IGS-RX164GP+

Industrial Managed Ethernet Switch

User Manual

Version 1.1

www.oringnet.com

ORing Industrial Networking Corp.

COPYRIGHT NOTICE

TRADEMARKS

ORing is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.
3F., NO.542-2, Jhongjheng Rd., Sindian District, New Taipei City 231, Taiwan, R.O.C.
Tel: + 886 2 2218 1066 // Fax: + 886 2 2218 1014
Website: www.oringnet.com

Technical Support
E-mail: support@oring-networking.com

Sales Contact
E-mail: sales@oringnet.com (Headquarters)
sales@oringnet.com.cn (China)

Table of Content

Getting Started

1.1 About the IGS-RX164GP+

IGS-RX164GP+ is a Din-Rial 10G Ethernet switch,support up to 16 10/100/1000BaseT(X) and 4 10Gigabit Ethernet ports. With completely support for Ethernet redundancy protocols MSTP (RSTP/STP compatible), the switch can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. Featuring a wide operating temperature from -40 to 75oC and can be managed centrally and conveniently via web browsers, Telnet and console (CLI) configuration, making it one of the most reliable choice for harsh industrial applications.

1.2 Software Features

- MSTP(RSTP/STP compatible) for Ethernet Redundancy
- Supports IPv6 new Internet protocol version
- HTTPS/SSH protocols for higher network security
- Supports SMTP client
- Supports IP-based bandwidth management
- Supports application-based QoS management
- IGMP v2/v3 (IGMP snooping support) for filtering multicast traffic
- Supports SNMP v1/v2c/v3 & RMON & 802.1Q VLAN network management
- Supports ACL, TACACS+ and 802.1x user authentication
- Supports Jumbo frame
- Multiple notifications during unexpected events
- Configuration via Web-based ,Telnet, Console (CLI)
- Supports LLDP Protocol

1.3 Hardware Specifications

ORing Switch Model	**IGS-RX164GP+**
Physical Ports	
10/100/1000Base-T(X) Ports in RJ45 Auto MDI/MDIX	**16**
1G/10GBase-X with SFP+ port	**4**
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3ab for 1000Base-T IEEE 802.3z for 1000Base-X IEEE 802.3ae for 10Gigabit Ethernet IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	16k
Priority Queues	8
Packet Buffer Size	16Mbit
Flash Memory	512Mbits
DRAM Size	8Gbits
Jumbo frame	Up to 12K Bytes
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 112Gbps Throughput (packet per second) : 83.32Mpps@64Bytes packet Max. Number of Available VLANs: 4095 VLAN ID Range : VID 1 to 4094 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Define
Security Features	Enable/disable ports, MAC based port security Port based network access control (802.1x)MAC-based authentication(802.1x) VLAN (802.1Q) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security Web and CLI authentication and authorization IP source guard, DHCP Snooping, Dynamic ARP Inspection Https / SSH enhance network security DOS/DDOS auto prevention
Software Features	TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging IGMP Snooping Application-based QoS management Port configuration, status, statistics, monitoring, security Port mirroring DHCP Server/Client/Relay SNTP Client
Routing Protocols	Unicast Routing - Static routing, RIP v1/v2, OSPF Multicast Routing -PIM-SM, PIM-DM, Routing Redundancy -VRRP
TSN protocols	IEEE 802.1AS, Qav, Qat

Network Redundancy	O-Ring with recovery time less than 30ms O-Chain MSTP /RSTP/STP
RS-232 Serial Console Port	RS-232 in DB9 connector with console cable. 115200bps, 8, N, 1
LED indicators	
Power Indicator (PWR)	Green : Power LED x 3
Ring Master Indicator (R.M.)	Green : Indicates that the system is operating in O-Ring Master mode
O-Ring Indicator (Ring)	Green : Indicates that the system operating in O-Ring mode Green Blinking: Indicates that the Ring is broken.
Fault Indicator (Fault)	Amber : Indicate unexpected event occurred
10/100/1000Base-T(X) RJ45 Port Indicator	Green for Link/Act indicator Dual color LED for speed indicator : Green for 1000Mbps, Amber for 100Mbps, Off-light for 10Mbps
1G/10GBase-X SFP+ Port Indicator	Green for port Link/Act.
Fault Contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Reset Function	
Reset Button	< 5 sec: System reboot, > 5 sec: Factory default
Power	
Redundant Input power	Dual DC inputs, 12~48VDC on 6-pin terminal block
Power consumption (Typ.)	23 Watts
Overload current protection	Present
Reverse Polarity Protection	Present
Physical Characteristic	
Enclosure	IP-30, Aluminum
Dimension (W x D x H)	116.4 (W) x 170 (D) x 180 (H) mm (4.58 x 6.69 x 7.08 inches)
Weight (g)	1,530g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 75°C (-40 to167°F)
Operating Humidity	5% to 95% Non-condensing
Regulatory Approvals	
EMC	CE EMC (EN 55024, EN 55032), EN 50121-4 (compliant), FCC Part 15 B
EMI	EN 55032, CISPR32, EN 61000-3-2, EN 61000-3-3, FCC Part 15 B class A
EMS	IEC/EN 61000-4-2 (ESD: Contact 8KV, Air 10KV), IEC/EN 61000-4-3 (RS: 3V), IEC/EN 61000-4-4 (EFT Power 2KV, Signal 2KV), IEC/EN 61000-4-5 (Surge: Power 4KV, Signal 4KV), IEC/EN 61000-4-6 (CS: 3V), IEC/EN 61000-4-8(PFMF),
Shock	IEC60068-2-27
Free Fall	IEC60068-2-31
Vibration	IEC60068-2-6
Safety	EN60950-1
MTBF	323,539 hrs
Warranty	**5 years**

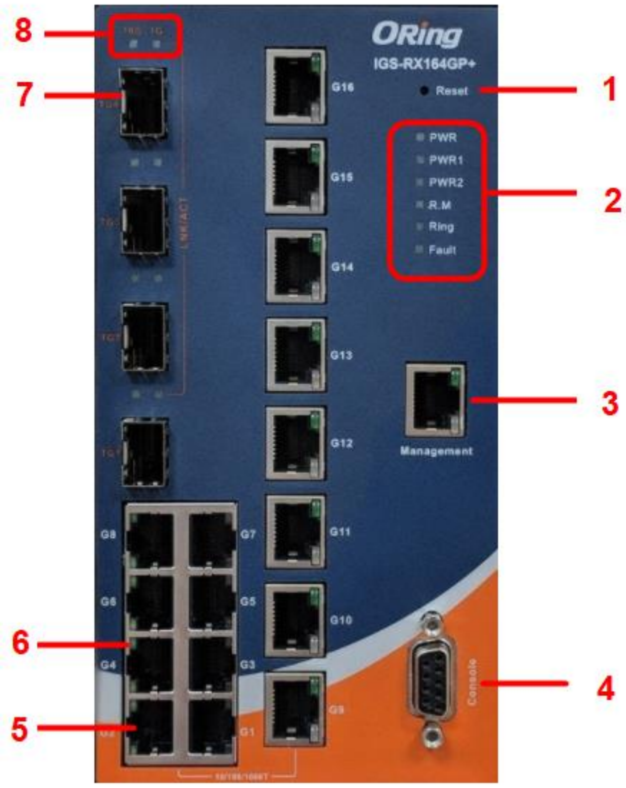
Hardware Overview

2.1 Front Panel

2.1.1 Ports and Connectors

The device comes with the following ports and connectors on the front panel.

Port	Description
Console port	1 x Console Port
Management Port	1 x Management Port
Reset button	1 x reset button. Press the button for 3 seconds to reset and 5 seconds to return to factory default.
Ethernet Port	16 x 100/1000Tx
SFP Port	4 x 1G/10G SFP Fiber



1. Reset Button

2. System LED Status

   PWR = power status LED .

   R.M = Ring Master Status LED

   Ring = Ring Status LED

   Fault LED = Fault Alarm LED

3. Management Port
4. Console Port
5. Ethernet Port(100M/1G)
6. 100M / 1G Port LED
7. SFP Port (1G/10G)
8. 1G/10G Port LED

Management

The switch can be controlled via a built-in web server which supports Internet Explorer (Internet Explorer 5.0 or above versions) and other Web browsers such as Chrome. Therefore, you can manage and configure the switch easily and remotely. You can also upgrade firmware via a web browser. The Web management function not only reduces network bandwidth consumption, but also enhances access speed and provides a user-friendly viewing screen.

By default, IE5.0 or later version do not allow Java applets to open sockets. You need to modify the browser setting separately in order to enable Java applets for network ports.

Preparing for Web Management

You can access the management page of the switch via the following default values:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

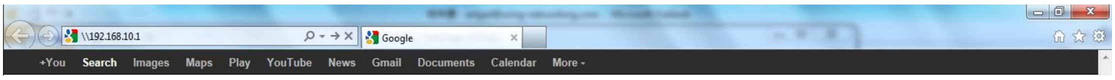
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

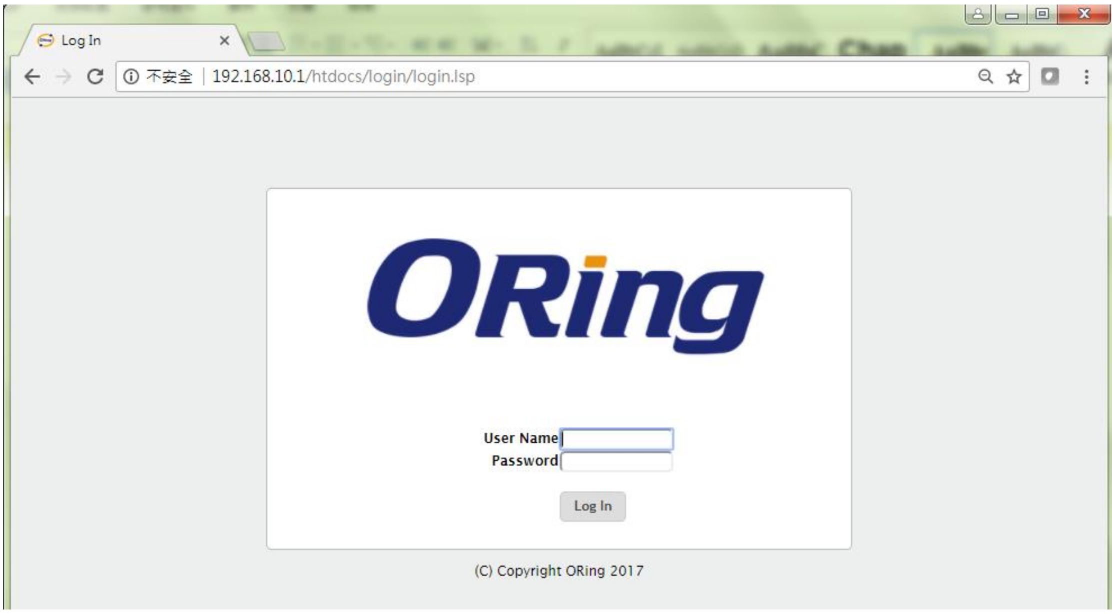
System Login

1. Launch the Internet Explorer.
2. Type http:// and the IP address of the switch. Press **Enter**.

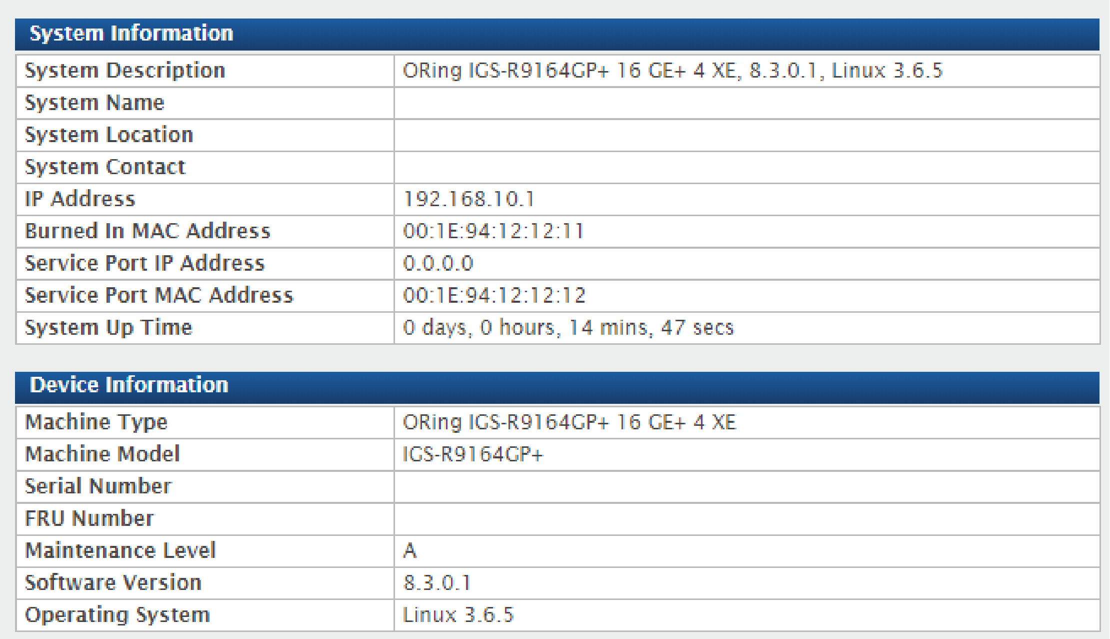


\\192.168.10.1

3. A login screen appears.
4. Type in the username and password. The default username and password is **admin**.
5. Click **Enter** or **OK** button, the management Web page appears.



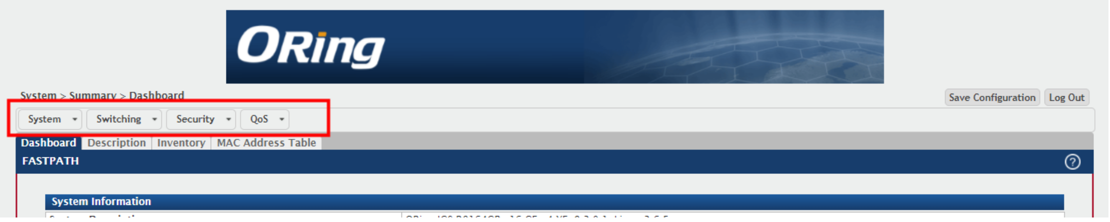
After logging in, you can see the information of the switch as below.



System Information	
System Description	ORing IGS-R9164GP+ 16 GE+ 4 XE, 8.3.0.1, Linux 3.6.5
System Name	
System Location	
System Contact	
IP Address	192.168.10.1
Burned In MAC Address	00:1E:94:12:12:11
Service Port IP Address	0.0.0.0
Service Port MAC Address	00:1E:94:12:12:12
System Up Time	0 days, 0 hours, 14 mins, 47 secs

Device Information	
Machine Type	ORing IGS-R9164GP+ 16 GE+ 4 XE
Machine Model	IGS-R9164GP+
Serial Number	
FRU Number	
Maintenance Level	A
Software Version	8.3.0.1
Operating System	Linux 3.6.5

On the top side of the management interface shows links to various settings. You can click on the links to access the configuration pages of different functions.



3.1 System

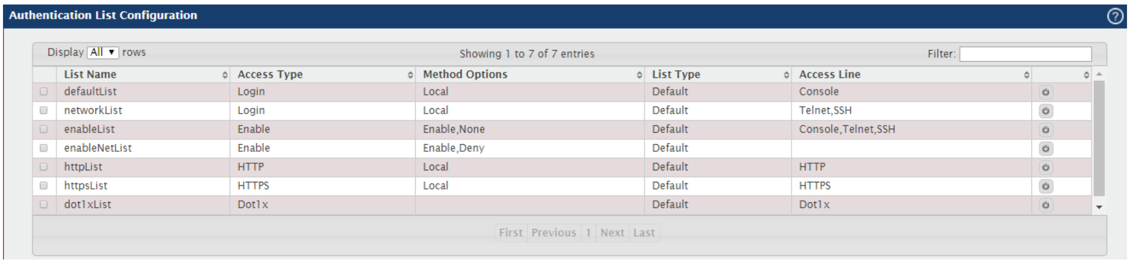
This menu, with all the system-related settings, a total of 17 projects, as follows

3.1.1 AAA

3.1.1.1 Authentication List

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

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



Authentication List Configuration

Display All ▾ rows   Showing 1 to 7 of 7 entries   Filter:

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

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: • **Login** – User EXEC-level management access to the command-line interface (CLI) by using a console connection or a telnet or SSH session. Access at this level has a limited number of CLI commands available to view or configure the system. • **Enable** – Privileged EXEC-level management access to the CLI by using a console connection or a telnet or SSH session. In Privileged EXEC mode, read-write users have access to all CLI commands.

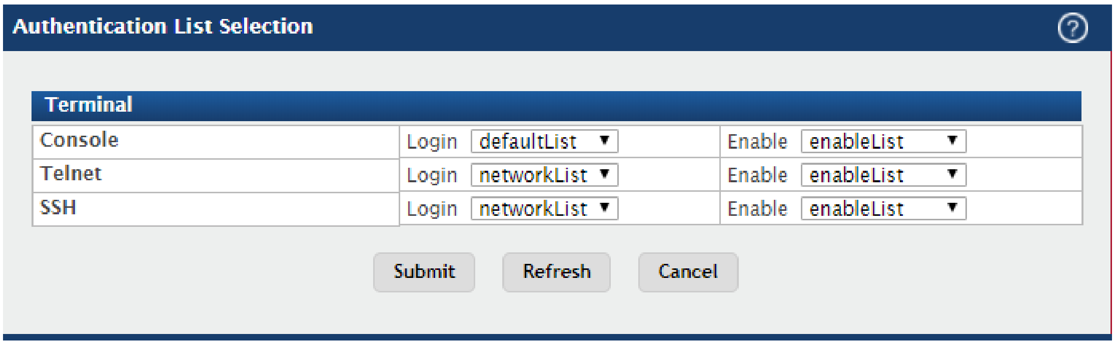
	• **HTTP** – Management-level access to the web-based user interface by using HTTP. • **HTTPS** – Management-level access to the web-based user interface by using secure HTTP. • **Dot1x** – Port-based access to the network through a switch port that is controlled by IEEE 802.1X.
Method Options	The method(s) 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. • **TACACS+** – Sends the user's ID and password to the configured TACACS+ 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.
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.

3.1.1.2 Authentication selection

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

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

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



Authentication List Selection

Terminal

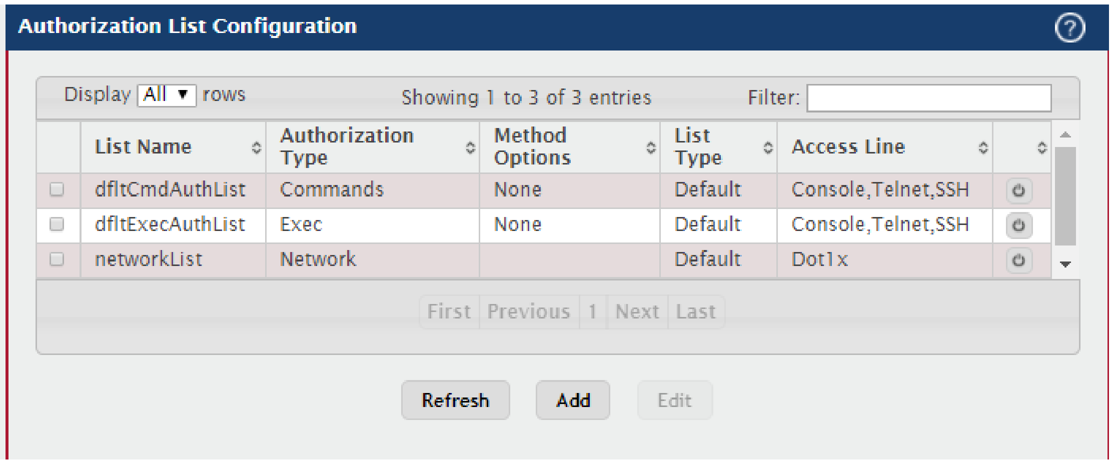
Console	Login defaultList	Enable enableList
Telnet	Login networkList	Enable enableList
SSH	Login networkList	Enable enableList

Field	Description
Console	The Login authentication list and the Enable authentication list to apply to users who attempt to access the CLI by using a connection to the console port.
Telnet	The Login authentication list and the Enable authentication list to apply to users who attempt to access the CLI by using a Telnet session.
Secure Telnet (SSH)	The Login authentication list and the Enable authentication list to apply to users who attempt to access the CLI by using a secure shell (SSH) session.
List Name	The name of the authentication list. This field can be configured only when adding a new authentication list.

