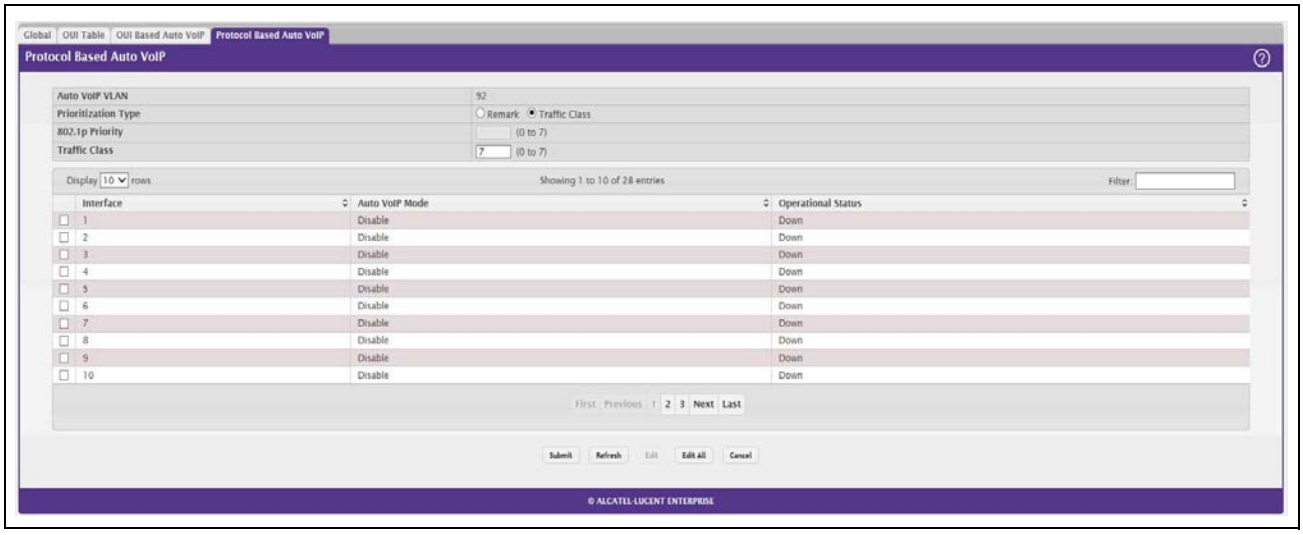
When a call-control protocol is detected the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

Protocol Based Auto VoIP

Use this page to configure the protocol-based Auto VoIP priority settings and to enable or disable the protocol-based Auto VoIP mode on the interfaces.

To display the Protocol Based Auto VoIP page, click **Quality of Service > Auto VoIP > Protocol Based Auto VoIP** in the navigation menu. A portion of the web page is shown below.

Figure 126: Protocol Based Auto VoIP



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**.

Table 122: Protocol Based Auto VoIP Fields

Field	*Description*
Prioritization Type	The method used to prioritize VoIP traffic when a call-control protocol is detected, which is one of the following: • **Remark** – Remark the voice traffic with the specified 802.1p priority value at the ingress interface. • **Traffic Class** – Assign VoIP traffic to the specified traffic class when egressing the interface.
802.1p Priority	The 802.1p priority used for protocol-based VoIP traffic. This field can be configured if the Prioritization Type is 802.1p Priority. If the Auto VoIP mode is enabled and the interface detects a call-control protocol, the device marks traffic in that session with the specified 802.1p priority value to ensure voice traffic always gets the highest priority throughout the network path. Egress tagging must be administratively enabled on the appropriate uplink port to carry the remarked priority at the egress port.
Traffic Class	The traffic class used for protocol-based VoIP traffic. This field can be configured if the Prioritization Type is Traffic Class. If the Auto VoIP mode is enabled and the interface detects a call-control protocol, the device assigns the traffic in that session to the configured Class of Service (CoS) queue. Traffic classes with a higher value are generally used for time-sensitive traffic. The CoS queue associated with the specified traffic class should be configured with the appropriate bandwidth allocation to allow priority treatment for VoIP traffic.
Interface	The interface associated with the rest of the data in the row. When editing Auto VoIP settings on one or more interfaces, this field identifies the interface(s) being configured.
Auto VoIP Mode	The administrative mode of the Auto VoIP feature on the interface: • **Enable** – The interface scans incoming traffic for the following call-control protocols: – Session Initiation Protocol (SIP) – H.323 – Skinny Client Control Protocol (SCCP) • **Disable** – The interface does not use the Auto VoIP feature to scan for call-control protocols.
Operational Status	The operational status of an interface. To be up, an interface must be administratively enabled and have a link.