3.1.1.3 Authorization List

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

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


Authorization List Configuration
Display All rows
Showing 1 to 3 of 3 entries
Filter:
First Previous 1 Next Last
Refresh
Add
Edit

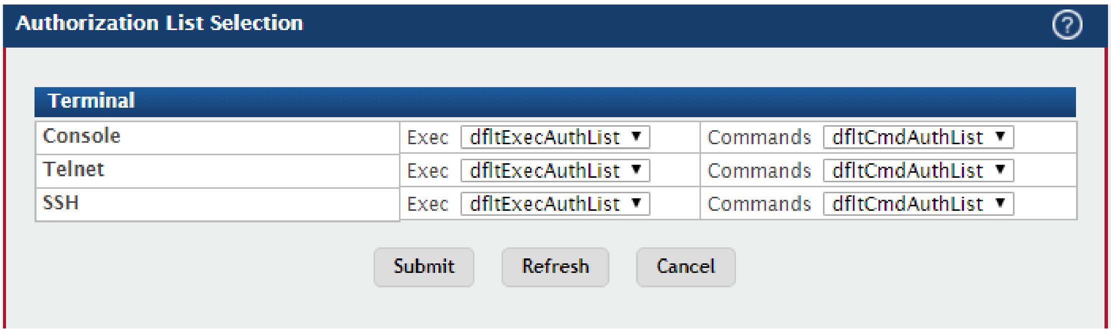
	List Name	Authorization Type	Method Options	List Type	Access Line	
□	dfltCmdAuthList	Commands	None	Default	Console,Telnet,SSH	
□	dfltExecAuthList	Exec	None	Default	Console,Telnet,SSH	
□	networkList	Network		Default	Dot1x	

Field	Description
List Name	The name of the authorization list. This field can be configured only when adding a new authorization list.
Authorization Type	The type of authorization list, which is one of the following: • **Command** – Determines which CLI commands a user is permitted to issue. When command authorization is enabled, each command a user enters must be validated before the command is executed. • **EXEC** – Determines whether a user can bypass User EXEC mode and enter Privileged EXEC mode directly after a successful Login authentication. • **Network** – Determines whether the user is permitted to access various network services. This authorization type
Method Options	The method(s) used to authorize a user's access to the device or network services. The possible methods are as follows: • **TACACS+** – When a user issues a CLI command, the device contacts the configured TACACS+ server to verify whether the user is allowed to issue the command. If approved, the command is

	executed. Otherwise, the command fails. • **RADIUS** – When a user is authenticated by the RADIUS server, the device downloads a list of permitted/denied commands from the RADIUS server. The list of authorized commands that are associated with the authenticated user is cached during the user's session. If this method is selected, the authentication method for the access type must also be RADIUS. • **Local** – Uses a list stored locally on the system to determine whether the user is authorized to access the given services. • **None** – No authorization is used. If the method is None, the authorization type is effectively disabled.
List Type	The type of authorization 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 authorization. The settings for this field are configured on the **Authorization Selection** page.

3.1.1.4 Authorization Selection

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



Authorization List Selection

Terminal		
Console	Exec dfltExecAuthList ▼	Commands dfltCmdAuthList ▼
Telnet	Exec dfltExecAuthList ▼	Commands dfltCmdAuthList ▼
SSH	Exec dfltExecAuthList ▼	Commands dfltCmdAuthList ▼

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

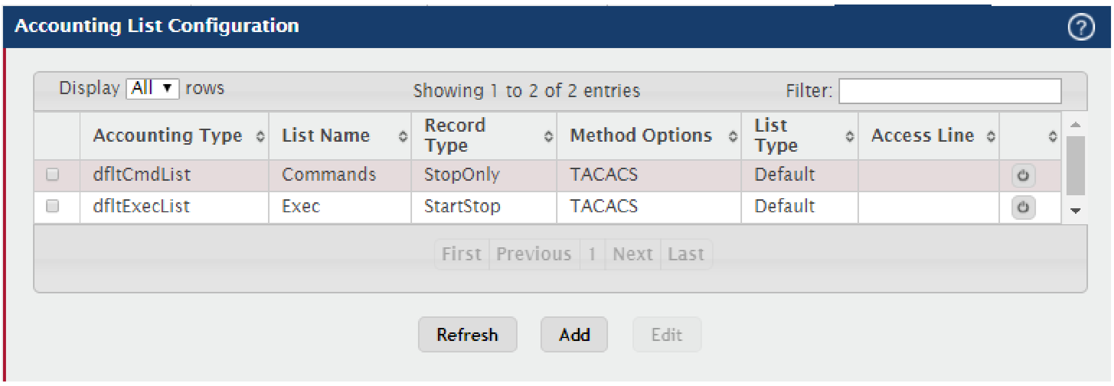
SSH	The Exec authorization list and the Commands authorization list to apply to users who access the CLI by using a secure shell (SSH) session.

3.1.1.5 Accounting List

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

Use the buttons to perform the following tasks:

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



Accounting List Configuration

Display All rows Showing 1 to 2 of 2 entries Filter:

	Accounting Type	List Name	Record Type	Method Options	List Type	Access Line	
□	dfltCmdList	Commands	StopOnly	TACACS	Default		
□	dfltExecList	Exec	StartStop	TACACS	Default		

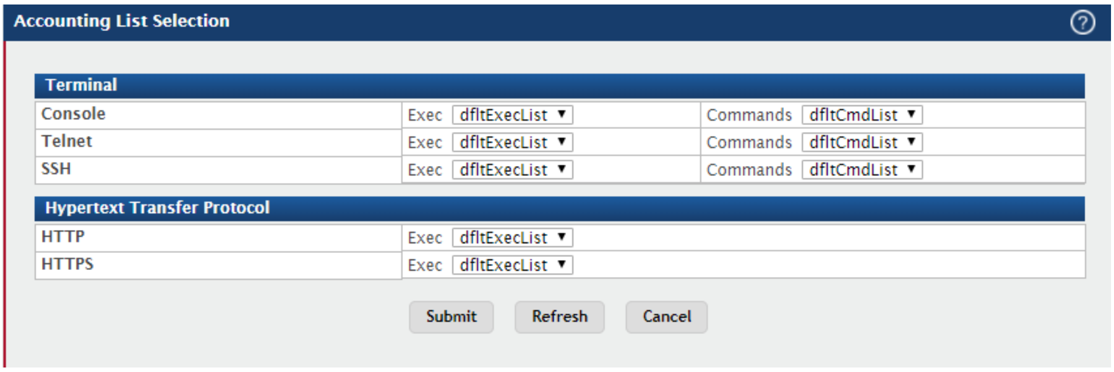
Field	Description
List Name	The name of the accounting list. This field can be configured only when adding a new accounting list.
Accounting Type	The type of accounting list, which is one of the following: • Command – Each CLI command executed by the user, along

	with the time the command was executed, is recorded and sent to an external AAA server. • EXEC – User login and logout times are recorded and sent to an external AAA server.
Record Type	Indicates when to record and send information about the user activity: StartStop – Accounting notifications are sent at the beginning and at the end of an exec session or a user-executed command. User activity does not wait for the accounting notification to be recorded at the AAA server. StopOnly – Accounting notifications are sent at the end of an exec session or a user-executed command. None – Accounting will not be notified.
Method Options	The method(s) used to record user activity. The possible methods are as follows: • TACACS+ – Accounting notifications are sent to the configured TACACS+ server. • RADIUS – Accounting notifications are sent to the configured RADIUS server.
List Type	The type of accounting 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 and Record Type settings are configurable. • Configured – The list has been added by a user.
Access Line	The access method(s) that use the list for accounting user activity. The settings for this field are configured on the Accounting Selection page. After you click Add or Edit, a window opens and allows you to configure accounting list settings. When adding an accounting list, you can configure the List Name, Accounting Type, and Record Type fields as well as the Accounting Methods. When editing an existing authentication list, only the Record Type and Accounting Methods can

	be configured. The following information describes how to set the Accounting Methods.

3.1.1.6 Accounting Select

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



Accounting List Selection

Terminal		
Console	Exec dfltExecList ▼	Commands dfltCmdList ▼
Telnet	Exec dfltExecList ▼	Commands dfltCmdList ▼
SSH	Exec dfltExecList ▼	Commands dfltCmdList ▼

Hypertext Transfer Protocol	
HTTP	Exec dfltExecList ▼
HTTPS	Exec dfltExecList ▼

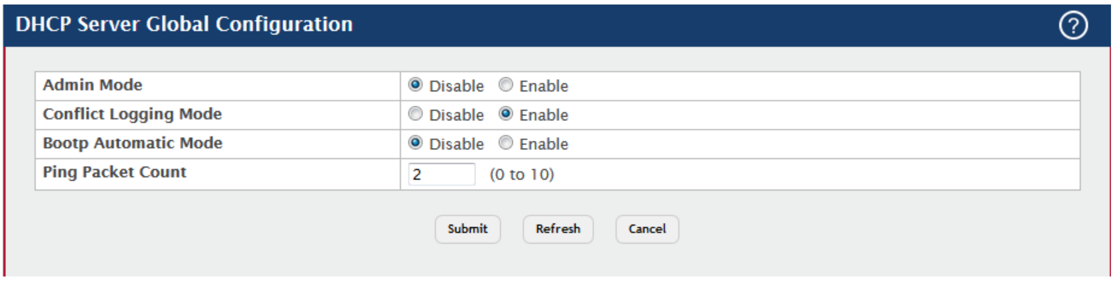
Field	Description
Exec	The accounting list to record user login and logout times.
Commands	The accounting list to record which actions a user takes on the system, such as page views or configuration changes. This list also records the time when the action occurred. For Terminal access methods, this list records the CLI commands a user executes and when each command is issued.
Terminal	
Console	The Exec accounting list and the Commands accounting list to apply to users who access the CLI by using a connection to the console port.
Telnet	The Exec accounting list and the Commands accounting list to apply to users who access the CLI by using a Telnet session.
SSH	The Exec accounting list and the Commands accounting list to apply to users who access the CLI by using a secure shell (SSH) session.
Hypertext Transfer Protocol	
HTTP	The Exec accounting list to apply to users who access the web-based management interface by using HTTP.
HTTPS	The Exec accounting list to apply to users who access the web-based management interface by using secure HTTP (HTTPS).

3.1.2 Advanced Configuration

3.1.2.1 DHCP Server

3.1.2.1.1 Global

Use this page to configure the global Dynamic Host Configuration Protocol (DHCP) server settings for the device. The device includes a DHCP server that can be configured to communicate with DHCP clients on the network and provide network information such as IP addresses, default gateways, and other network settings like DNS and SNTP server information.


DHCP Server Global Configuration

Admin Mode	● Disable ○ Enable
Conflict Logging Mode	○ Disable ● Enable
Bootp Automatic Mode	● Disable ○ Enable
Ping Packet Count	2 (0 to 10)

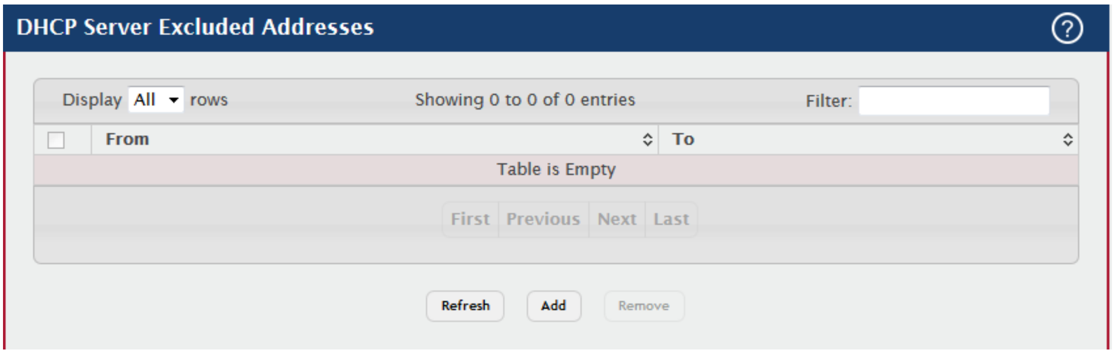
Field	Description
Admin Mode	Enables or disables the BOOTP automatic mode. When enabled, the DHCP server supports the allocation of automatic addresses for BOOTP clients. When disabled the DHCP server supports only static addresses for BOOTP clients.
Conflict Logging Mode	Enables or disables the BOOTP automatic mode. When enabled, the DHCP server supports the allocation of automatic addresses for BOOTP clients. When disabled the DHCP server supports only static addresses for BOOTP clients.
Bootp Automatic Mode	Enables or disables the BOOTP automatic mode. When enabled, the DHCP server supports the allocation of automatic addresses for BOOTP clients. When disabled the DHCP server supports only static addresses for BOOTP clients.
Ping Packet Count	The number of packets the server sends to a pool address to check for duplication as part of a ping operation. If the server receives a response to the ping, the address is considered to be in conflict and is removed from the pool.

3.1.2.1.2 Excluded Addresses

Use this page to view and configure the IP addresses the DHCP server should not assign to clients.

Use the buttons to perform the following tasks:

- To add one or more IP addresses to exclude, click Add and specify the IPv4 address or range of addresses in the available fields.
- To remove an excluded address or range of addresses, select each entry to delete and click Remove.



Field	Description
Form	The IP address to exclude. In a range of addresses, this value is the lowest address to exclude.
To	The highest address to exclude in a range of addresses. If the excluded address is not part of a range, this field shows the same value as the From field. When adding a single IP address to exclude, you can enter the same address specified in the From field or leave the field with the default value.

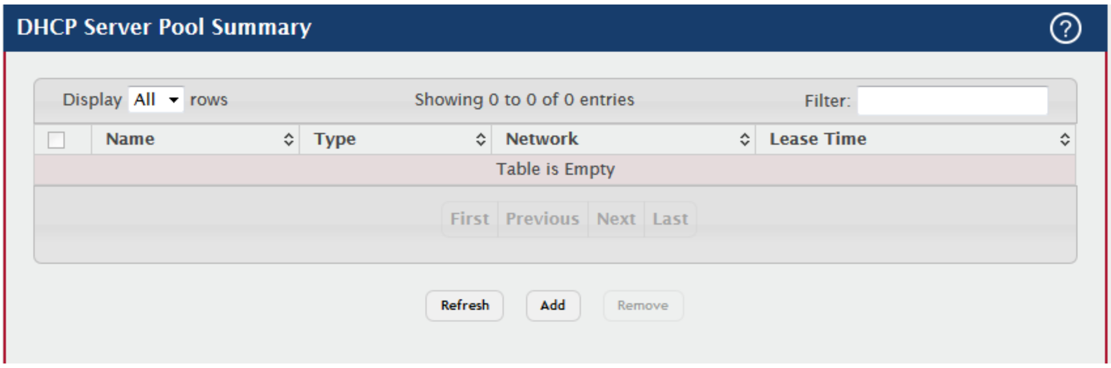
3.1.2.1.3 Poll Summary / Poll Configuration

Use this page to view the currently configured DHCP server pools and to add and remove pools. A DHCP server pool is a set of network configuration information available to DHCP clients that request the information.

Use the buttons to perform the following tasks:

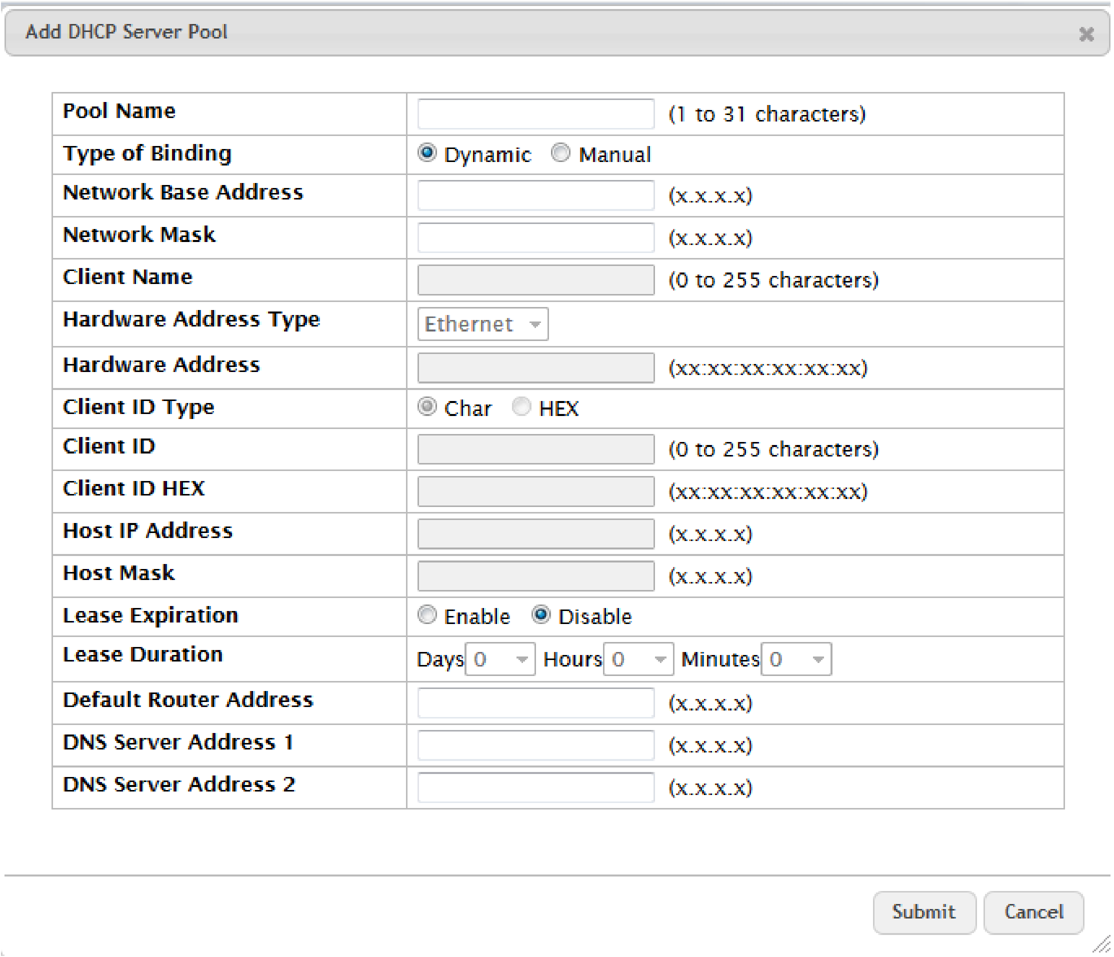
To add a pool, click Add and configure the pool information in the available fields.

To remove a pool, select each entry to delete and click Remove. You must confirm the action before the pool is deleted.