- If you change any of the settings on the page, click Submit to send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a Save is performed.
- Click **Refresh** to update the page with the most current data from the switch.

Configuring Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. 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 127: CoS IP DSCP Mapping Configuration

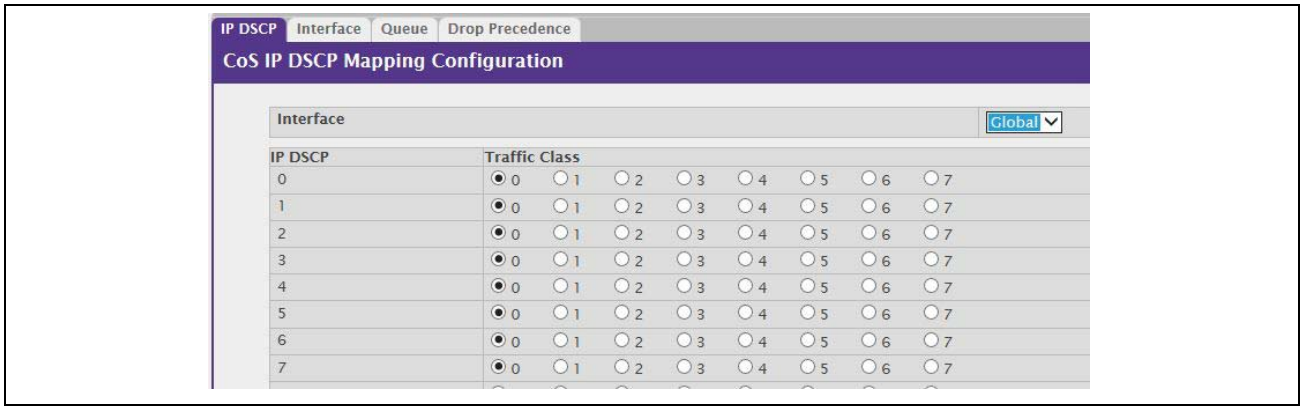


Table 123: IP DSCP Mapping Configuration Fields

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 128: Interface Configuration

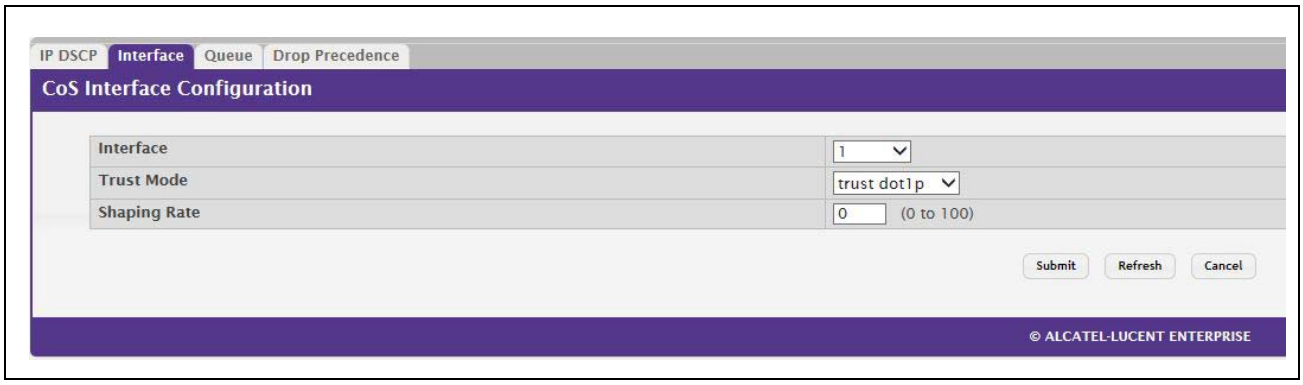


Table 124: Interface Configuration Fields

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.
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 0-100, in increments of 1. A value of 0 means the maximum is unlimited.
WRED Decay Exponent	Specifies the decay exponent value used with the WRED average queue length calculation algorithm. Default value is 9. Valid Range is (0 to 15).

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 129: Interface Queue Configuration