Display All rows Showing 0 to 0 of 0 entries Filter:

□	Name	Type	Network	Lease Time
Table is Empty				



Pool Name		(1 to 31 characters)
Type of Binding	● Dynamic ○ Manual	
Network Base Address		(x.x.x.x)
Network Mask		(x.x.x.x)
Client Name		(0 to 255 characters)
Hardware Address Type	Ethernet	
Hardware Address		(xx:xx:xx:xx:xx:xx)
Client ID Type	● Char ○ HEX	
Client ID		(0 to 255 characters)
Client ID HEX		(xx:xx:xx:xx:xx:xx)
Host IP Address		(x.x.x.x)
Host Mask		(x.x.x.x)
Lease Expiration	○ Enable ● Disable	
Lease Duration	Days 0 Hours 0 Minutes 0	
Default Router Address		(x.x.x.x)
DNS Server Address 1		(x.x.x.x)
DNS Server Address 2		(x.x.x.x)

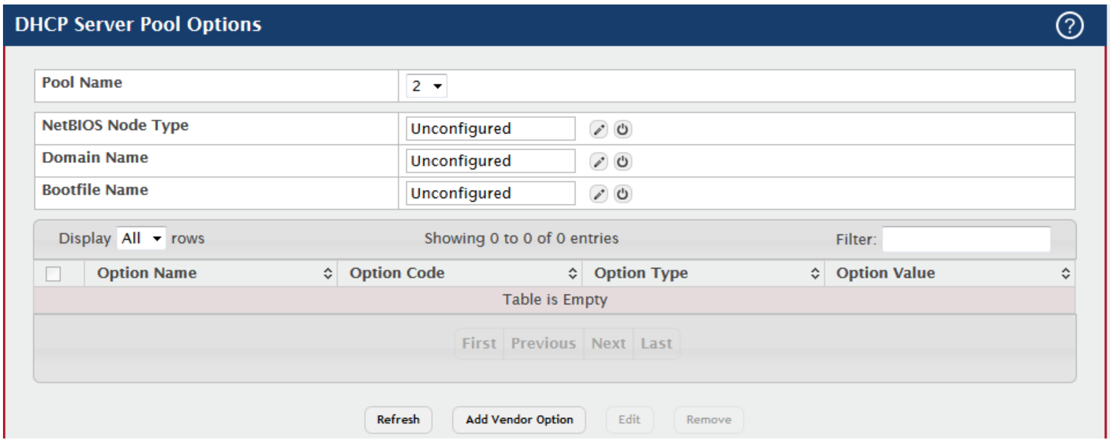
Field	Description
Name	The name that identifies the DHCP server pool.
Type of Binding	The type of binding for the pool. The options are: **Manual** – The DHCP server assigns a specific IP address to the client based on the client's MAC address. This type is also known as

	Static. **Dynamic** – The DHCP server can assign the client any available IP address within the pool. This type is also known as Automatic. **Undefined** – The pool has been created by using the CLI, but the pool information has not been configured.
Network	For a Manual pool, indicates the host IP address to assign the client. For a Dynamic pool, indicates the network base address.
Lease Time	The amount of time the information the DHCP server allocates is valid.
Network Base Address	(Dynamic pools only) The network portion of the IP address. A DHCP client can be offered any available IP address within the defined network as long as it has not been configured as an excluded address.
Network Mask	(Dynamic pools only) The subnet mask associated with the Network Base Address that separates the network bits from the host bits.
Client Name(optional)	(Manual pools only) The system name of the client. The Client Name should not include the domain name. Hardware Address Type
Hardware Address Type	(Manual pools only) The protocol type (Ethernet or IEEE 802) used by the client's hardware platform. This value is used in response to requests from BOOTP clients.
Hardware Address	(Manual pools only) The MAC address of the client.
Client ID	(Manual pools only) The value some DHCP clients send in the Client Identifier field of DHCP messages. This value is typically identical to the Hardware Address value. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of the hardware address. If the client's DHCP request includes the client identifier, the Client ID field on the DHCP server must contain the same value, and the Hardware Address Type field must be set to the appropriate value. Otherwise, the DHCP server will not respond to the client's request.
Host IP Address	(Manual pools only) The IP address to offer the client.
Host Mask	(Manual pools only) The subnet mask to offer the client.
Lease Duration	The number of Days, Hours, and Minutes the lease is valid. This field cannot be configured if the Lease Expiration Mode is disabled.
Defatul Router Address(Optional)	The IP address of the router to which the client should send traffic. The default router should be in the same subnet as the client. To add additional default routers, use the DHCP Server Pool Configuration

	page.
DNS Server Address (Optional)	The IP addresses of up to two DNS servers the client should use to resolve host names into IP addresses. To add additional DNS servers, use the DHCP Server Pool Configuration page.
NetBIOS Server	Lists the IP address of each NetBIOS Windows Internet Naming Service (WINS) name server that is available for the selected pool.

3.1.2.1.4 Poll Options

Use this page to configure additional DHCP pool options, including vendor-defined options. DHCP options are collections of data with type codes that indicate how the options should be used. When a client broadcasts a request for information, the request includes the option codes that correspond to the information the client wants the DHCP server to supply.



DHCP Server Pool Options

Pool Name	2
NetBIOS Node Type	Unconfigured
Domain Name	Unconfigured
Bootfile Name	Unconfigured

Display All rows Showing 0 to 0 of 0 entries Filter:

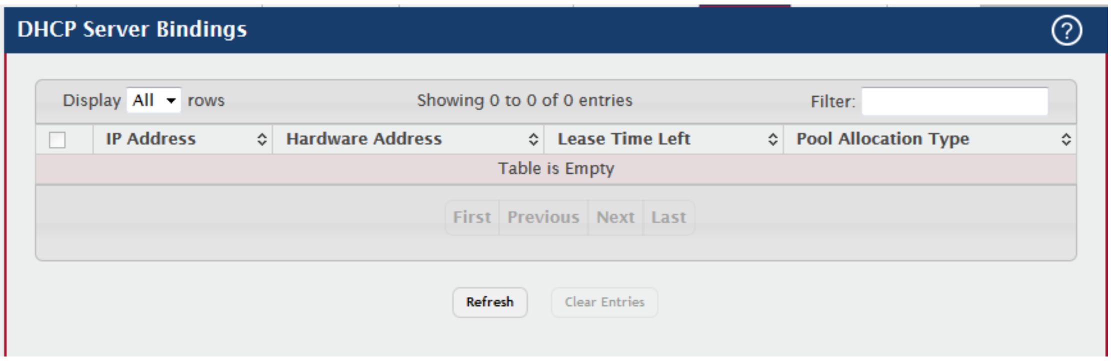
□	Option Name	Option Code	Option Type	Option Value
Table is Empty				

Field	Description
Pool Name	Select the pool to configure. The menu includes all pools that have been configured on the device.
NetBIOS Node Type	The method the client should use to resolve NetBIOS names to IP addresses. To configure this field, click the Edit icon in the row. To reset the field to the default value, click the Reset icon in the row. The options are: **B-Node Broadcast** – Broadcast only **P-Node Peer-to-Peer** – NetBIOS name server only **M-Node Mixed** – Broadcast, then NetBIOS name server **H-Node Hybrid** – NetBIOS name server, then broadcast
Domain Name	The default domain name to configure for all clients in the selected

	pool.
Bootfile Name	The name of the default boot image that the client should attempt to download from a specified boot server. The option table shows the Vendor Options that have been added to the selected pool. Use the buttons to perform the following tasks: To add a vendor option, click Add Vendor Option and configure the desired information in the available fields. To edit a vendor option, select the entry to change and click Edit. To remove a vendor option, select each entry to delete and click Remove. You must confirm the action before the entry is deleted.
Option Name	Identifies whether the entry is a fixed option or a vendor-defined option (Vendor).
Option Code	The number that uniquely identifies the option.
Option Type	The type of data to associate with the Option Code, which can be one of the following: **ASCII** **HEX** **IP Address**
Option Value	The data associated with the Option Code. When adding or editing a vendor option, the field(s) available for configuring the value depend on the selected Option Type. If the value you configure contains characters that are not allowed by the selected Option Type, the configuration cannot be applied.

3.1.2.1.5 Bindings

Use this page to view and delete entries in the DHCP Bindings table. After a client leases an IP address from the DHCP server, the server adds an entry to its database. The entry is called a binding.



DHCP Server Bindings

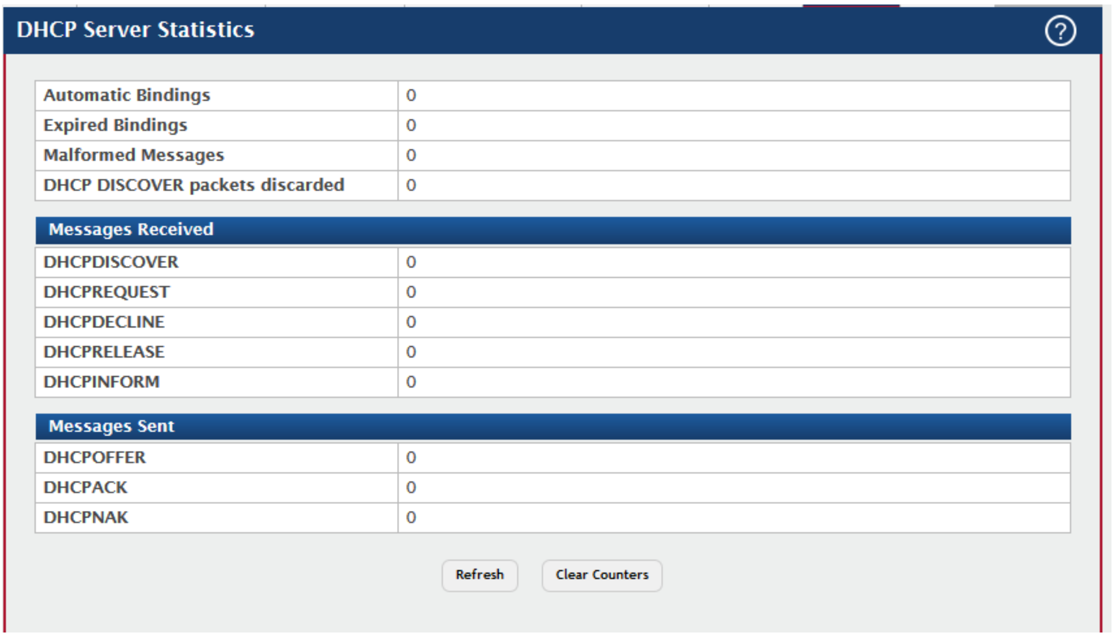
Display All rows   Showing 0 to 0 of 0 entries   Filter:

☐	IP Address	Hardware Address	Lease Time Left	Pool Allocation Type
Table is Empty				

Field	Description
IP Address	The IP Address of the DHCP client.
Hardware Address	The MAC address of the DHCP client.
Lease Time Left	The amount of time left until the lease expires in days, hours, and minutes.
Pool Allocation Type	The type of binding used: **Dynamic** – The address was allocated dynamically from a pool that includes a range of IP addresses. **Manual** – A static IP address was assigned based on the MAC address of the client. **Inactive** – The pool is not in use.
Clear Entries (Button)	To remove an entry from the table, select each entry to delete and click Clear Entries. You must confirm the action before the binding is deleted.

3.1.2.1.6 Statistics

This page displays the DHCP server statistics for the device, including information about the bindings and DHCP messages. The values on this page indicate the various counts that have accumulated since they were last cleared.



DHCP Server Statistics

Automatic Bindings	0
Expired Bindings	0
Malformed Messages	0
DHCP DISCOVER packets discarded	0

Messages Received	
DHCPDISCOVER	0
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0

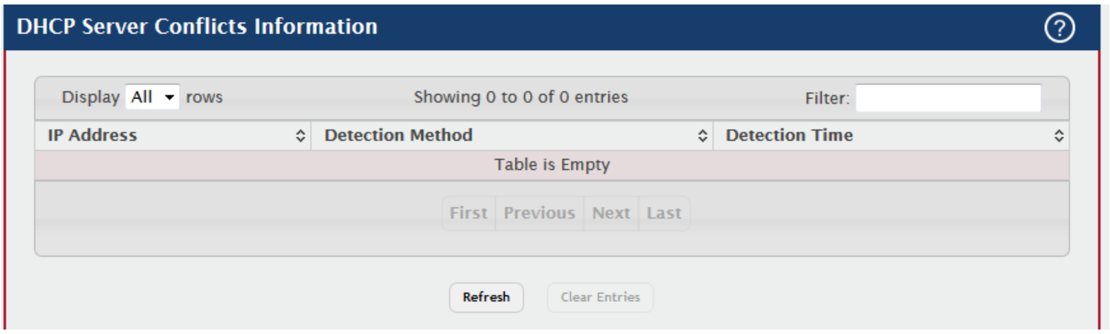
Messages Sent	
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

Field	Description
Automatic Bindings	The total number of IP addresses from all address pools with automatic bindings that the DHCP server has assigned to DHCP clients.
Expired Bindings	The number of IP addresses that the DHCP server has assigned to DHCP clients that have exceeded the configured lease time.
Malformed Messages	The number of messages received from one or more DHCP clients that were improperly formatted.
DHCP DISCOVER packets discarded	The number of messages discarded from one or more DHCP Discovers.
Messages Received	
DHCPDISCOVER	The number of DHCP discovery messages the DHCP server has received. A DHCP client broadcasts this type of message to discover available DHCP servers.
DHCPREQUEST	The number of DHCP request messages the DHCP server has received. A DHCP client broadcasts this type of message in response to a DHCP offer message it received from a DHCP server.
DHCPDECLINE	The number of DHCP decline messages the DHCP server has received from clients. A client sends a decline message if the DHCP client detects that the IP address offered by the DHCP server is already in use on the network. The server then marks the address as unavailable.
DHCPRELEASE	The number of DHCP release messages the DHCP server has

	received from clients. This type of message indicates that a client no longer needs the assigned address.
DHCPINFORM	The number of DHCP inform messages the DHCP server has received from clients. A client uses this type of message to obtain DHCP options.
Messages Sent	
DHCPOFFER	The number of DHCP offer messages the DHCP server has sent to DHCP clients in response to DHCP discovery messages it has received.
DHCPACK	The number of DHCP acknowledgement messages the DHCP server has sent to DHCP clients in response to DHCP request messages it has received. The server sends this message after the client has accepted the offer from this particular server. The DHCP acknowledgement message includes information about the lease time and any other configuration information that the DHCP client has requested.
DHCPNAK	The number of negative DHCP acknowledgement messages the DHCP server has sent to DHCP clients. A server might send this type of message if the client requests an IP address that is already in use or if the server refuses to renew the lease.
Clear Counters (Button)	Reset all DHCP server statistics counters.

3.1.2.1.7 Conflicts

This page displays information about IP address conflicts detected during the DHCP message exchange process between the server and client. An address conflict occurs when two hosts on the same network use the same IP address. Any address detected as a duplicate is removed from the pool and will not be offered to any DHCP clients until the conflict is resolved.



DHCP Server Conflicts Information

Display All rows | Showing 0 to 0 of 0 entries | Filter:

IP Address	Detection Method	Detection Time
Table is Empty		

Field	Description
IP Address	The IP address that has been detected as a duplicate.
Detection Method	The method used to detect the conflict, which is one of the following: **Gratuitous ARP** – The DHCP client detected the conflict by broadcasting an ARP request to the address specified in the DHCP offer message sent by the server. If the client receives a reply to the ARP request, it declines the offer and reports the conflict. **Ping** – The server detected the conflict by sending an ICMP echo message (ping) to the IP address before offering it to the DHCP client. If the server receives a response to the ping, the address is considered to be in conflict and is removed from the pool. **Host Declined** – The server received a DHCPDECLINE message from the host. A DHCPDECLINE message indicates that the host has discovered that the IP address is already in use on the network.
Detection Time	The time when the conflict was detected in days, hours, minutes and seconds since the system was last reset (i.e., system up time).
Clear Entries (Button)	Clears all of the address conflict entries.

3.1.2.2 DNS

3.1.2.2.1 Configuration

Use this page to configure the Domain Name System (DNS) client settings on the device, control the entries in the local domain name list, and add or remove the addresses of DNS servers the device can contact to resolve host names into IPv4 or IPv6 addresses.

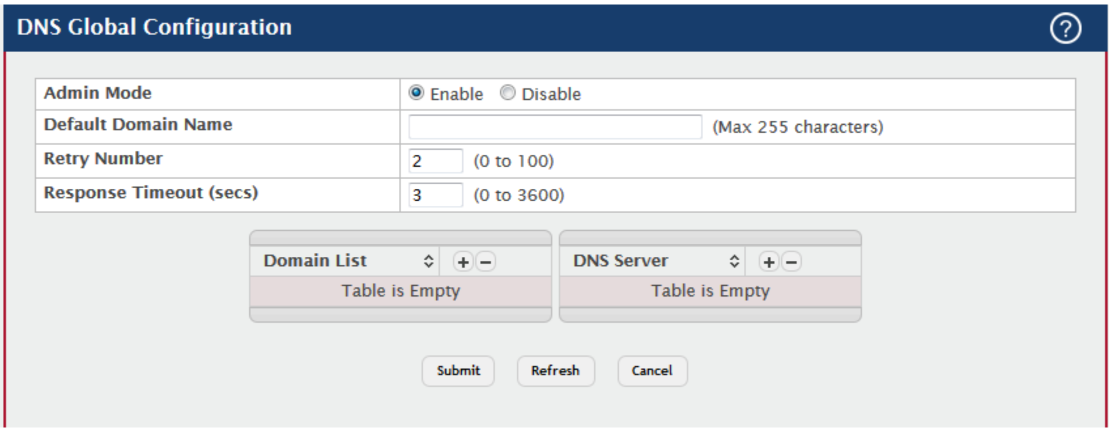
Use the buttons to perform the following tasks:

· To add an entry to the Domain List or list of DNS servers, click the + (plus) button and enter the desired information.

· To edit the IPv4 or IPv6 address of a configured DNS server, click the Edit icon associated with the entry to edit and update the desired information.

· To delete an entry from the list, click the – (minus) button associated with the entry to remove.

· To delete all entries from the list, click the – (minus) button in the heading row.



DNS Global Configuration

Admin Mode	● Enable ○ Disable
Default Domain Name	(Max 255 characters)
Retry Number	2 (0 to 100)
Response Timeout (secs)	3 (0 to 3600)

Domain List
Table is Empty

DNS Server
Table is Empty

\

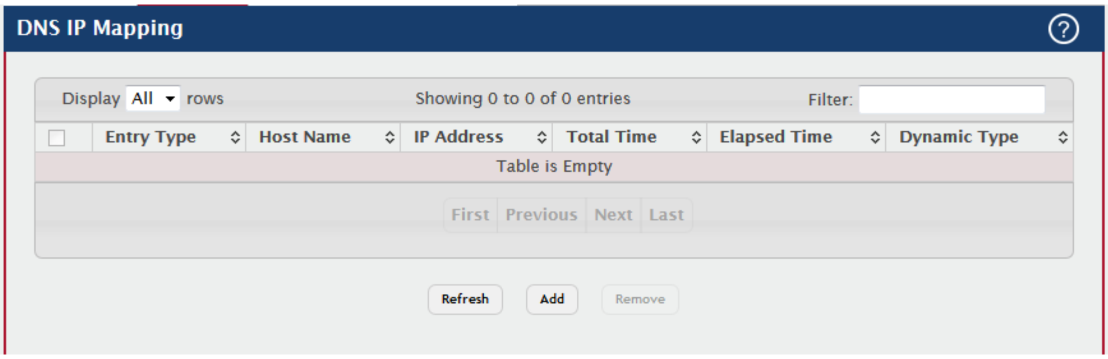
Field	Description
Admin Mode	The administrative mode of the DNS client.
Default Domain Name	The default domain name for the DNS client to use to complete unqualified host names. Domain names are typically composed of a series of labels concatenated with dots. After a default domain name is configured, if you enter a host name and do not include the domain name information, the default domain name is automatically appended to the host name.
Retry Number	The number of times the DNS client should attempt to send DNS queries to a DNS server on the network.
Response Timeout (secs)	The number of seconds the DNS client should wait for a response to a DNS query.
Domain List	The list of domain names that have been added to the DNS client's domain list. If a DNS query that includes the default domain name is not resolved, the DNS client attempts to use the domain names in this list to extend the hostname into a fully-qualified domain name. The DNS client uses the entries in the order that they appear in the list.
DNS Server	A unique IPv4 or IPv6 address used to identify a DNS server. The order in which you add servers determines the precedence of the server. The DNS server that you add first has the highest precedence and will be used before other DNS servers that you add.

3.1.2.2.2 IP Mapping

Use this page to view and manage the Static and Dynamic entries in the DNS IP mapping table. Use the buttons to perform the following tasks:

· To statically map an IP address to a hostname, click Add and configure the fields available in the Add DNS Entry dialog box.

· To delete one or more entries, select each entry to delete and click Remove.


DNS IP Mapping

Display All rows Showing 0 to 0 of 0 entries Filter:

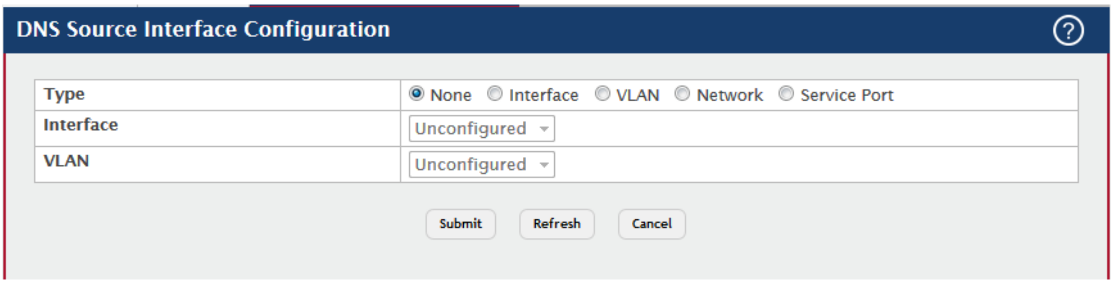
□	Entry Type	Host Name	IP Address	Total Time	Elapsed Time	Dynamic Type
Table is Empty						

Field	Description
Entry Type	Type of DNS entry: • Static – An entry that has been manually configured on the device. • Dynamic – An entry that the device has learned by using a configured DNS server to resolve a hostname.
Host Name	The name that identifies the system. For Static entries, specify the Host Name after you click Add. A host name can contain up to 255 characters if it contains multiple levels in the domain hierarchy, but each level (the portion preceding a period) can contain a maximum of 63 characters. If the host name you specify is a single level (does not contain any periods), the maximum number of allowed characters is 63.
IP Address	The IPv4 or IPv6 address associated with the configured Host Name. For Static entries, specify the IP Address after you click Add. You can specify either an IPv4 or an IPv6 address. The following fields include values for Dynamic entries only. For Static entries, these fields are blank.
Total Time	The number of seconds that the entry will remain in the table.
Elapsed Time	The number of seconds that have passed since the entry was added

	to the table. When the Elapsed Time reaches the Total Time, the entry times out and is removed from the table.
Dynamic Type	The type of address in the entry, for example IP or (less common) X.121.

3.1.2.2.3 Souce Interface Configuration

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



DNS Source Interface Configuration

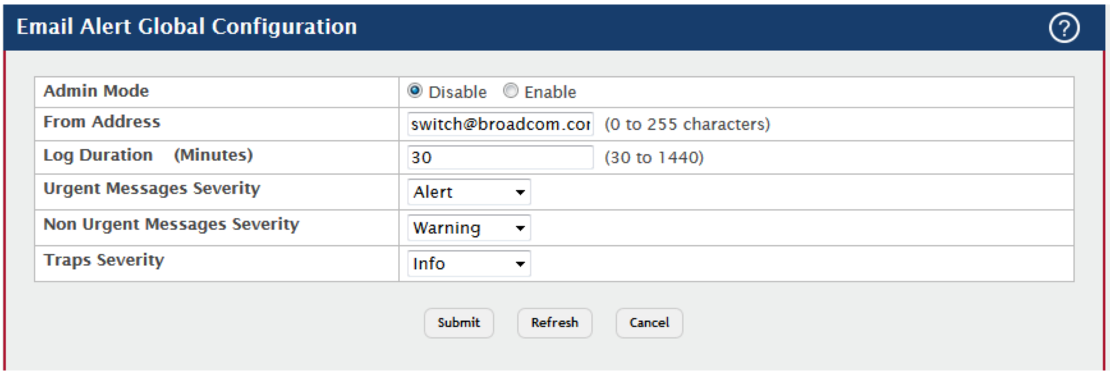
Type	● None ○ Interface ○ VLAN ○ Network ○ Service Port
Interface	Unconfigured
VLAN	Unconfigured

Field	Description
Type	The type of interface to use as the source interface: **None –** The primary IP address of the originating (outbound) interface is used as the source address. **Interface –** The primary IP address of a physical port is used as the source address. **VLAN –** The primary IP address of a VLAN routing interface is used as the source address. **Network –** The network source IP is used as the source address. **Service Port –** The management port source IP is used as the source address.
Interface	When the selected Type is Interface, select the physical port to use as the source interface. VLAN ID
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.

3.1.2.3 Email Alerts

3.1.2.3.1 Global

Use this page to configure system-wide settings for the Email Alert feature, which allows the device to send log messages to one or more email addresses. You must configure information about the network Simple Mail Transport Protocol (SMTP) server for email to be successfully sent from the device.



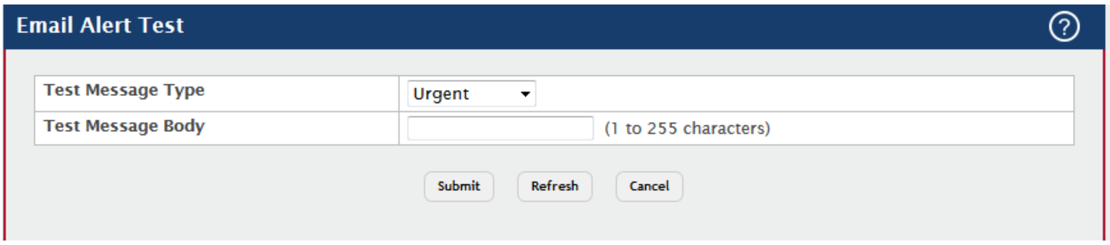
Email Alert Global Configuration

Admin Mode	● Disable ○ Enable
From Address	switch@broadcom.coı (0 to 255 characters)
Log Duration (Minutes)	30 (30 to 1440)
Urgent Messages Severity	Alert
Non Urgent Messages Severity	Warning
Traps Severity	Info

Field	Description
Admin Mode	Sets the administrative mode of the feature. • Enable – The device can send email alerts to the configured SMTP server. • Disable – The device will not send email alerts.
From Address	Specifies the email address of the sender (the device).
Log Duration	Determines how frequently the non critical messages are sent to the SMTP server.
Urgent Messages Severity	Configures the severity level for log messages that are considered to be urgent. Messages in this category are sent immediately. The security level you select and all higher levels are considered to be urgent.
Non Urgent Messages Severity	Configures the severity level for log messages that are considered to be nonurgent. Messages in this category are collected and sent in a digest form at the time interval specified by the Log Duration field. The security level you select and all levels up to, but not including the lowest Urgent Messages Severity level are considered nonurgent. Messages below the security level you specify are not sent via email
Traps Severity	The severity level for trap log messages.

3.1.2.3.2 Test

Use this page to verify that the email alert settings are configured properly. After you specify the settings on this page and click Submit, the device will use the configured SMTP server to send an email to the configured email addresses.



Email Alert Test

Test Message Type	Urgent
Test Message Body	(1 to 255 characters)

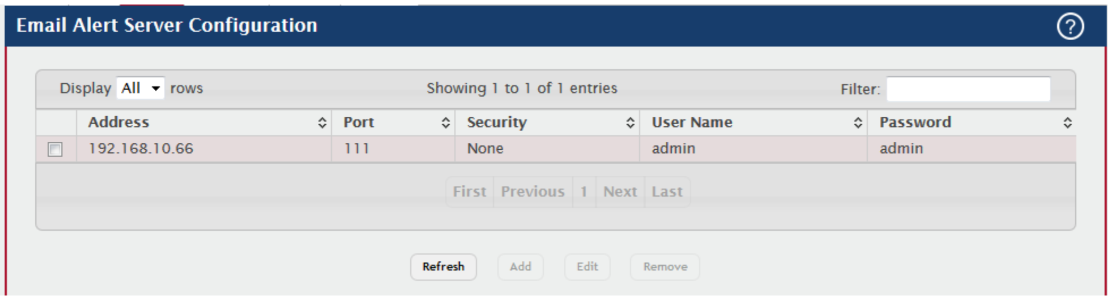
Field	Description
Test Message Type	Specifies the type of message to test for email alert functionality.
Test Message Body	Specifies the text contained in the body of the email alert test message.

3.1.2.3.3 Server

Use this page to add, edit, and remove information about the network SMTP (mail) server that handles email alerts sent from the device.

Use the buttons to perform the following tasks:

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



Email Alert Server Configuration

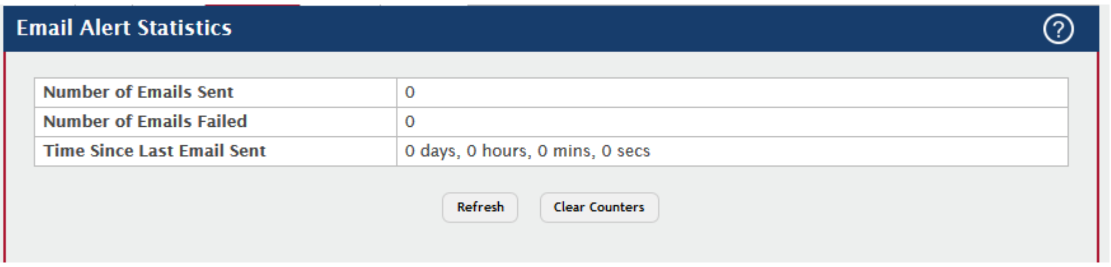
Display All rows Showing 1 to 1 of 1 entries Filter:

	Address	Port	Security	User Name	Password
□	192.168.10.66	111	None	admin	admin

Field	Description
Address	Shows the IPv4/IPv6 address or host name of the SMTP server that handles email alerts that the device sends.
Port	Specifies the TCP port that email alerts are sent to on the SMTP server.
Security	Specifies the type of authentication to use with the mail server, which can be TLSv1 (SMTP over SSL) or None (no authentication is required).
User Name	If the Security is TLSv1, this field specifies the user name required to access the mail server.
Password	If the Security is TLSv1, this field specifies the password associated with the configured user name for mail server access. When adding or editing the server, you must retype the password to confirm that it is entered correctly.

3.1.2.3.4 Statistics

Use this page to view information about the email alerts the device has sent or attempted to send. The statistics are cleared when the system is reset.

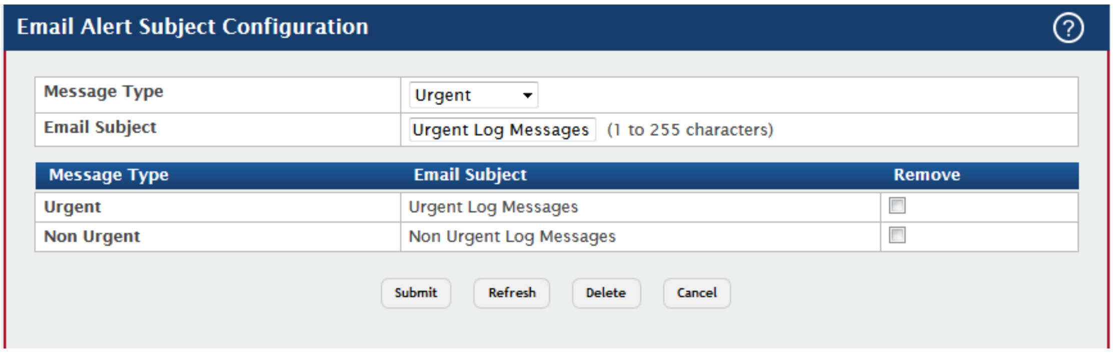


Number of Emails Sent	0
Number of Emails Failed	0
Time Since Last Email Sent	0 days, 0 hours, 0 mins, 0 secs

Field	Description
Number of Emails Sent	The number of email alerts that were successfully sent since the counters were cleared or the system was reset.
Number of Emails Failed	The number of email alerts that failed to be sent since the counters were cleared or system was reset.
Time Since Last Email Sent	The amount of time in days, hours, minutes, and seconds that has passed since the last email alert was successfully sent.
Clear Counters (Button)	Reset all email alert statistics counters to zero.

3.1.2.3.5 Subject

Use this page to view and edit the subject line of the urgent and non urgent email alert messages sent from the device.



Email Alert Subject Configuration

Message Type	Urgent
Email Subject	Urgent Log Messages (1 to 255 characters)

Message Type	Email Subject	Remove
Urgent	Urgent Log Messages	□
Non Urgent	Non Urgent Log Messages	□

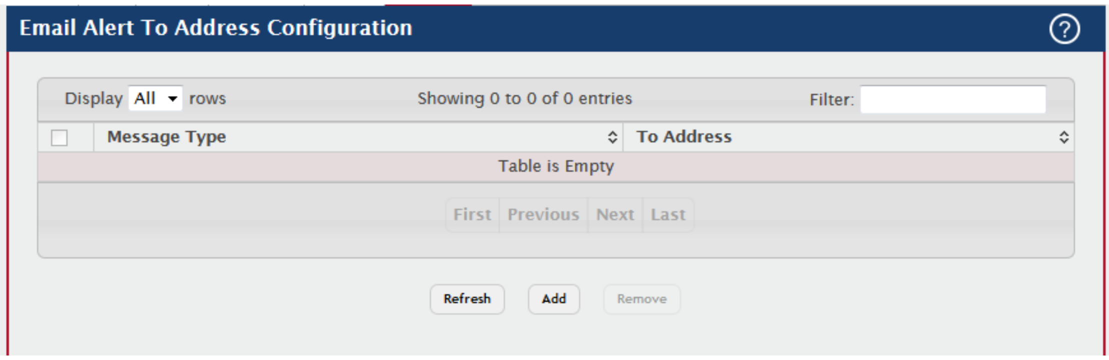
Field	Description
Message Type	Select the message type with the subject to edit.
Email Subject	Specify the text to be displayed in the subject of the email alert message for the selected message type.
Remove	To reset the email alert subject to the default value, select the Remove option associated with the message type to reset, and click Delete.

3.1.2.3.6 Address

Use this page to configure the email addresses to which email alert messages are sent.

Use the buttons to perform the following tasks:

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



Email Alert To Address Configuration

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Message Type	To Address
Table is Empty		

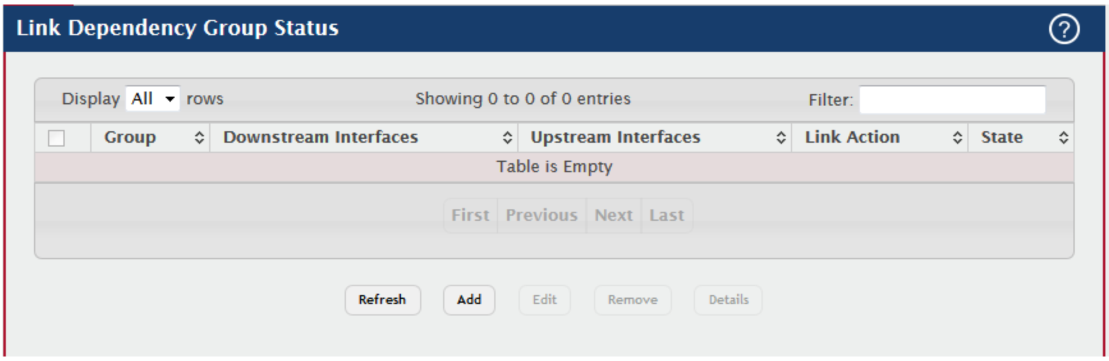
Field	Description
Message Type	Specifies whether to send urgent, non urgent, or both types of email alert message to the associated address.
To Address	The valid email address of an email alert recipient.

3.1.2.4 Link Dependency – Group

Use this page to configure link dependency groups. Link dependency allows the link status of one interface to be dependent on the link status of another interface. Link state groups define the interface link dependency.

Use the buttons to perform the following tasks:

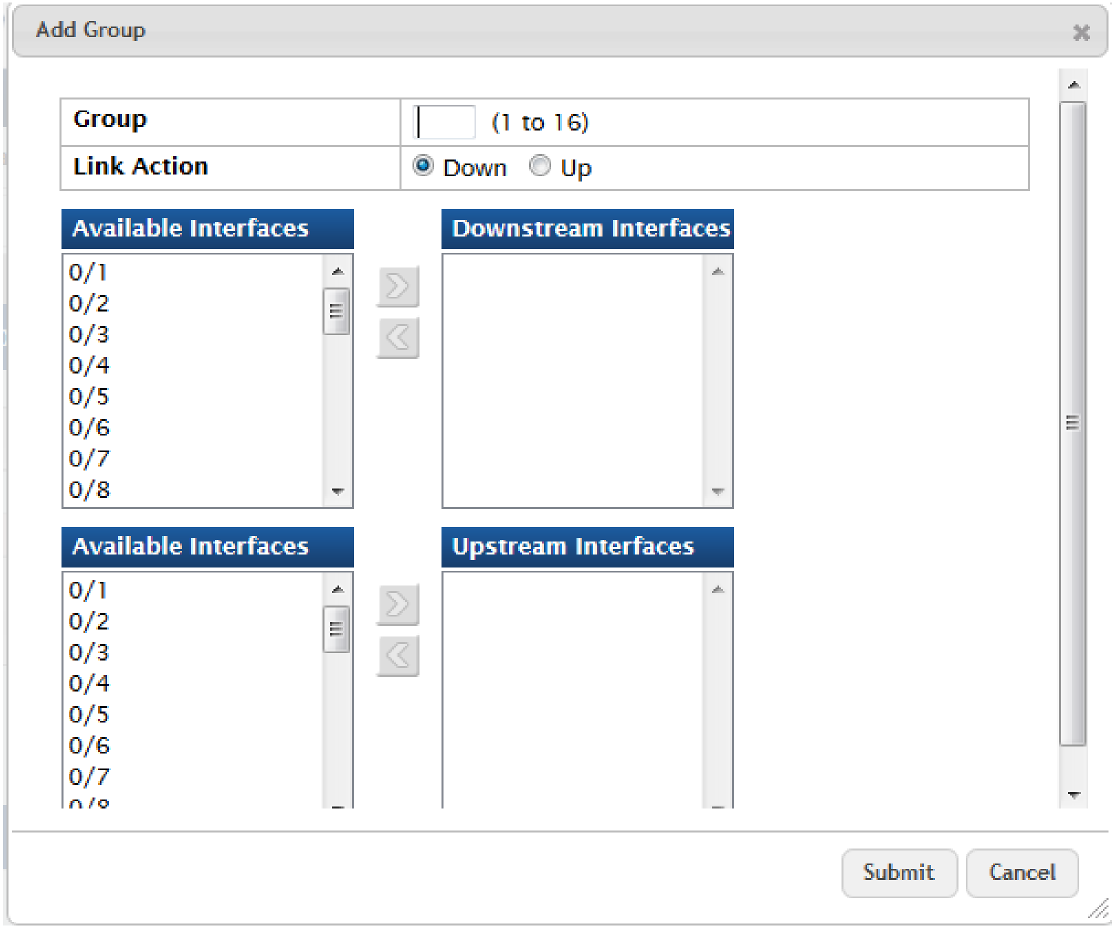
- To add a group, click **Add** and specify a group ID and other parameters in the available fields.
- To edit an existing group, select the entry to modify and click **Edit.** Then, configure the desired group settings.
- To remove one or more configured groups, select each entry to delete and click **Remove.** You must confirm the action before the entry is deleted.



Link Dependency Group Status

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Group	Downstream Interfaces	Upstream Interfaces	Link Action	State
Table is Empty					



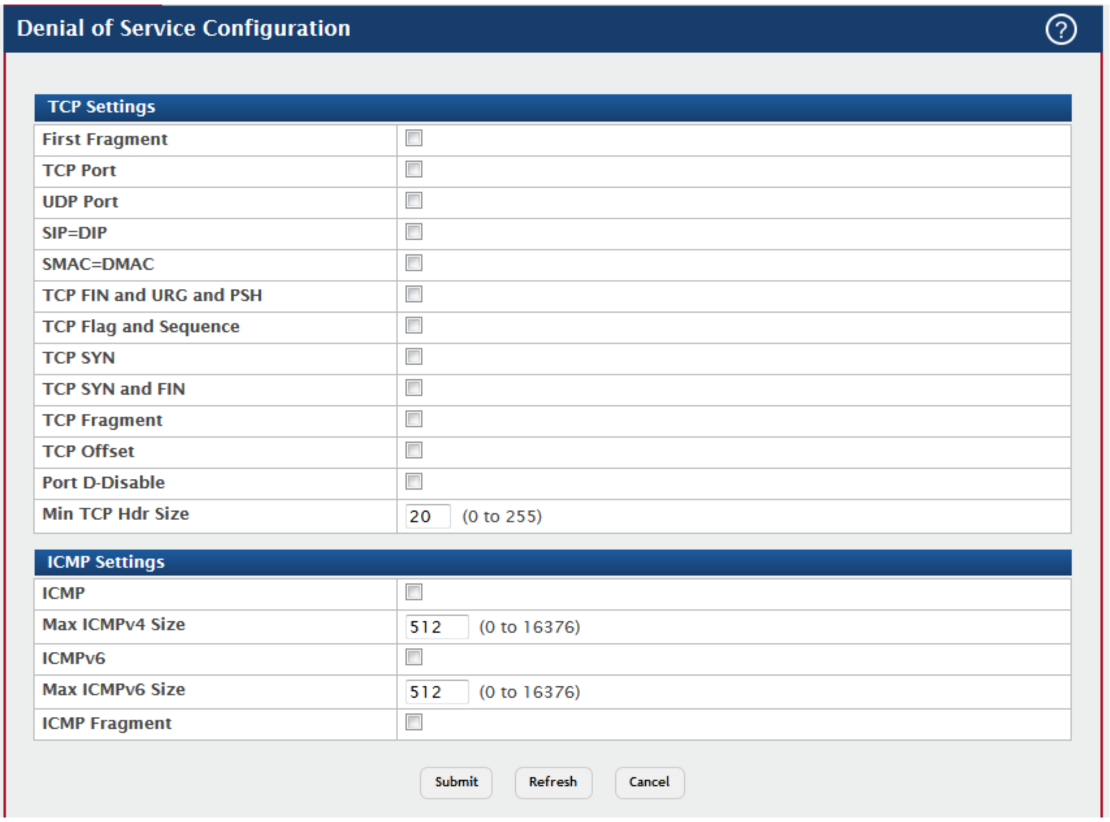
Group	(1 to 16)
Link Action	● Down ○ Up

Field	Description
Group	The unique link dependency group identifier.
Downstream Interfaces	The set of interfaces dependent on other interfaces.
Upstream Interfaces	The set of interfaces that other interfaces are dependent on.
Link Action	The action performed on downstream interfaces when the upstream interfaces are down, which can be one of the following: • **Up –** Downstream interfaces are up when upstream interfaces are down. • **Down –** Downstream interfaces go down when upstream interfaces are down.
State	The group state, which can be one of the following:

	• Up – Link action is up and no upstream interfaces have their link up, or link action is down and there are upstream interfaces that have their link up. • Down – Link is down when the above conditions are not true. After you click Add, the Add Group window opens and allows you to add groups. The following information describes the additional field in this window.
Available Interfaces	The interfaces that can be added to the group. An interface defined as an upstream interface cannot be defined as a downstream interface in the same link state group or in a different group. Similarly, an interface defined as a downstream interface cannot be defined as an upstream interface. To move an interface between the Available Interfaces and Downstream Interfaces or Upstream Interfaces fields, click the interface (or CTRL + click to select multiple interfaces), and then click the appropriate arrow to move the selected interfaces to the desired field. When you click Edit, the Edit Group window opens and allows you to edit an existing group. When you click Details, the Group Entry Details window opens. The following information describes the additional fields in this window.
Link Up	The list of upstream and downstream interfaces that currently have their link up.
Link Down	The list of upstream and downstream interfaces that currently have their link down.