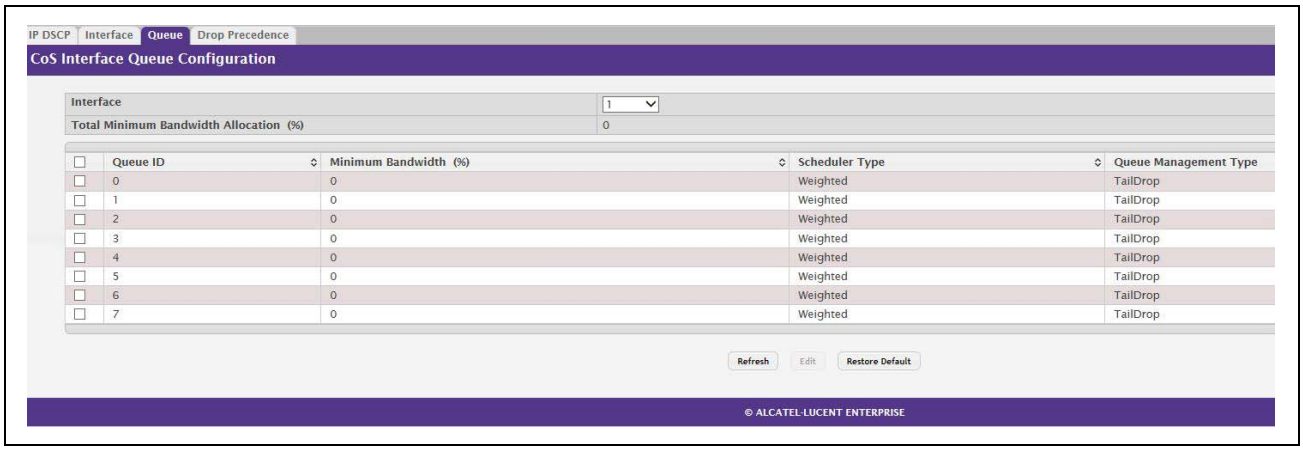


Table 125: Interface Queue Configuration Fields

Field	*Description*
Interface	Specifies the interface (physical, LAG, or Global) to configure.
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.

Table 125: Interface Queue Configuration Fields (Cont.)

Field	*Description*
Scheduler Type	Selects the type of queue processing from the drop-down menu. Options are **Weighted** and **Strict**. Defining on a per-queue basis allows the user to create the desired service characteristics for different types of traffic. • **Weighted:** Weighted round robin associates a weight to each queue. This is the default. • **Strict:** Strict priority services traffic with the highest priority on a queue first
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 Defaults for all Queues** to reset the settings for the selected interface.
- To reset the defaults for all interfaces, select Global from the **Slot/Port** menu before you click the button.

Appendix A: Configuration Examples

This appendix contains examples of how to configure selected features available in the OS2220 Websmart software. Each example contains procedures on how to configure the feature by using the Web interface and/or SNMP.

This appendix describes how to perform the following procedures:

- Configuring VLANs
- Configuring Multiple Spanning Tree Protocol
- Configuring 802.1X Network Access Control

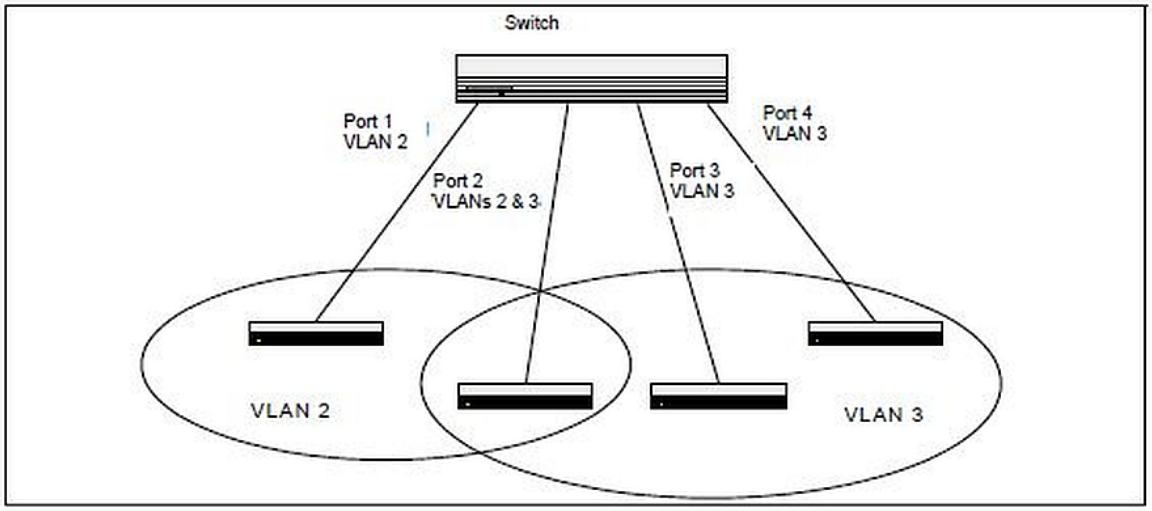
Note: Each configuration example starts from a factory-default configuration unless otherwise noted.

Configuring VLANs

The diagram in this section shows a switch with four ports configured to handle the traffic for two VLANs. Port 2 handles traffic for both VLANs, while port 1 is a member of VLAN 2 only, and ports 3 and 4 are members of VLAN 3 only.