3.1.2.5 Protection-Denial of Service

Use this page to configure settings that help prevent Denial of Service (DoS) attacks against the network. The system provides support for classifying and blocking several types of DoS attacks.



Denial of Service Configuration

TCP Settings	
First Fragment	□
TCP Port	□
UDP Port	□
SIP=DIP	□
SMAC=DMAC	□
TCP FIN and URG and PSH	□
TCP Flag and Sequence	□
TCP SYN	□
TCP SYN and FIN	□
TCP Fragment	□
TCP Offset	□
Port D-Disable	□
Min TCP Hdr Size	20 (0 to 255)

ICMP Settings	
ICMP	□
Max ICMPv4 Size	512 (0 to 16376)
ICMPv6	□
Max ICMPv6 Size	512 (0 to 16376)
ICMP Fragment	□

Field	Description
TCP Settings	These options help prevent the device and the network from attacks that exploit the TCP header size or the information in the TCP or UDP headers of packets that the device receives.
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	Enable this option to allow the device to drop packets that have TCP

Sequence	control flags set to 0 and the TCP sequence number set to 0.
TCP SYN	Enable this option to allow the device to drop packets that have TCP Flags SYN set.
TCP SYN and FIN	Enable this option to allow the device to drop packets that have TCP Flags SYN and FIN set.
TCP Fragment	Enable this option to allow the device to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
TCP Offset	Enable this option to allow the device to drop packets that have a TCP header Offset set to 1.
Port D-Disable	Enable this option to allow the device to diagnostically disable the interface which may be exposed to DoS attacks.
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 field.
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.
ICMP Fragment	Enable this option to allow the device to drop fragmented ICMP packets.

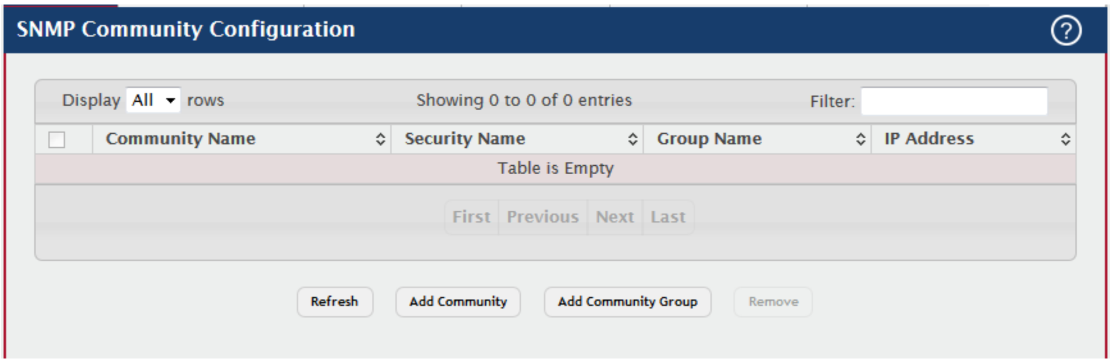
3.1.2.6 SNMP

3.1.2.6.1 Community

Use this page to define SNMP communities for SNMPv1 and SNMPv2. Access rights for SNMPv1 and SNMPv2 are managed by defining communities. When the community names are changed, access rights are also changed.

Use the buttons to perform the following tasks:

- To add a community, click Add and configure the desired settings.
- To delete a configured community from the list, select the check box associated with each entry to delete and click Remove.



SNMP Community Configuration

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Community Name	Security Name	Group Name	IP Address
Table is Empty				

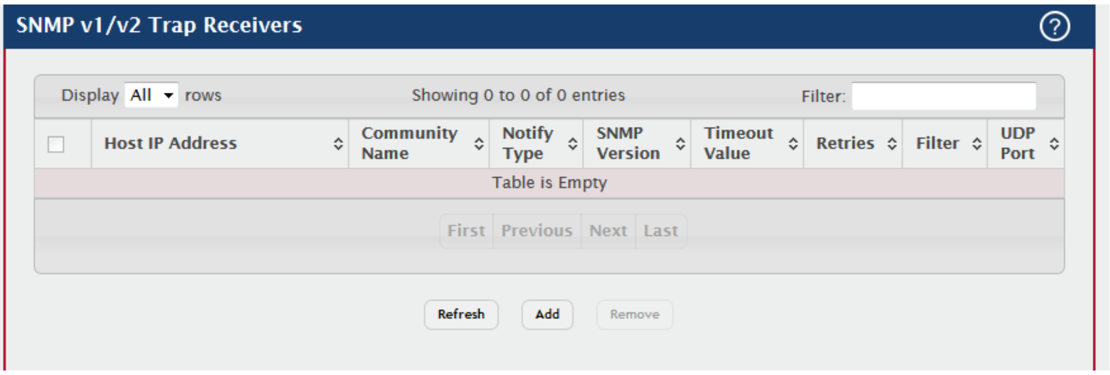
Field	Description
Community Name	Community name used in SNMPv1/v2 packets. This is configured in the client and identifies the access the user may connect with.
Security Name	Identifies the Security entry that associates Communities and Groups for a specific access type.
Group Name	Identifies the Group associated with this Community entry.
Community Access	Specifies the access control policy for the community.
Community View	Specifies the community view for the community. If the value is empty, then no access is granted.
IP Address	Specifies the IP address that can connect with this community.
Add Community Group (Button)	Add a new SNMP Community Group.

3.1.2.6.2 Trap Receiver v1 / v2

Use this 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.

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.



SNMP v1/v2 Trap Receivers

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Host IP Address	Community Name	Notify Type	SNMP Version	Timeout Value	Retries	Filter	UDP Port
Table is Empty								

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.

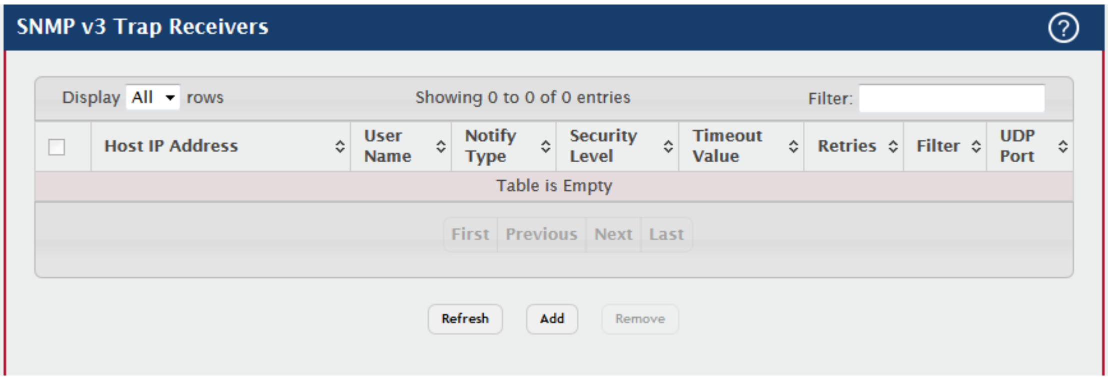
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP management host.
Filter	The name of the filter for the SNMP management host. The filter is configured by using the CLI and defines which MIB objects to include or exclude from the view. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

3.1.2.6.3 Trap Receiver v3

Use this page to configure settings for each SNMPv3 management host that will receive notifications about traps generated by the device. The SNMP management host is also known as the SNMP trap receiver.

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.**


SNMP v3 Trap Receivers

Display All rows   Showing 0 to 0 of 0 entries   Filter:

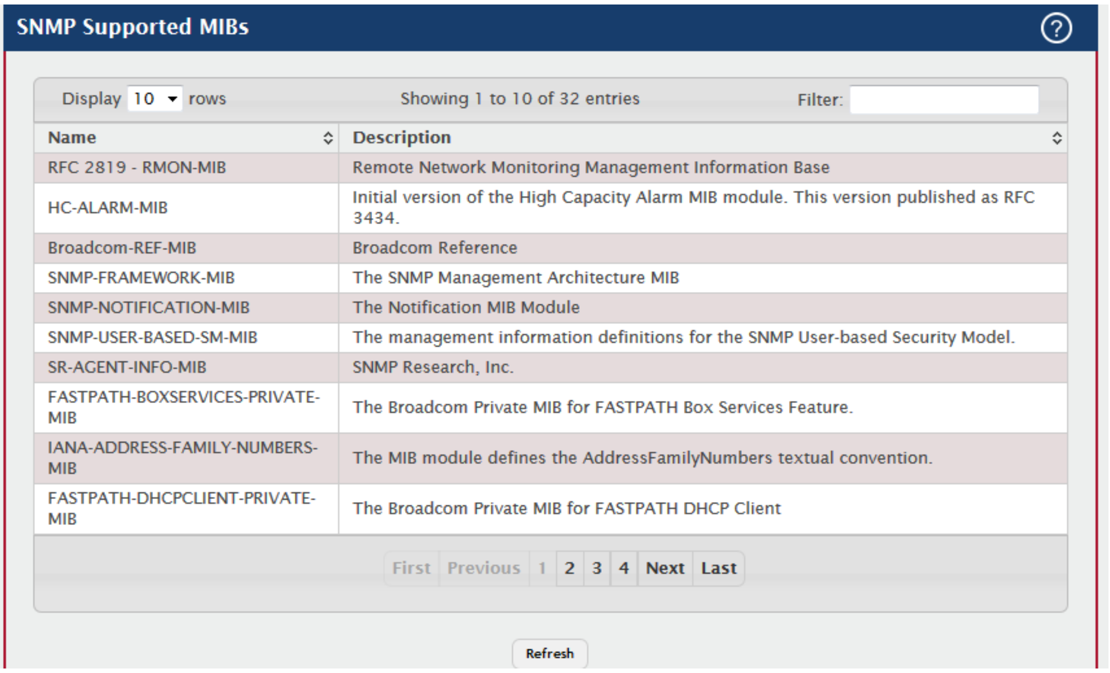
□	Host IP Address	User Name	Notify Type	Security Level	Timeout Value	Retries	Filter	UDP Port
Table is Empty								

Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the device.
User Name	The name of the SNMP user that is authorized to receive the SNMP notification.
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. **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.
Security Level	The security level associated with the SNMP user, which is one of the following: **No Auth No Priv** – No authentication and no data encryption (no security). **Auth No Priv** – Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption. **Auth Priv** – Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.
Timeout Value	The number of seconds to wait for an acknowledgment from the SNMP receiver before resending an inform message.
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP receiver.
Filter	The name of the filter for the SNMP management host. The filter is configured by using the CLI and defines which MIB objects to include or exclude from the view. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

3.1.2.6.4 Supported MIBs

This page displays the list of all MIBs supported by the SNMP management agent running on this device.



SNMP Supported MIBs

Display 10 rows Showing 1 to 10 of 32 entries Filter:

Name	Description
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
HC-ALARM-MIB	Initial version of the High Capacity Alarm MIB module. This version published as RFC 3434.
Broadcom-REF-MIB	Broadcom Reference
SNMP-FRAMEWORK-MIB	The SNMP Management Architecture MIB
SNMP-NOTIFICATION-MIB	The Notification MIB Module
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SR-AGENT-INFO-MIB	SNMP Research, Inc.
FASTPATH-BOXSERVICES-PRIVATE-MIB	The Broadcom Private MIB for FASTPATH Box Services Feature.
IANA-ADDRESS-FAMILY-NUMBERS-MIB	The MIB module defines the AddressFamilyNumbers textual convention.
FASTPATH-DHCPCLIENT-PRIVATE-MIB	The Broadcom Private MIB for FASTPATH DHCP Client

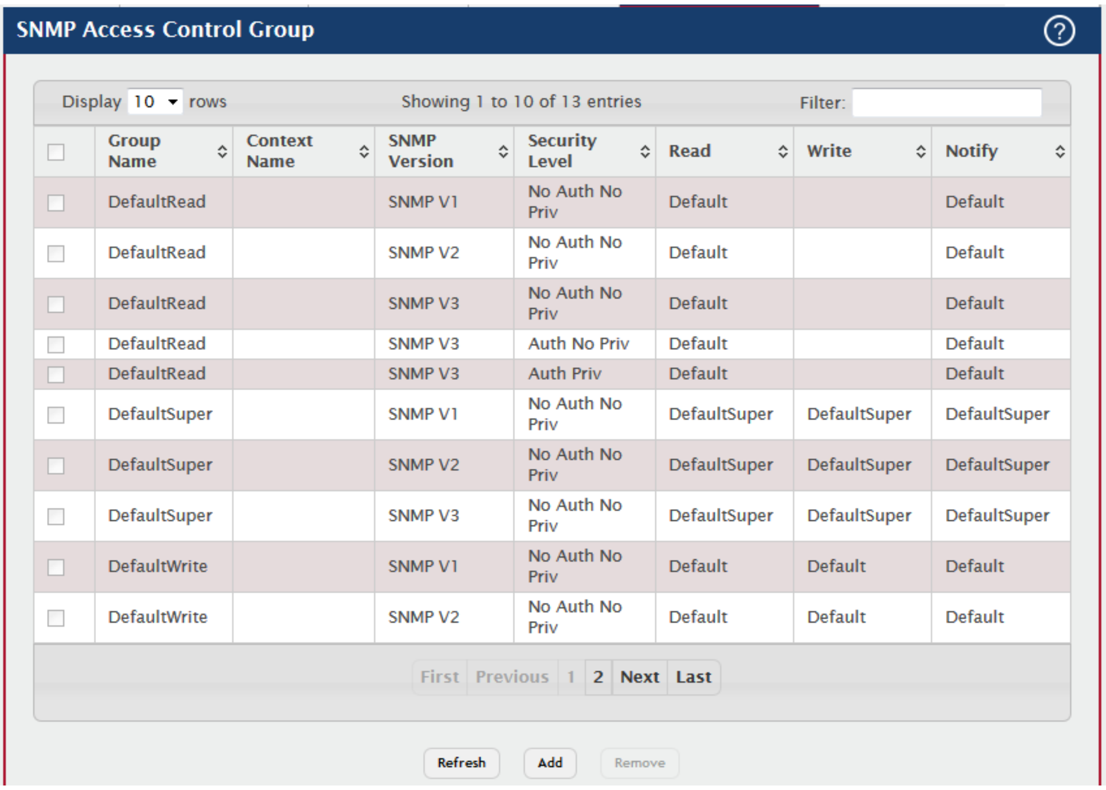
Field	Description
Name	The RFC number, if applicable, followed by the defined name of the MIB.
Description	The RFC title, or a brief description of the MIB.

3.1.2.6.5 Access Control Group

Use this page to configure SNMP access control groups. These SNMP groups allow network managers to assign different levels of authorization and access rights to specific device features and their attributes. The SNMP group can be referenced by the SNMP community to provide security and context for agents receiving requests and initiating traps as well as for management systems and their tasks. An SNMP agent will not respond to a request from a management system outside of its configured group, but an agent can be a member of multiple groups at the same time to allow communication with SNMP managers from different groups. Several default SNMP groups are preconfigured on the system.

Use the buttons to perform the following tasks:

- To add an SNMP group, click **Add** and specify the desired settings.
- To remove one or more SNMP groups, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.



SNMP Access Control Group

Display 10 rows Showing 1 to 10 of 13 entries Filter:

□	Group Name	Context Name	SNMP Version	Security Level	Read	Write	Notify
□	DefaultRead		SNMP V1	No Auth No Priv	Default		Default
□	DefaultRead		SNMP V2	No Auth No Priv	Default		Default
□	DefaultRead		SNMP V3	No Auth No Priv	Default		Default
□	DefaultRead		SNMP V3	Auth No Priv	Default		Default
□	DefaultRead		SNMP V3	Auth Priv	Default		Default
□	DefaultSuper		SNMP V1	No Auth No Priv	DefaultSuper	DefaultSuper	DefaultSuper
□	DefaultSuper		SNMP V2	No Auth No Priv	DefaultSuper	DefaultSuper	DefaultSuper
□	DefaultSuper		SNMP V3	No Auth No Priv	DefaultSuper	DefaultSuper	DefaultSuper
□	DefaultWrite		SNMP V1	No Auth No Priv	Default	Default	Default
□	DefaultWrite		SNMP V2	No Auth No Priv	Default	Default	Default

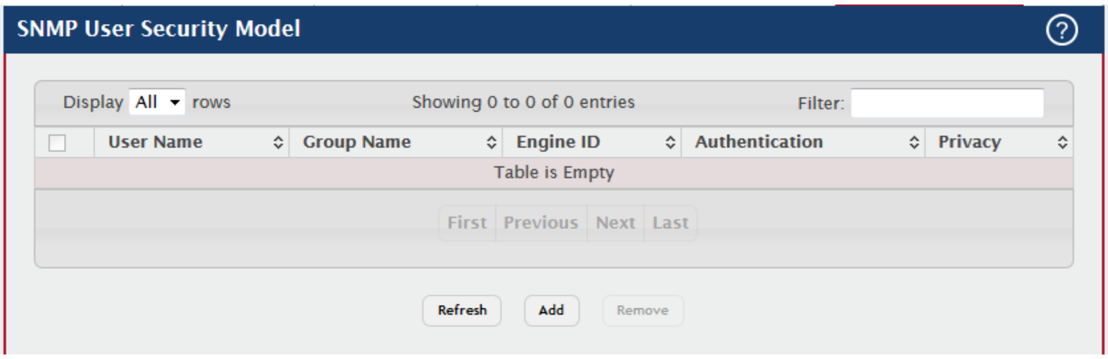
Field	Description
Group Name	The name that identifies the SNMP group.
Context Name	The SNMP context associated with the SNMP group and its views. A user or a management application specifies the context name to get the performance information from the MIB objects associated with that context name. The Context EngineID identifies the SNMP entity that should process the request (the physical router), and the Context Name tells the agent in which context it should search for the objects requested by the user or the management application.
SNMP Version	The SNMP version associated with the group.
Security Level	The security level associated with the group, which is one of the following: **No Auth No Priv** – No authentication and no data encryption (no security). This is the only Security Level available for SNMPv1 and SNMPv2 groups. **Auth No Priv** – Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.

	Auth Priv – Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.
Read	The level of read access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that restricts management access to viewing the contents of the agent.
Write	The level of write access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that permits management read-write access to the contents of the agent but not to the community.
Notify	The level of notify access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that permits sending SNMP traps or informs.

3.1.2.6.6 User Security Model

This page provides the capability to configure the SNMP V3 user account(s).

- To add a user, click **Add**. The **Add New SNMP User** dialog box opens. Specify the new account information in the available fields.
- To remove a user, select one or more table entries and click **Remove** to delete the selected entries.


SNMP User Security Model

Display All rows   Showing 0 to 0 of 0 entries   Filter:

□	User Name	Group Name	Engine ID	Authentication	Privacy
Table is Empty					

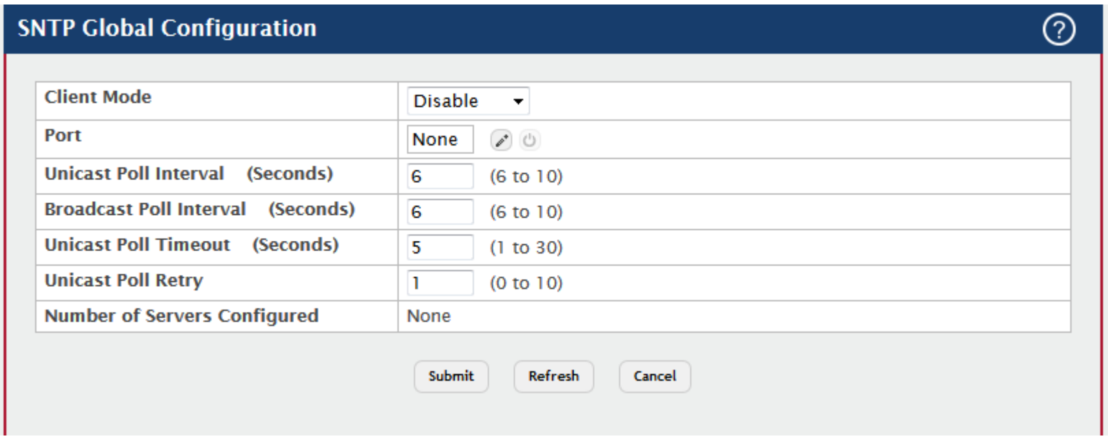
Field	Description
Engine ID	Each SNMPv3 agent has an engine ID that uniquely identifies the agent in the device. If given this entry will be used only for packets whose engine id is this. This field takes an hexadecimal string in the

	form 0102030405.
User Name	Specifies the name of the SNMP user being added for the User-based Security Model (USM). Each user name must be unique within the SNMP agent user list. A user name cannot contain any leading or embedded blanks.
Group Name	A SNMP group is a group to which hosts running the SNMP service belong. A group name parameter is simply the name of that group by which SNMP communities are identified. The use of a group name provides some security and context for agents receiving requests and initiating traps and does the same for management systems and their tasks. An SNMP agent won't respond to a request from a management system outside its configured group, but an agent can be a member of multiple groups at the same time. This allows for communications with SNMP managers from different groups.
Authentication Method	Specifies the authentication protocol to be used on authenticated messages on behalf of the specified user. **None -** No authentication will be used for this user. **MD5** - MD5 protocol will be used. **SHA** - SHA protocol will be used.
Password	Specifies the password used to generate the key to be used in authenticating messages on behalf of this user. This parameter must be specified if the Authentication method parameter is not None.
Privacy	Specifies the privacy protocol to be used on encrypted messages on behalf of the specified user. This parameter is only valid if the Authentication method parameter is not None. **None -** No privacy protocol will be used. **DES** - DES protocol will be used.
Authentication Key	Specifies the password used to generate the key to be used in encrypting messages to and from this user. This parameter must be specified if the Privacy parameter is not None.

3.1.2.7 SNTP

3.1.2.7.1 Global Configuration

Use this page to enable the Simple Network Time Protocol (SNTP) client on the device and to configure the SNTP client settings. Enabling and configuring the SNTP client allows the device to synchronization the system time with a valid SNTP server on the network.



SNTP Global Configuration

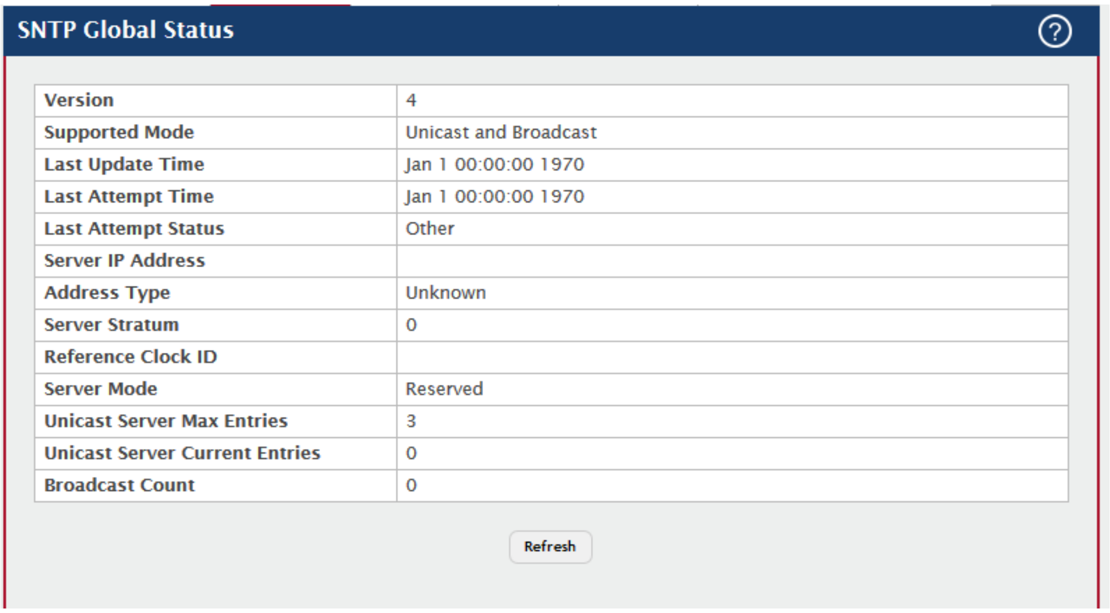
Client Mode	Disable
Port	None
Unicast Poll Interval (Seconds)	6 (6 to 10)
Broadcast Poll Interval (Seconds)	6 (6 to 10)
Unicast Poll Timeout (Seconds)	5 (1 to 30)
Unicast Poll Retry	1 (0 to 10)
Number of Servers Configured	None

Field	Description
Client Mode	Specifies the mode of operation of SNTP Client. An SNTP client may operate in 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.
Unicast Poll Interval	Specifies the interval, in seconds, between unicast poll requests expressed as a power of two when configured in unicast mode.
Broadcast Poll Interval	Specifies the interval, in 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.

Unicast Poll Timeout	Specifies the timeout value, in seconds, to wait for an SNTP response when configured in unicast mode.
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.
Number of Servers Configured	Specifies the number of current valid unicast server entries configured for this client.

3.1.2.7.2 Global Status

This page displays global status information related to SNTP operation in the device.



SNTP Global Status

Version	4
Supported Mode	Unicast and Broadcast
Last Update Time	Jan 1 00:00:00 1970
Last Attempt Time	Jan 1 00:00:00 1970
Last Attempt Status	Other
Server IP Address	
Address Type	Unknown
Server Stratum	0
Reference Clock ID	
Server Mode	Reserved
Unicast Server Max Entries	3
Unicast Server Current Entries	0
Broadcast Count	0

Field	Description
Version	Specifies the SNTP version the client supports.
Supported Mode	Specifies the SNTP modes the client supports. A single client can support multiple modes.
Last Update Time	Specifies the local date and time (UTC) when the SNTP client last updated the system clock.
Last Attempt Time	Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.
Last Attempt Status	Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes.

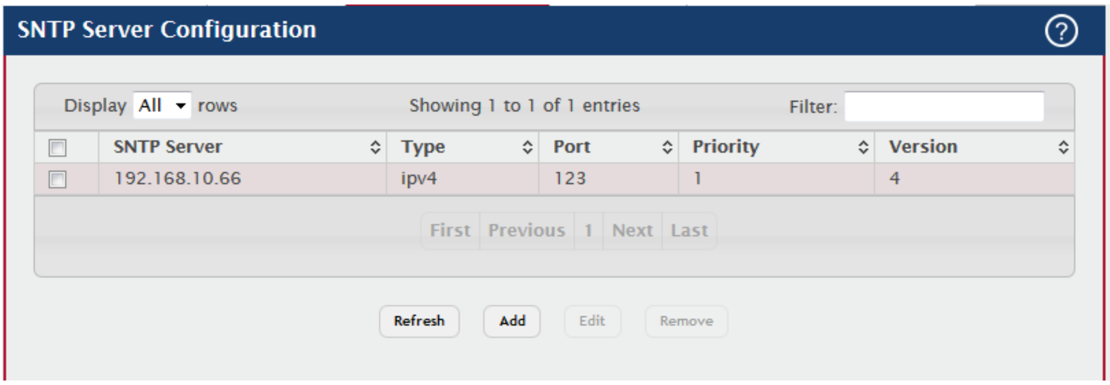
	Other – None of the following values apply, or no message has been received. **Success** – The SNTP operation was successful, and the system time was updated. **Request Timed Out** – A directed SNTP request timed out without receiving a response from the SNTP server. **Bad Date Encoded** – The time provided 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. **Kiss Of Death Rate Exceeded** – SNTP server status for the rate exceeded case.
Server IP Address	Specifies the IP address or hostname 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 (IP address or DNS hostname) of the SNTP server for the last received valid packet.
Server Stratum	Specifies the claimed stratum of the server for the last received valid packet. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock.
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 Server 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 the last reboot.

3.1.2.7.3 Server Configuration

Use this page to add and remove the addresses of one or more SNTP servers the device can contact to synchronize the system time and to configure various information about the SNTP servers.

Use the buttons to perform the following tasks:

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



SNTP Server Configuration

Display All rows Showing 1 to 1 of 1 entries Filter:

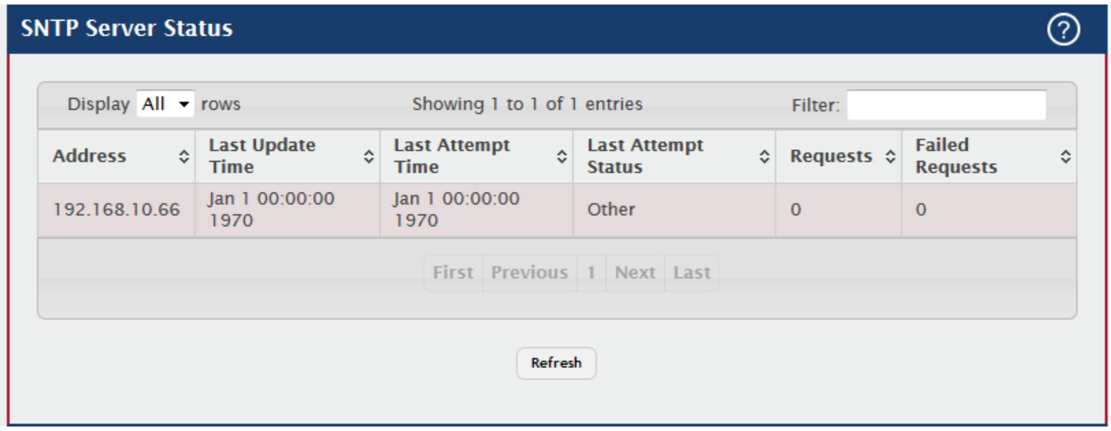
□	SNTP Server	Type	Port	Priority	Version
□	192.168.10.66	ipv4	123	1	4

Field	Description
SNTP Server	The address or host name of an SNTP server the device can use to synchronize the system time.
Type	The configured SNTP server address type, which can be ipv4 , ipv6, or DNS.
Port	The UDP port on the server to which SNTP requests are sent.
Priority	The order in which to query the servers. The SNTP client on the device continues sending SNTP requests to different servers until a successful response is received or all servers are exhausted. A server entry with a lower priority value is queried before one with a higher priority. If more than one server has the same priority, the SNTP client contacts the servers in the order that they appear in the table.
Version	Specifies the NTP version running on the server. After you click Add, the Add SNTP Server window opens and allows you to configure information about the new SNTP server. In addition

	to other fields previously described, the window includes the Host Name or IP Address field. The following information describes this field.
Host Name or IP Address	Specify the IPv4 address, IPv6 address, or DNS-resolvable host name of the SNTP server. Unicast SNTP requests will be sent to this address. The address you enter is displayed in the SNTP Server field on the main page. The address type is automatically detected.

3.1.2.7.4 Server Status

This page displays status information for all SNTP servers that have been configured on the device.



SNTP Server Status

Display All rows   Showing 1 to 1 of 1 entries   Filter:

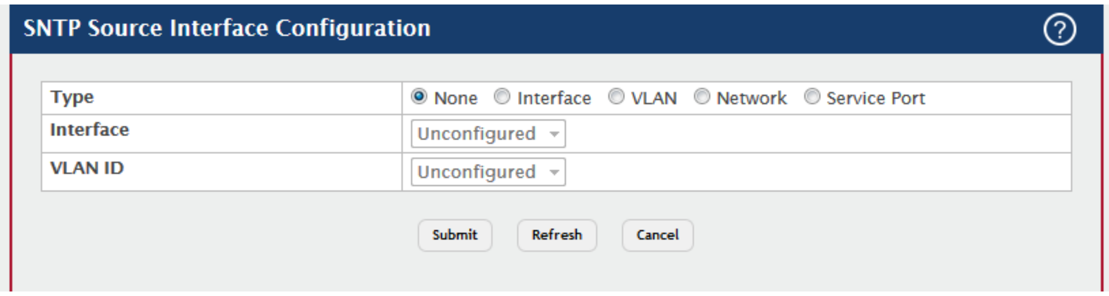
Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests
192.168.10.66	Jan 1 00:00:00 1970	Jan 1 00:00:00 1970	Other	0	0

Field	Description
Address	The hostname or IP address for each SNTP server that has been configured.
Last Update Time	The local date and time (UTC) included in the response from this server that 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 values apply, or no message has been received. **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. **Kiss Of Death Rate Exceeded** – SNTP server status for the rate exceeded case.
Requests	Specifies the number of SNTP requests made to this server since the system was last reset.
Failed Requests	Specifies the number of failed SNTP requests made to this server since the system was last reset.

3.1.2.7.5 Source interface Configuration

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



SNTP Source Interface Configuration

Type	● None ○ Interface ○ VLAN ○ Network ○ Service Port
Interface	Unconfigured
VLAN ID	Unconfigured

Field	Description
Type	The type of interface to use as the source interface: **None** – The primary IP address of the originating (outbound) interface is used as the source address. **Interface** – The primary IP address of a physical port is used as the

	source address. **VLAN** – The primary IP address of a VLAN routing interface is used as the source address. **Network** – The network source IP is used as the source address. **Service Port** – The management port source IP is used as the source address.
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.

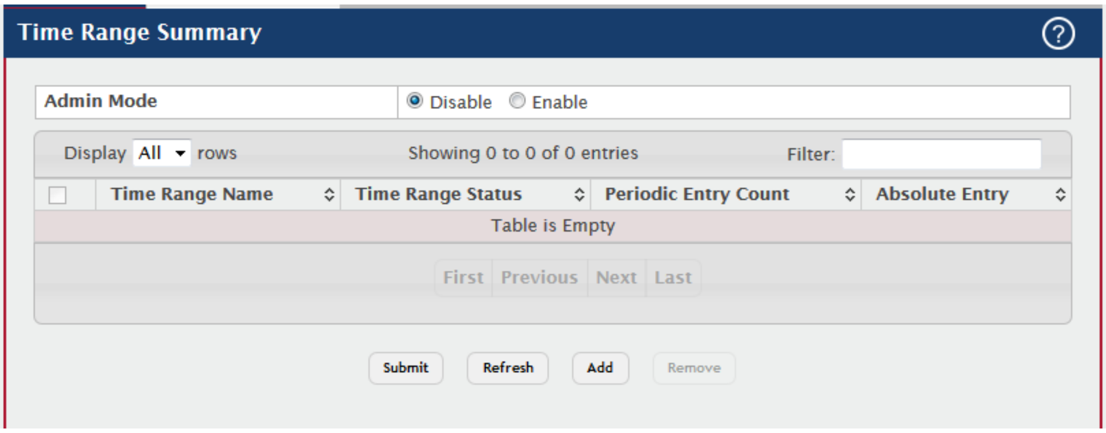
3.1.2.8 Time Ranges

3.1.2.8.1 Configuration

Use this page to add and remove time range configrations. Time ranges can be referenced in time-based Access Control List (ACL) rules to allow the rule to be active and operational only during the time period specified in the time range. The time range feature uses the system clock to determine the time and day. Configuring the device to use an SNTP server for time synchronization can help ensure the system time is accurate.

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.



Time Range Summary

Admin Mode ● Disable ○ Enable

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Time Range Name	Time Range Status	Periodic Entry Count	Absolute Entry
Table is Empty				

Field	Description
Admin Mode	Enables or disables the Time Range administrative mode. When

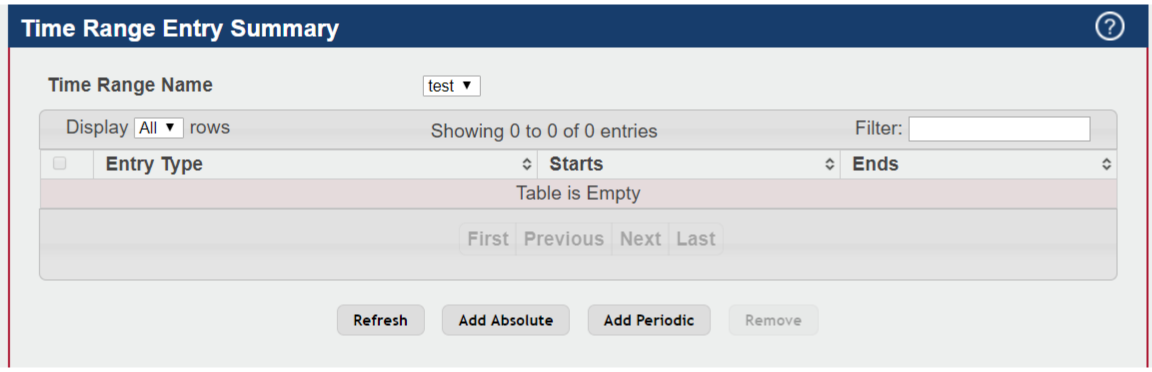
	enabled, actions with subscribed components are performed for existing time range entries.
Time Range Name	The unique ID or name that identifies this time range. A time-based ACL rule can reference the name configured in this field.
Time Range Status	Shows whether the time range is Active or Inactive. A time range is Inactive if the current day and time do not fall within any time range entries configured for the time range.
Periodic Entry Count	The number of periodic time range entries currently configured for the time range.
Absolute Entry	Shows whether an absolute time entry is currently configured for the time range.

3.1.2.8.2 Entry Configuration

Use this page to configure entries in an existing time range configuration. Each time range configuration can have multiple Periodic entries but only one Absolute entry. 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. The start and end times for entries are based on a 24-hour clock. For example, 6:00 PM is 18:00.

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.



Field	Description
Time Range Name	The menu includes all existing time range configurations.
Entry Type	The type of time range entry, which is one of the following: **Absolute** – Occurs once or has an undefined start or end period. The duration of an Absolute entry can be hours, days, or even years. Each time entry configuration can have only one Absolute entry. **Periodic** – Recurring entry that takes place at fixed intervals. This type of entry occurs at the same time on one or more days of the week.
Starts	For an Absolute entry, indicates the time, day, month, and year that the entry begins. If this field is blank, the Absolute entry became active when it was configured. For a Periodic entry, indicates the time and day(s) of the week that the entry begins.
Ends	For an Absolute entry, indicates the time, day, month, and year that the entry ends. If this field is blank, the Absolute entry does not have a defined end. For a Periodic entry, indicates the time and day(s) of the week that the entry ends.

After you click Add Absolute, the configuration window for the Absolute time range entry appears. The following information describes the fields in the Add Absolute Time Range Entry window.

Field	Description
Time Range Name	The time range configuration that will include the Absolute time range entry.
Start Time	Select this option to configure values for the Start Date and the Starting Time of Day. If this option is not selected, the entry becomes active immediately.
Start Date	Click the calendar icon to select the day, month, and year when this

	entry becomes active. This field can be configured only if the Start Time option is selected.
Starting Time of Day	Specify the time of day that the entry becomes active by entering the information in the field or by using the scroll bar in the Choose Time window. Click Now to use the current time of day. Click Done to close the Choose Time window. This field can be configured only if the Start Time option is selected.
End Time	Select this option to configure values for the End Date and the Ending Time of Day. If this option is not selected, the entry does not have an end time; after the configured Start Time begins, the entry will remain active indefinitely.
End Date	Click the calendar icon to select the day, month, and year when this entry should no longer be active. This field can be configured only if the End Time option is selected.
Ending Time of Day	Specify the time of day that the entry becomes inactive by entering the information in the field or by using the scroll bar in the Choose Time window. Click Now to use the current time of day. Click Done to close the Choose Time window. This field can be configured only if the End Time option is selected.

After you click Add Periodic, the configuration window for the Periodic time range entry appears. The following information describes the fields in the Add Periodic Time Range Entry window.