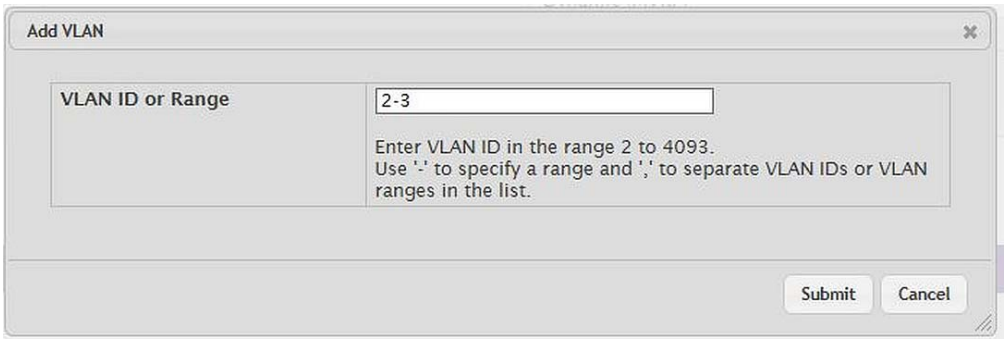
The following examples show how to create VLANs, assign ports to the VLANs, and assign a VLAN as the default VLAN to a port.

Figure 130: VLAN Example Network Diagram



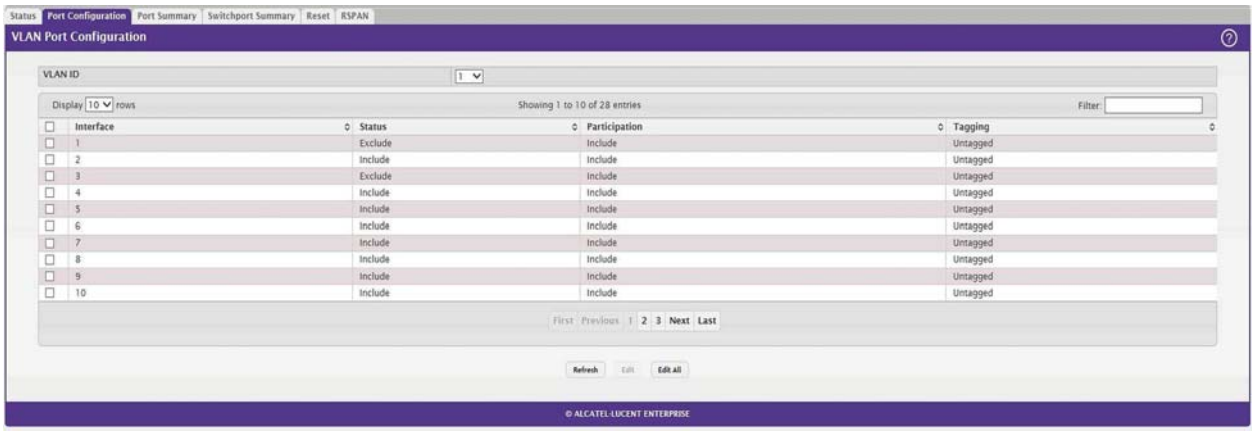
Using the Web Interface to Configure VLANs

1. Access the **Switching > VLAN > Status** page.
2. Click **Add** to create a new VLAN.
3. Type 2-3 in the VLAN ID-Individual/Range field.



4. Click **Submit**.
5. From the **Port Configuration Page**, Select VLAN 2 from the VLAN ID List.
6. From the Participation column in the interface table, select Include for ports 1 and 2 to specify that these ports are members of VLAN 2.
7. Select the interface check box and click **Edit**. Select the Tagging All check box to specify that frames will always be transmitted tagged from ports that are members of VLAN 2.
8. Click **Submit**.
9. Select VLAN 3 from the VLAN ID and Name List.
10. Select the Participate option in the VLAN field.
11. For ports 2, 3 and 4, select Include from the Participation menu to specify that these ports are members of VLAN 3.
12. Click **Submit**.
13. Go to the **Switching > VLAN > Port Configuration** page.
14. From the Interface menu, select 1.
15. In the Acceptable Frame Types field, select AdmitTaggedOnly to specify that untagged frames will be rejected on receipt.
16. Click **Submit**.
17. From the Interface menu, select 2.
18. In the Port VLAN ID field, enter 3 to assign VLAN 3 as the default VLAN for the port.

19. In the Acceptable Frame Types field, select AdmitTaggedOnly to specify that untagged frames will be rejected on receipt.