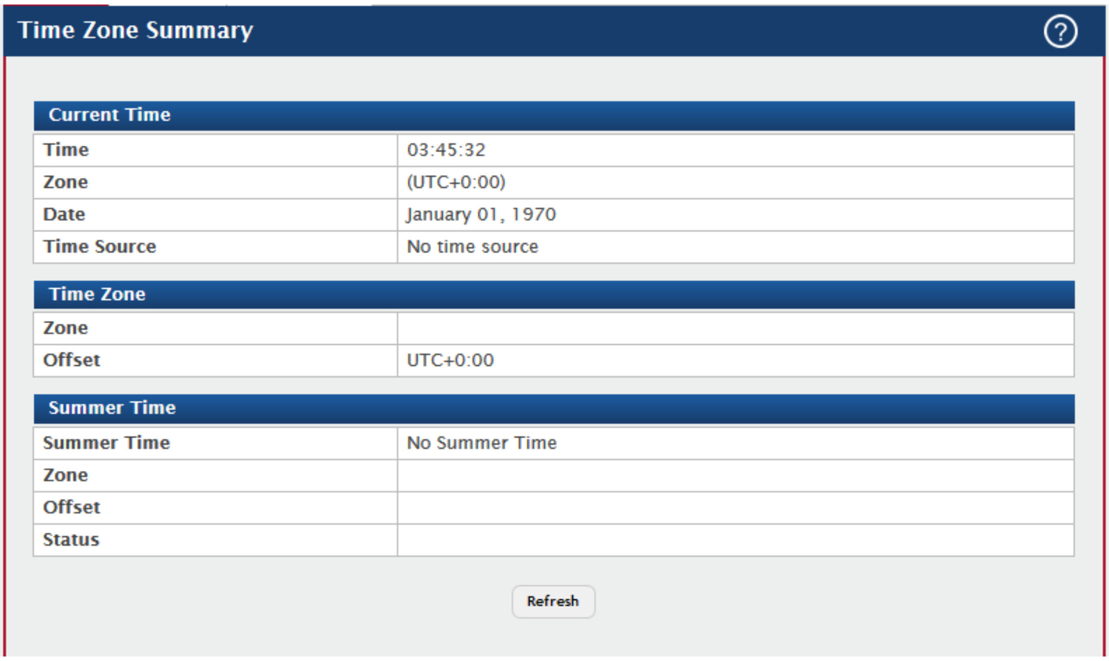
Field	Description
Time Range Name	The time range configuration that will include the Periodic time range entry.
Applicable Days	Select the days on which the Periodic time range entry is active: **Daily** – Every day of the week **Weekdays** – Monday through Friday **Weekend** – Saturday and Sunday **Days of Week** – User-defined start days
Start Days	Indicates on which days the time entry becomes active. If the selected option in the Applicable Days field is Days of Week, select one or more days on which the entry becomes active. To select multiple days, hold the Ctrl key and select each desired start day.
Starting Time of Day	Specify the time of day that the entry becomes active by entering the information in the field or by using the scroll bar in the Choose Time

	window. Click Now to use the current time of day. Click Done to close the Choose Time window.
End Days	Indicates on which days the time entry ends. If the selected option in the Applicable Days field is Days of Week, select one or more days on which the entry ends. To select multiple days, hold the Ctrl key and select each desired end day.
Ending Time of Day	Specify the time of day that the entry becomes inactive by entering the information in the field or by using the scroll bar in the Choose Time window. Click Now to use the current time of day. Click Done to close the Choose Time window.

3.1.2.9 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.

3.1.2.9.1 Summary



Time Zone Summary

Current Time	
Time	03:45:32
Zone	(UTC+0:00)
Date	January 01, 1970
Time Source	No time source

Time Zone	
Zone	
Offset	UTC+0:00

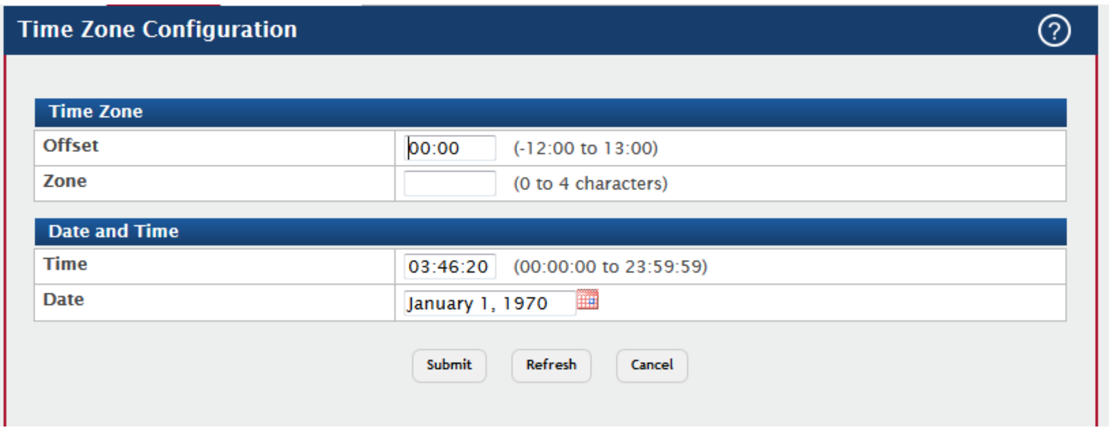
Summer Time	
Summer Time	No Summer Time
Zone	
Offset	
Status	

Field	Description
Current Time	
Time	The current time on the system clock. This time is used to provide time stamps on log messages. Additionally, some CLI show commands include the time in the command output.
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	
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).
Summer Time	
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.

3.1.2.9.2 Time Zone

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.



Time Zone Configuration

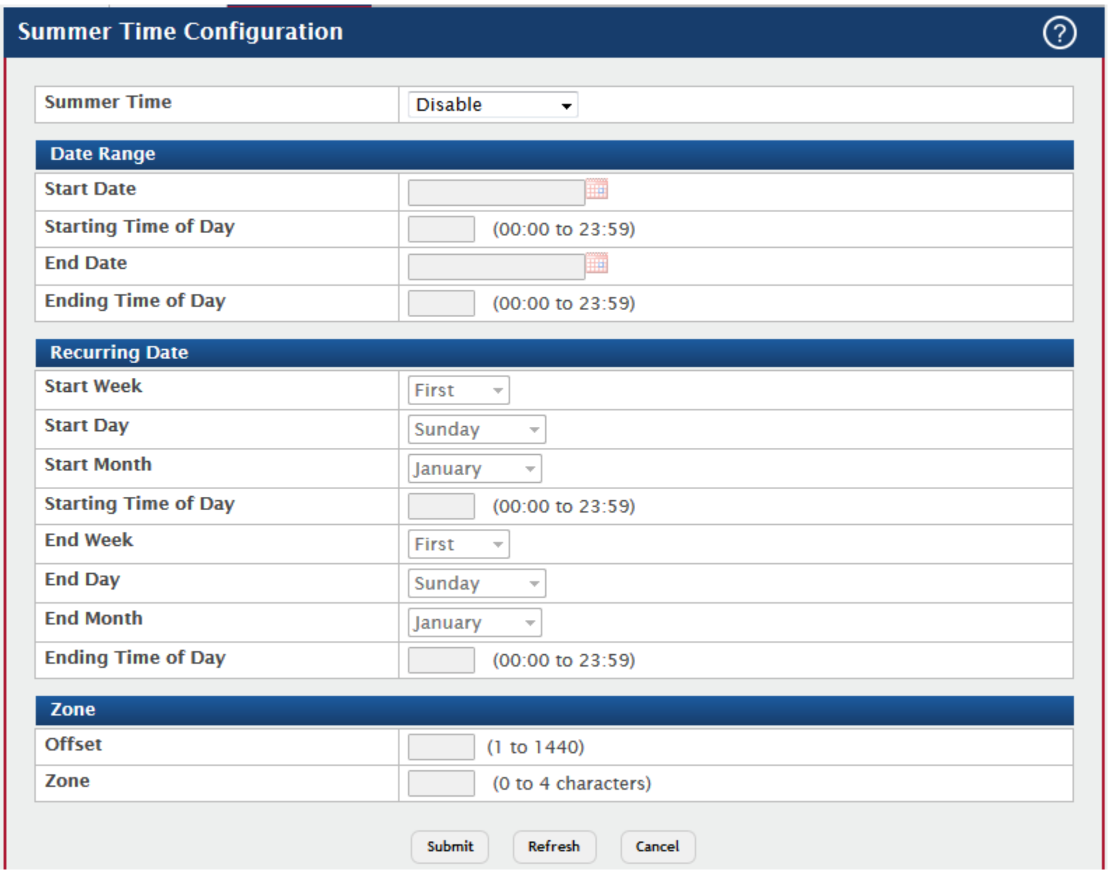
Time Zone	
Offset	00:00 (-12:00 to 13:00)
Zone	(0 to 4 characters)

Date and Time	
Time	03:46:20 (00:00:00 to 23:59:59)
Date	January 1, 1970

Field	Description
Time Zone	
Offset	The system clock's 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	
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.

3.1.2.9.3 Summer Time

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.



Summer Time Configuration

Summer Time	Disable

Date Range

Start Date	
Starting Time of Day	(00:00 to 23:59)
End Date	
Ending Time of Day	(00:00 to 23:59)

Recurring Date

Start Week	First
Start Day	Sunday
Start Month	January
Starting Time of Day	(00:00 to 23:59)
End Week	First
End Day	Sunday
End Month	January
Ending Time of Day	(00:00 to 23:59)

Zone

Offset	(1 to 1440)
Zone	(0 to 4 characters)

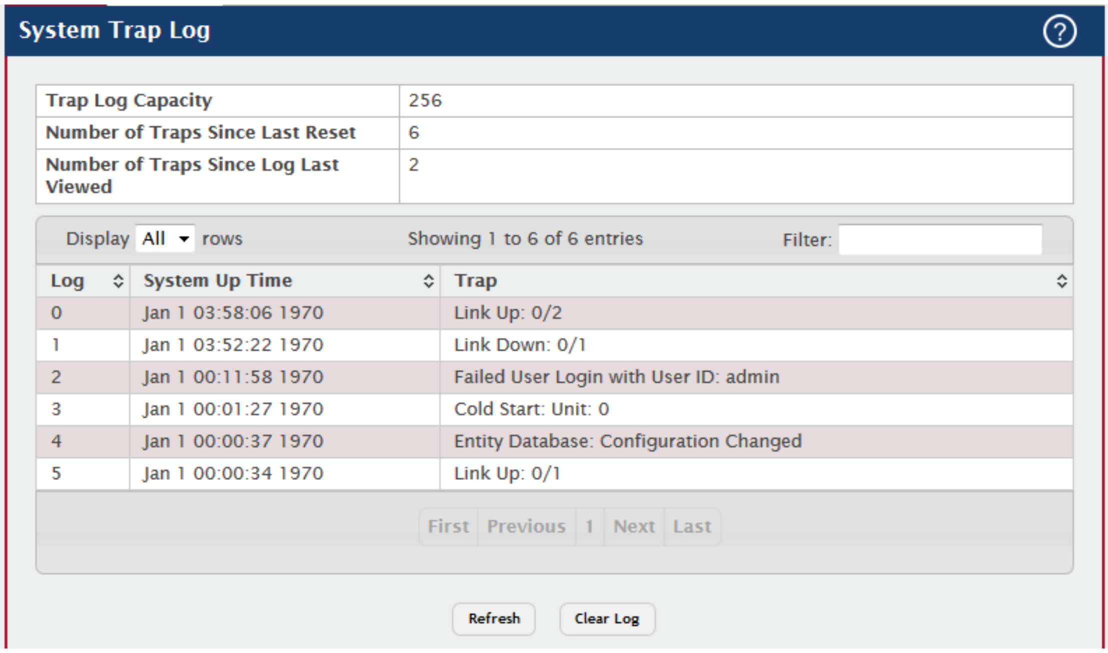
Field	Description
Summer Time	The summer time mode on the system: **Disable** – Summer time is not active, and the time does not shift based on the time of year. **Recurring** – Summer time occurs at the same time every year. The start and end times and dates for the time shift must be manually configured. **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 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.
Date Range	
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	
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	
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.

3.1.2.10 Trap Manager

3.1.2.10.1 Trap Log

This page displays information about the SNMP traps that have been logged to the device. You can save the trap log to a file on a remote system by using the Upload page.



Trap Log Capacity	256
Number of Traps Since Last Reset	6
Number of Traps Since Log Last Viewed	2

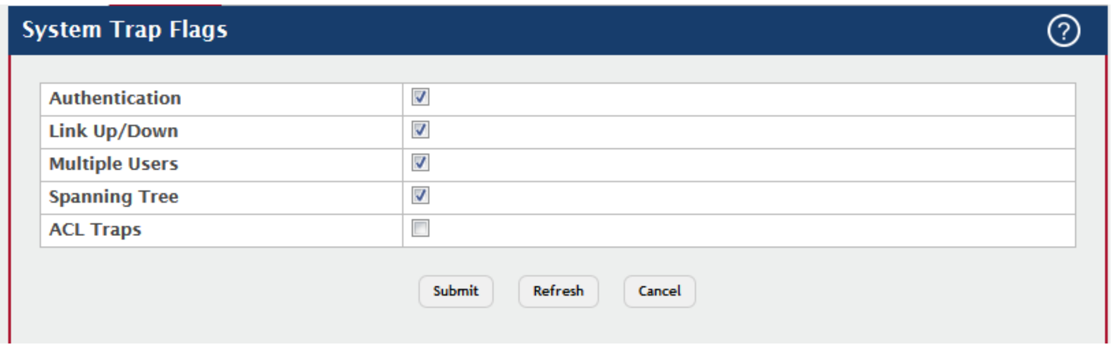
Display All rows Showing 1 to 6 of 6 entries Filter:

Log	System Up Time	Trap
0	Jan 1 03:58:06 1970	Link Up: 0/2
1	Jan 1 03:52:22 1970	Link Down: 0/1
2	Jan 1 00:11:58 1970	Failed User Login with User ID: admin
3	Jan 1 00:01:27 1970	Cold Start: Unit: 0
4	Jan 1 00:00:37 1970	Entity Database: Configuration Changed
5	Jan 1 00:00:34 1970	Link Up: 0/1

Field	Description
Trap Log Capacity	The maximum number of traps the log can store. If the number of traps exceeds the capacity, new entries overwrite the oldest entries.
Number of Traps Since Last Reset	The number of traps the system has generated since the trap log entries were last cleared, either by clicking the Clear Log button or by resetting the system.
Number of Traps Since Log Last Viewed	The number of traps the system has generated since the traps were last displayed. Displaying the traps by any available method (for example, uploading the file from the switch or viewing the logs from a terminal interface) will cause this counter to be reset to 0.
Log	The sequence number of this trap.
System Up Time	The time at which this trap occurred, expressed in days, hours, minutes and seconds since the device was last reset.
Trap	Provides information about the trap.
Clear Log (Button)	Clears the current entries from the log file and resets the counters. The page is repopulated with new traps as they occur on the system.

3.1.2.10.2 Trap Flags

Use this page to specify which software features should generate SNMP traps. If the trap flag is enabled for a feature and a significant event occurs, the SNMP agent on the device sends a trap message to any enabled SNMP trap receivers and writes a message to the trap log.



System Trap Flags

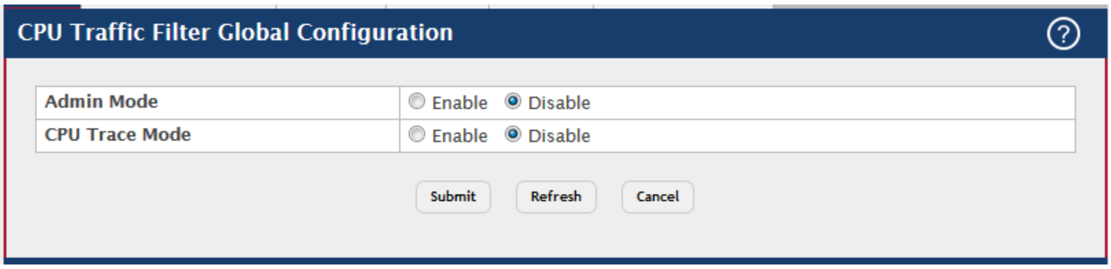
Authentication	☑
Link Up/Down	☑
Multiple Users	☑
Spanning Tree	☑
ACL Traps	□

Field	Description
Authentication	Specify whether to enable SNMP notifications when events involving authentication occur, such as when a user attempts to access the device management interface and fails to provide a valid username and password.
Link Up/Down	Specify whether to enable SNMP notifications when the administrative or operational state of a physical or logical link changes.
Multiple Users	Specify whether to enable SNMP notifications when the same user ID is logged into the device more than once at the same time (either via telnet or the serial port).
Spanning Tree	Specify whether to enable SNMP notifications when various spanning tree events occur.
ACL Traps	Specify whether to enable SNMP notifications when a packet matches a configured ACL rule that includes ACL logging.

3.1.2.11 CPU Traffice Filter

3.1.2.11.1 Global

Use this page to view and modify the CPU Traffic Filter settings on the device.



CPU Traffic Filter Global Configuration

Admin Mode	○ Enable ● Disable
CPU Trace Mode	○ Enable ● Disable

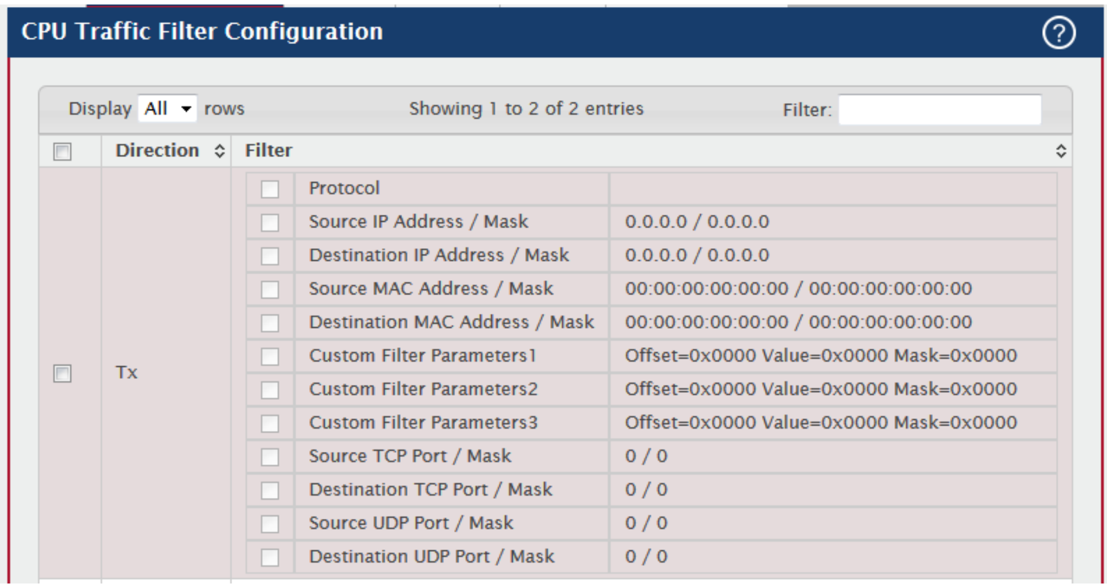
Field	Description
Admin Mode	This configures CPU-traffic mode. The packets in the Rx/Tx directions are matched when the mode is enabled. The default value is disabled.
CPU Trace Mode	This configures CPU packet tracing. The packet may be received by multiple components. If the feature is enabled and tracing configured then the packets are traced per the defined filter.

3.1.2.11.2 Filter Configuration

Use this page to create or remove CPU Traffic Filters and to view summary information about the filters that exist on the device.

Use the buttons to perform the following tasks:

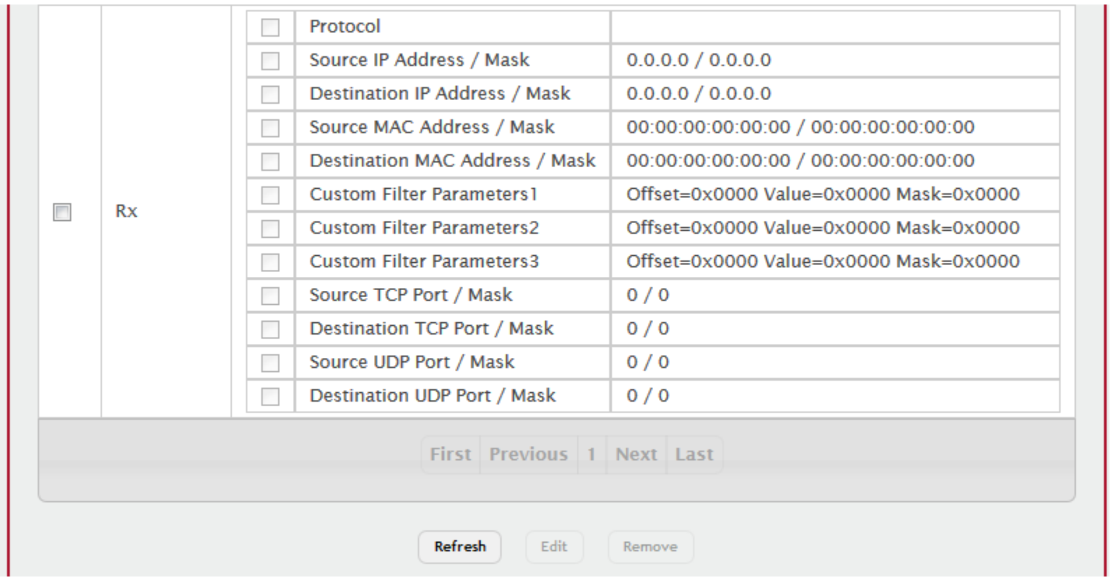
- To Edit existing filter for a direction, select the entry to modify and click **Edit**. To edit CPU Traffic filters for both directions, select Tx and Rx and click **Edit**.
- To remove one or more configured filters, select each entry to delete and click **Remove.** You must confirm the action before the entry is deleted.