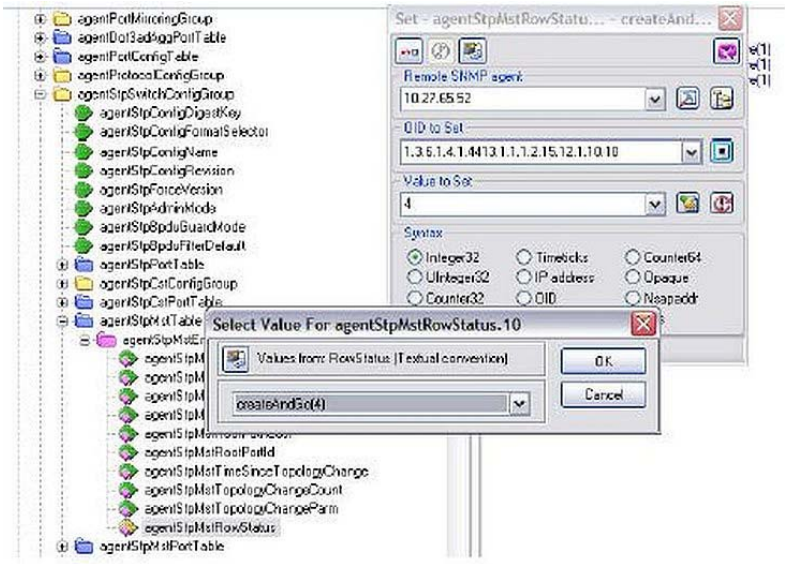
20. Click **Submit.**

Using the SNMP to Configure VLANs

1. Use the objects in dot1qVlanStaticTable (in dot1qVlan in the QBRIDGE-MIB module) to create VLANs 2 and 3.

Set the dot1qVlanStaticRowStatus object to ‘CreateandGo (4)’ to create a VLAN. If the other parameters are not specified, simply specifying the dot1qVlanIndex and dot1qVlanStaticRowStatus is sufficient to create the VLAN.

The full path to the object is iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).qBridgeMIB(7). qBridgeMIBObjects(1).dot1qVlan(4).dot1qVlanStaticTable(3).dot1qVlanStaticEntry(1).dot1qVlanStaticRowStatus(5).



2. To assign ports 1 and 2 to VLAN2, retrieve the current dot1qStaticEgressPorts mask and append interfaces 1 and 2 to this mask by setting the first octet to 0xC0.

   The dot1qVlanStaticEgressPorts bit mask can be constructed according to the following rules:

   - Each octet within this value specifies a set of eight ports, with the first octet specifying ports (1-8), the second octet specifying ports (9-16), and so on.
   - Within each octet, the most significant bit represents the lowest numbered port, and the least significant bit represents the highest numbered port. Thus, each port of the bridge is represented by a single bit within the value of this object. If that bit has a value of (1), then that port is included in the set of ports. The port is not included if its bit has a value of (0).

   For example if the switch has 12 ports and we want to add ports 1 and 4 in the VLAN and exclude all other ports, then the bit mask in hex will be 0x50 0x00.

3. To specify that frames will always be transmitted tagged from ports that are members of VLAN 2, use the dot1qVlanStaticUntaggedPorts object and set the value of the appropriate number of octets to 0.

   Each octet represents eight ports, so for a 48-port switch, the first six octets would be zero.

4. To specify that ports 1 and 2 will only accept tagged frames and will reject untagged frames on receipt, set the dot1qPortAcceptableFrameTypes object to admitOnlyVlanTagged(2).

   The object is in dot1qPortVlanEntry in the dot1qPortVlanTable.

5. To assign VLAN3 as the default VLAN for interface 2., set the value of dot1qPvid for 2 (instance 2) to 3.

6. To assign ports 2, 3, and 4 to VLAN3, retrieve the current dot1qStaticEgressPorts mask and append the interfaces to this mask by setting the first octet to 0x70.

Configuring Multiple Spanning Tree Protocol

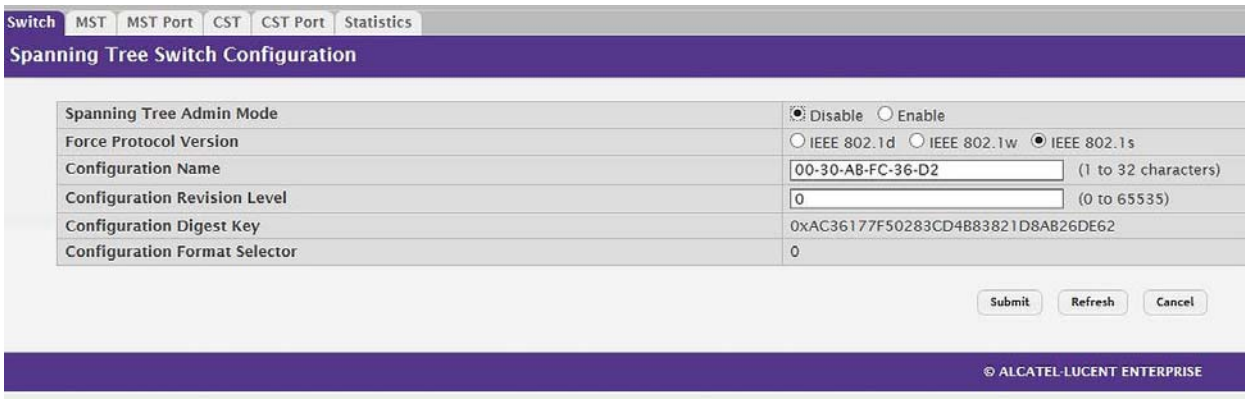
This example shows how to enable IEEE 802.1s Multiple Spanning Tree (MST) protocol on the switch and all of the ports and to set the bridge priority.

To make multiple switches be part of the same MSTP region, make sure the Force Protocol Version setting for all switches is IEEE 802.1s. Also, make sure the configuration name, digest key, and revision level are the same for all switches in the region.

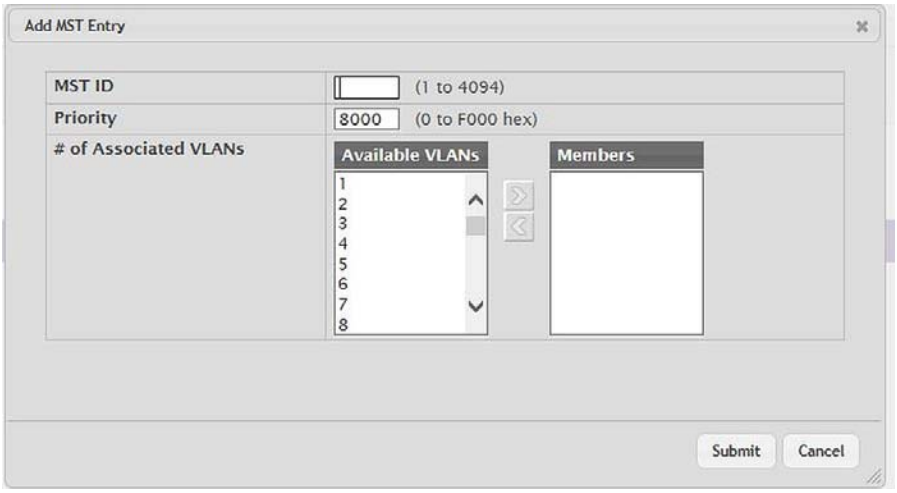
Note: The digest key is generated based on the association of VLANs to different instances. To ensure the digest key is same, the mapping of VLAN to instance must be the same on each switch in the region. For example, if VLAN 10 is associated with instance 10 on one switch, you must associate VLAN 10 and instance 10 on the other switches.

Using the Web UI to Configure MSTP

1. Create VLANs 10 and 20.
   a. Access the **Switching > VLAN > Status** page.
   b. Click **Add** to create a VLAN.
   c. Select the VLAN ID-Individual option and enter 10.
   d. Click **Submit**.
   e. Repeat the steps to add VLAN 20.
2. Enable MSTP (IEEE 802.1s) on the switch and change the configuration name.
   Changing the configuration name allows all the bridges that want to be part of the same region to join.
   a. Go to the **Switching > Spanning Tree > Switch** page.
   b. From the Spanning Tree Admin Mode menu, select Enable.
   c. In the Configuration Name field, enter ALE.
   d. Click **Submit**.



3. Create two MST instances.
   a. Go to the **Switching > Spanning Tree > MST** page.
   b. From the MST page, click **Add**.
   c. In the MST ID field, enter 10.
   d. Associate MST ID 10 with VLAN 10 and assign a bridge priority of 16384.
   e. Click **Submit**.
   f. Repeat the steps to create an MST instance with an ID of 20.



4. Use similar procedures to associate MST instance 20 to VLAN 20 and assign it a bridge priority value of 61440.

   By using a lower priority for MST 20, MST 10 becomes the root bridge.

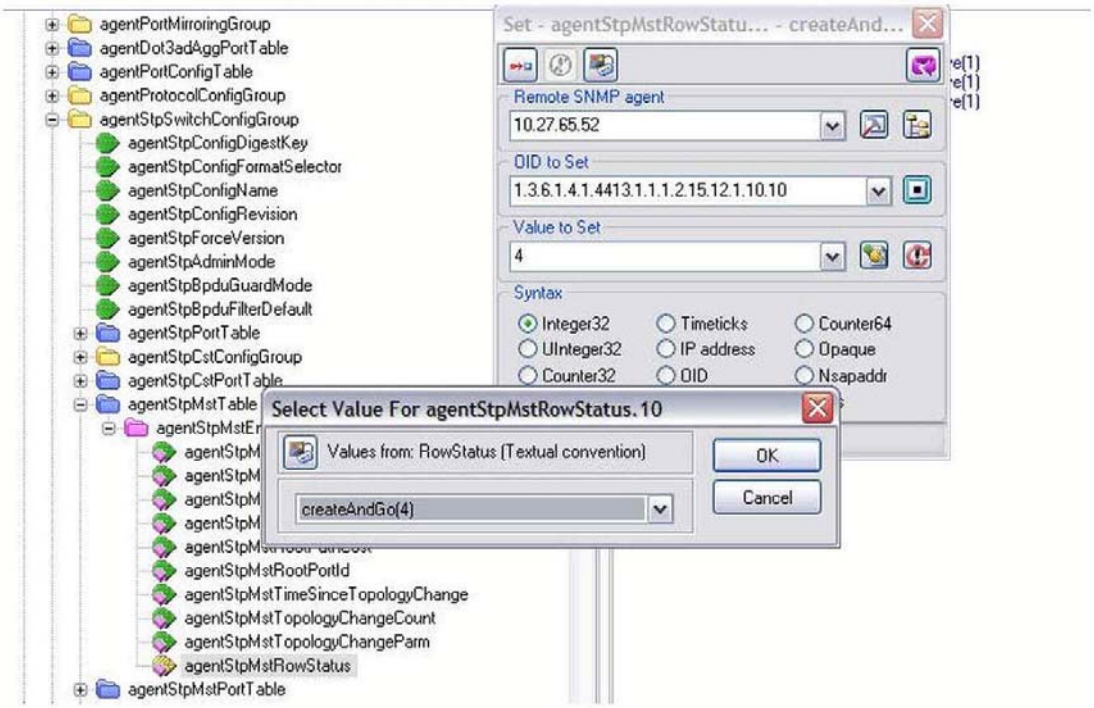
5. Force port 2 to be the root port for MST 20, which is the non-root bridge.
   a. Go to the **Switching > Spanning Tree > MST** page.
   b. From the MST ID menu, select 20.
   c. From the Interface menu, select 2.
   d. In the Port Priority field, enter 64.
   e. Click **Submit**.

Using SNMP to Configure MSTP

1. Use the objects in dot1qVlanStaticTable (in dot1qVlan in the QBRIDGE-MIB module) to create VLANs 10 and 20.
2. To enable spanning tree globally, set the agentStpAdminMode object in the FASTPATH-SWITCHING-MIB module to enable (2).

   The full path to the object is iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).broadcom(4413).broadcomProducts(1).fastPath(1).fastPathSwitching(1).agentConfigGroup(2).agentStpSwitchConfigGroup(15).agentStpAdminMode(6).

3. Use the agentStpConfigName object in the agentStpSwitchConfigGroup to change the name so that all the bridges that want to be part of the same region can form the region.
4. Use the agentStpMstRowStatus object in the agentStpMstTable to create MST instances 10 and 20.



5. Use the agentStpMstBridgePriority object to set the bridge priorities for MST 10 and MST 20:
   - For MST ID 10, set the value to 16384 to make it the root bridge.
   - For MST ID 20, set the value to 61440 to ensure the other bridge is the root bridge.
6. Use the agentStpMstVlanRowStatusAssociate object in the agentStpMstVlanTable to associate MST instance 10 to VLAN 10 and MST instance 20 to VLAN 20.
   - For MST ID 20, the OID to set is 1.3.6.1.4.1.4413.1.1.1.2.15.14.1.1.10.10 (the final .10 is the VLAN ID)
   - For MST ID 20, the OID to set is 1.3.6.1.4.1.4413.1.1.1.2.15.14.1.1.20.20

   Set the value to CreateAndGo (4)
7. Use the agentStpPortState in agentStpPortTable under agentStpSwitchConfigGroup to enable STP on interface 1 and interface 2.

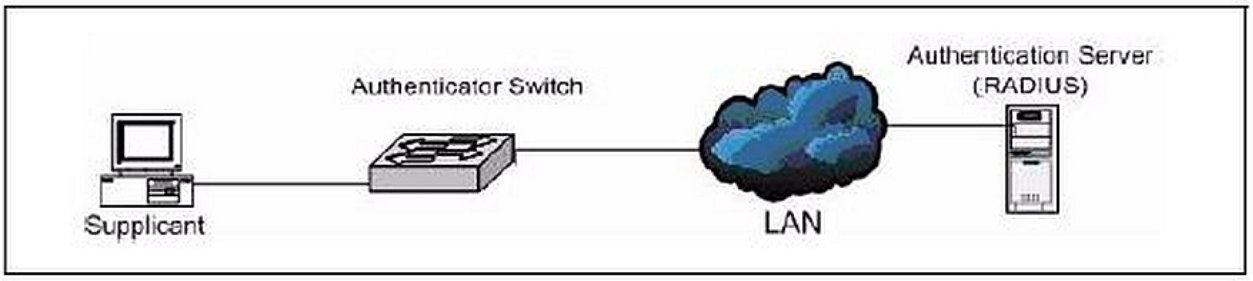
   For instance 1 and 2, set the value to enable (1).
8. Use the agentStpMstPortPriority object in agentStpMstPortTable to change the port priority on interface 2 to force the port to be the root port on the non-root bridge.

   For instance 2, set the value to 64.

Configuring 802.1X Network Access Control

This example configures a single RADIUS server used for authentication and accounting at 10.10.10.10. The shared secret is configured to be *secret*. The switch is configured to require that the 802.1X access method is through a RADIUS server. IEEE 802.1X port-based access control is enabled for the system, and interface 1 is configured to be in force-authorized mode because this is where the RADIUS server and protected network resources are located.

Figure 131: Switch with 802.1x Network Access Control

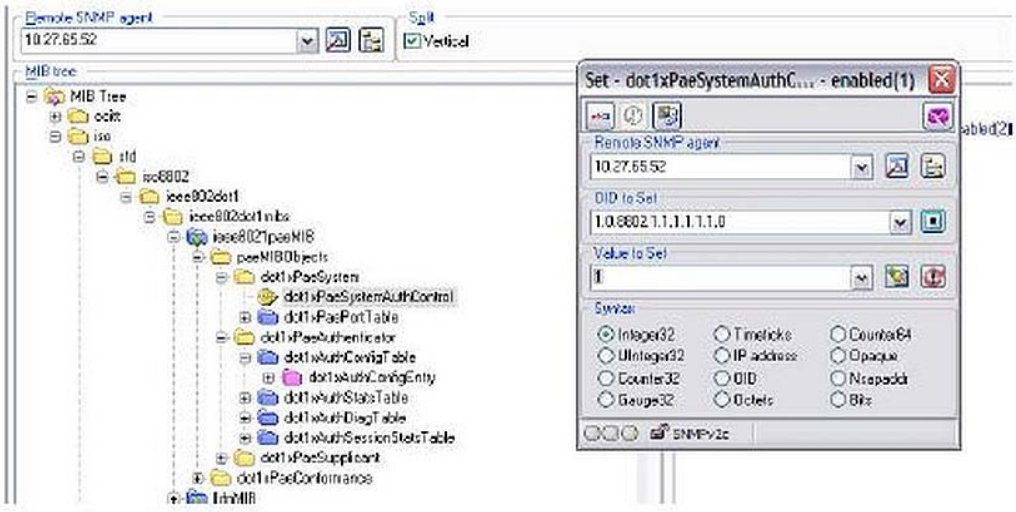


If a user, or supplicant, attempts to communicate via the switch on any interface except interface 1, the system challenges the supplicant for login credentials. The system encrypts the provided information and transmits it to the RADIUS server. If the RADIUS server grants access, the system sets the 802.1X port state of the interface to authorized, and the supplicant is able to access network resources.

Using SNMP to configure 802.1X Port-Based Access Control

1. Use the agentRadiusServerStatus in the agentRadiusServerConfigTable under the FASTPATH-RADIUS-AUTH-CLIENT-MIB to create a new RADIUS server entry.
2. Use the agentRadiusServerAddress object to configure the RADIUS authentication server IP address as 10.10.10.10.
3. Use the agentRadiusServerSecret object to configure the RADIUS authentication server secret.
4. Use the agentRadiusAccountingStatus object in the agentRadiusAccountingConfigTable to create a RADIUS accounting server.
5. User the agentRadiusAccountingServerAddress object to configure the RADIUS accounting server IP address. as 10.10.10.10.
6. Use the agentRadiusAccountingSecret object to configure the RADIUS accounting server secret.
7. Use the agentRadiusAccountingStatus object to enable RADIUS accounting mode.
8. Use the agentUserConfigDefaultAuthenticationList object in agentAuthenticationGroup in the FASTPATH-SWITCHING module to set RADIUS as the default login list for dot1x.

9. To enable 802.1X authentication on the switch, set the dot1xPaeSystemAuthControl object in the IEEE8021-PAE-MIB module to enable (1).



10. To set the 802.1X mode for port 1 to Force Authorized, use theagentDot1xPortControlMode object in the agentDot1xPortConfigTable, which is in FASTPATH-DOT1X-ADVANCED-FEATURES-MIB.