CPU Traffic Filter Configuration

Display All rows Showing 1 to 2 of 2 entries Filter:

□	Direction	Filter		
□	Tx	□	Protocol	
		□	Source IP Address / Mask	0.0.0.0 / 0.0.0.0
		□	Destination IP Address / Mask	0.0.0.0 / 0.0.0.0
		□	Source MAC Address / Mask	00:00:00:00:00:00 / 00:00:00:00:00:00
		□	Destination MAC Address / Mask	00:00:00:00:00:00 / 00:00:00:00:00:00
		□	Custom Filter Parameters1	Offset=0x0000 Value=0x0000 Mask=0x0000
		□	Custom Filter Parameters2	Offset=0x0000 Value=0x0000 Mask=0x0000
		□	Custom Filter Parameters3	Offset=0x0000 Value=0x0000 Mask=0x0000
		□	Source TCP Port / Mask	0 / 0
		□	Destination TCP Port / Mask	0 / 0
		□	Source UDP Port / Mask	0 / 0
		□	Destination UDP Port / Mask	0 / 0



□	Rx	□	Protocol	
		□	Source IP Address / Mask	0.0.0.0 / 0.0.0.0
		□	Destination IP Address / Mask	0.0.0.0 / 0.0.0.0
		□	Source MAC Address / Mask	00:00:00:00:00:00 / 00:00:00:00:00:00
		□	Destination MAC Address / Mask	00:00:00:00:00:00 / 00:00:00:00:00:00
		□	Custom Filter Parameters1	Offset=0x0000 Value=0x0000 Mask=0x0000
		□	Custom Filter Parameters2	Offset=0x0000 Value=0x0000 Mask=0x0000
		□	Custom Filter Parameters3	Offset=0x0000 Value=0x0000 Mask=0x0000
		□	Source TCP Port / Mask	0 / 0
		□	Destination TCP Port / Mask	0 / 0
		□	Source UDP Port / Mask	0 / 0
		□	Destination UDP Port / Mask	0 / 0

Field	Description
Tx / Rx	
Protocol	This configures specific protocol filters. The statistics and/or the traces for configured filters are obtained for the packet matching configured filter. The protocol options are: STP LACPDU ARP UDLD LLDP IP OSPF BGP DHCP BCAST MCAST UCAST Source IP Destination IP Source MAC Destination MAC Custom Source TCP Destination TCP

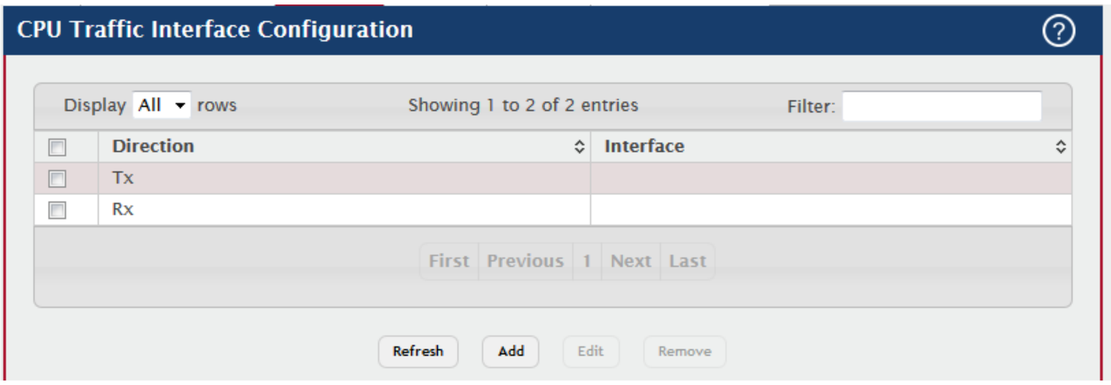
	Source UDP Destination UDP
IP Address	This configures Source or Destination IP address specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured Source / Destination IP/Mask.
MAC Address	This configures Source / Destination MAC address specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured Source / Destination MAC address.
Custom	This configures custom filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured data at specific offset. If the mask is not specified then default mask is 0xFF.
TCP Port	This configures Source / Destination TCP Port specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured Source / Destination TCP Port.
UDP Port	This configures Source / Destination UDP Port specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured Source / Destination UDP Port.

3.1.2.11.3 Interfaces

Use this page to associate the CPU filters to interface or list of interfaces. The interfaces can be physical or logical LAG. The statistics counters are updated only for the configured interfaces. Similarly, the traces can also be obtained for configured interfaces.

Use the buttons to perform the following tasks:

- To add CPU Traffic filter to interface(s), click **Add**.
- To remove one or more associated filters, select each entry to delete and click **Remove.** You must confirm the action before the entry is deleted.



□	Direction	Interface
□	Tx	
□	Rx	

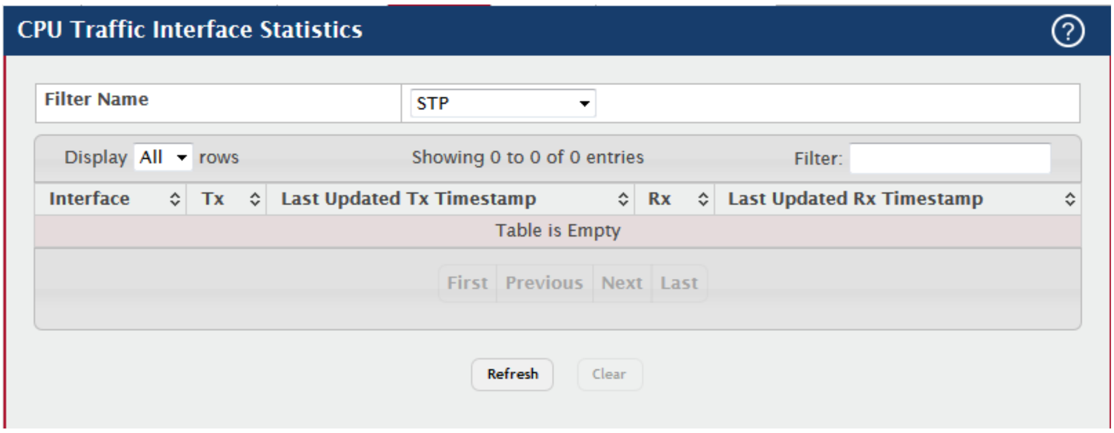
Field	Description
Interface	The interfaces can be physical or logical LAG.
Direction	Only two software filter is supported (one filter each direction Tx or Rx) with condition matching as one, many or all in the below list in Tx or Rx or Both direction.

3.1.2.11.4 Statistics

Use this page to view per interface statistics for configured CPU filters.

Use the buttons to perform the following tasks:

- To clear interface statistics, and click **Clear.** You must confirm the action before the entry is deleted.



CPU Traffic Interface Statistics

Filter Name: STP

Display All rows Showing 0 to 0 of 0 entries Filter:

Interface	Tx	Last Updated Tx Timestamp	Rx	Last Updated Rx Timestamp
Table is Empty				

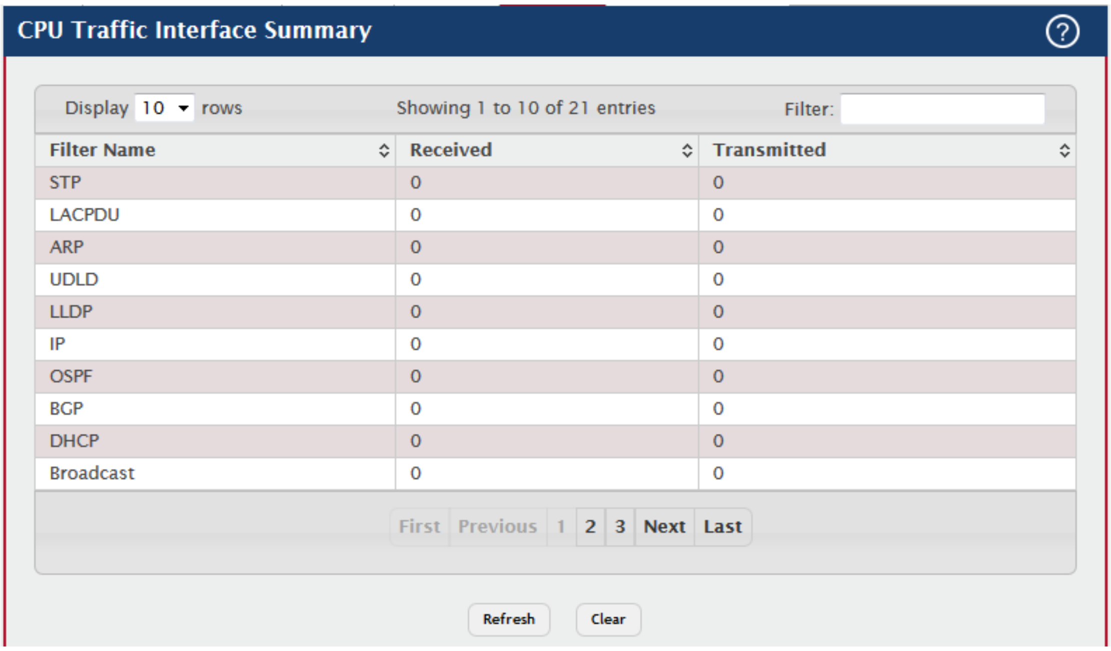
Field	Description
Interface	The interfaces can be physical or logical LAG.
Tx	The counter statistics for an interface associated with Tx direction.
Last Updated Tx Timestamp	Indicates the time when the sent packet count on an interface was last updated, based on the user defined packet filter on the interface.
Rx	The counter statistics for an interface associated with Rx direction.
Last Updated Rx Timestamp	Indicates the time when the received packet count on an interface was last updated, based on the user defined packet filter on the interface.

3.1.2.11.5 Summary

Use this page to view all interface summary for CPU filters.

Use the buttons to perform the following tasks:

- To clear filter summary, and click **Clear.** You must confirm the action before the entry is deleted.



CPU Traffic Interface Summary

Display 10 rows Showing 1 to 10 of 21 entries Filter:

Filter Name	Received	Transmitted
STP	0	0
LACPDU	0	0
ARP	0	0
UDLD	0	0
LLDP	0	0
IP	0	0
OSPF	0	0
BGP	0	0
DHCP	0	0
Broadcast	0	0

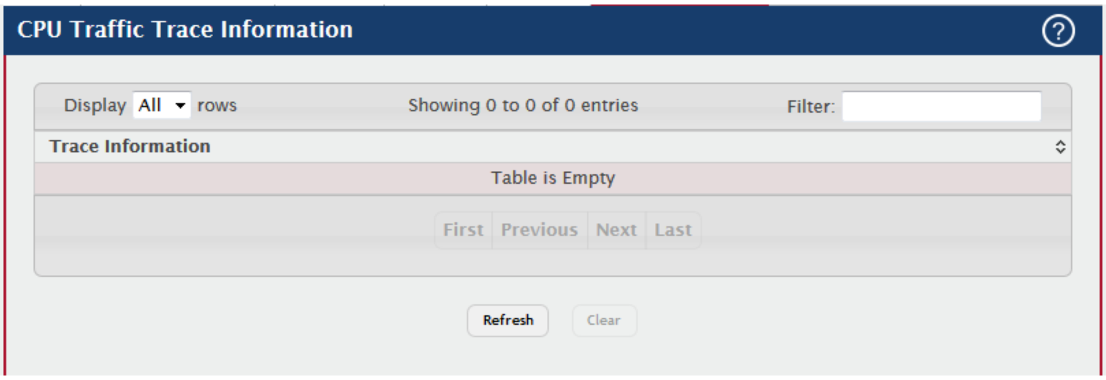
Field	Description
Transmitted	The counter statistics for all interfaces, which are associated with Tx direction.
Received	The counter statistics for all interfaces, which are associated with Rx direction.

3.1.2.11.6 Trace Information

Use this page to view CPU Trace information.

Use the buttons to perform the following tasks:

- To clear CPU Trace information, and click **Clear.** You must confirm the action before the entry is deleted.



CPU Traffic Trace Information

Display All rows Showing 0 to 0 of 0 entries Filter:

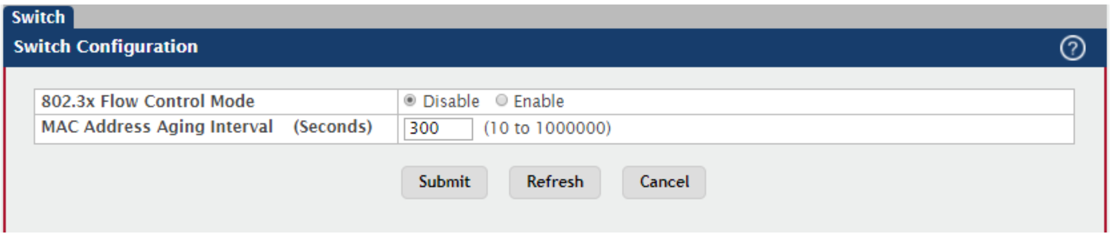
Trace Information
Table is Empty

Field	Description
Trace Information	It provides trace information for the matching packets as defined in the filters until the packet is delivered to registered application.

3.1.3 Basic Configuration

3.1.3.1 Switch

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



Switch

Switch Configuration

802.3x Flow Control Mode	● Disable ○ Enable
MAC Address Aging Interval (Seconds)	300 (10 to 1000000)

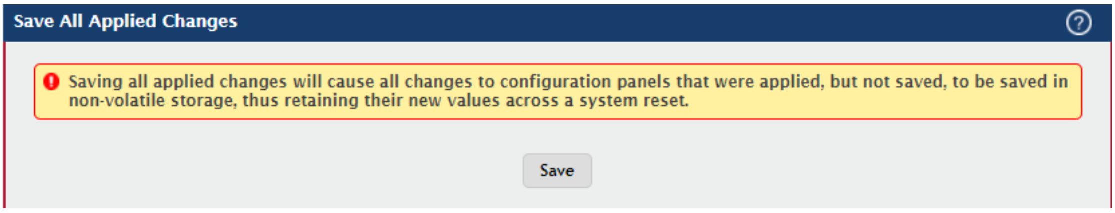
Field	Description
802.3x Flow Control Mode	The 802.3x flow control mode on the switch. IEEE 802.3x flow control works by pausing a port when the port becomes oversubscribed. This allows lower-speed switches to communicate with higher-speed switches. A lower-speed or congested switch can send a PAUSE 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.

3.1.4 Configuration Storage

3.1.4.1 Save

Initiates a save of all system configuration after displaying a confirmation message. All of the current system configuration settings, including any that have been changed by the user, are stored into non-volatile memory so that they are preserved across a system reset.

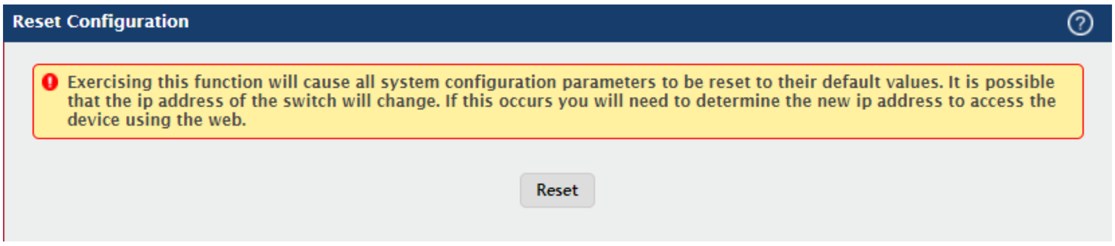


Save All Applied Changes

Saving all applied changes will cause all changes to configuration panels that were applied, but not saved, to be saved in non-volatile storage, thus retaining their new values across a system reset.

3.1.4.2 Reset

Initiates the action to reset all configuration parameters to their factory default settings after displaying a confirmation message. All configuration changes, including those that were previously saved, are reset in the running system by this action. It is possible that the ip address of the switch will change. If this occurs you will need to determine the new ip address to access the device using the web.

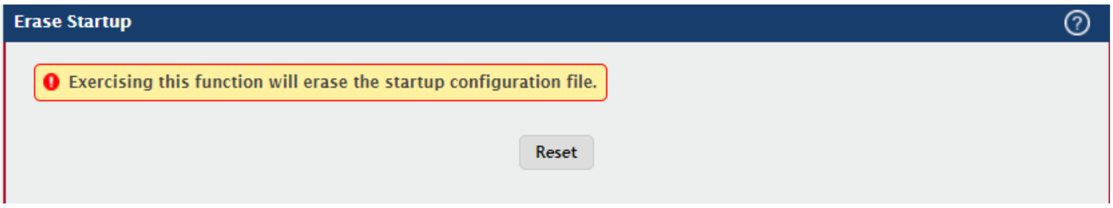


Reset Configuration

Exercising this function will cause all system configuration parameters to be reset to their default values. 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.

3.1.4.3 Erase startup

Initiates the action to erase the text-based configuration file stored in non-volatile memory after displaying a confirmation message. If the system resets and no startup-config file is found, the system will begin the AutoInstall process to automatically update the image and download a configuration file.

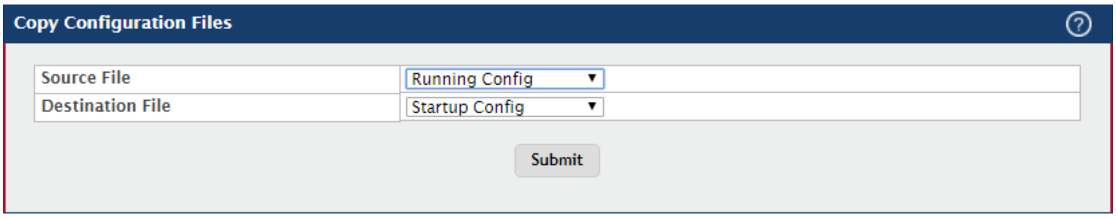


Erase Startup

Exercising this function will erase the startup configuration file.

3.1.4.4 Copy

Use this page to copy the information contained in one configuration file to another configuration file on the device. When you click Submit, the copy action takes place immediately, and the source file overwrites the destination file



Copy Configuration Files

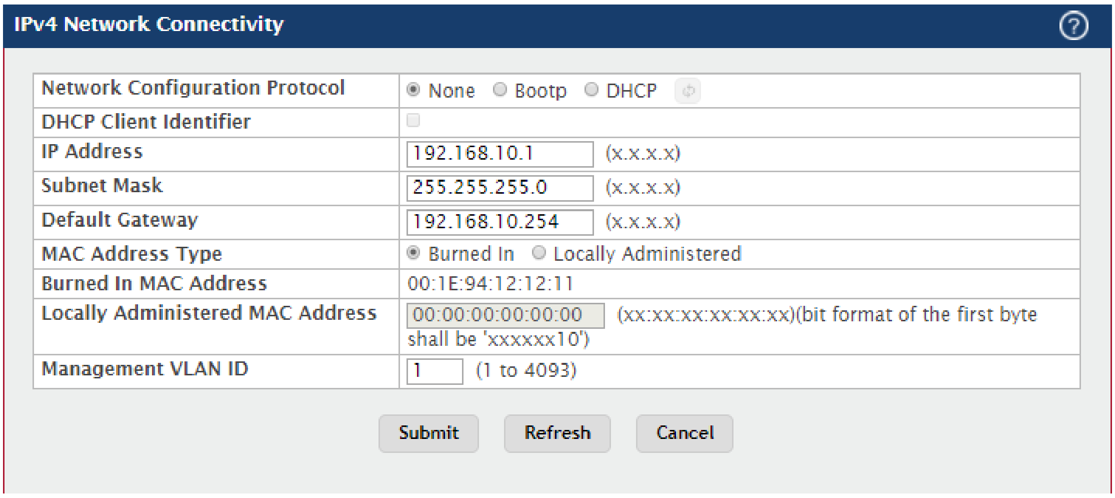
Source File	Running Config
Destination File	Startup Config

Field	Description
Source File	Select the configuration file that will overwrite the contents in the selected destination file. The source file options are as follows: **Running Config** – The file that contains the configuration that is currently active on the system. Copying the Running Config file to the Startup Config file is effectively the same as performing a Save. **Startup Config** – The file that contains the configuration that loads when the system boots. **Backup Config** – The file that is used to store a copy of the running or startup configuration.
Destination File	Select file to be overwritten by the contents in the selected source file. The destination file options are as follows: **Startup Config** – The file that contains the configuration that loads when the system boots. **Backup Config** – The file that is used to store a copy of the running or startup configuration.

3.1.5 Connectivity

3.1.5.1 IPv4

Use this page to configure and view the IPv4 network connectivity information on the network interface. The network interface is the logical interface that allows remote management of the device via any of the front-panel switch ports. To enable management of the device over an IPv4 network by using a Web browser, SNMP, Telnet, or SSH, you must first configure it with an IP address, subnet mask, and default gateway. The configuration parameters associated with the network interface do not affect the configuration of the front-panel ports through which traffic is switched or routed.



IPv4 Network Connectivity

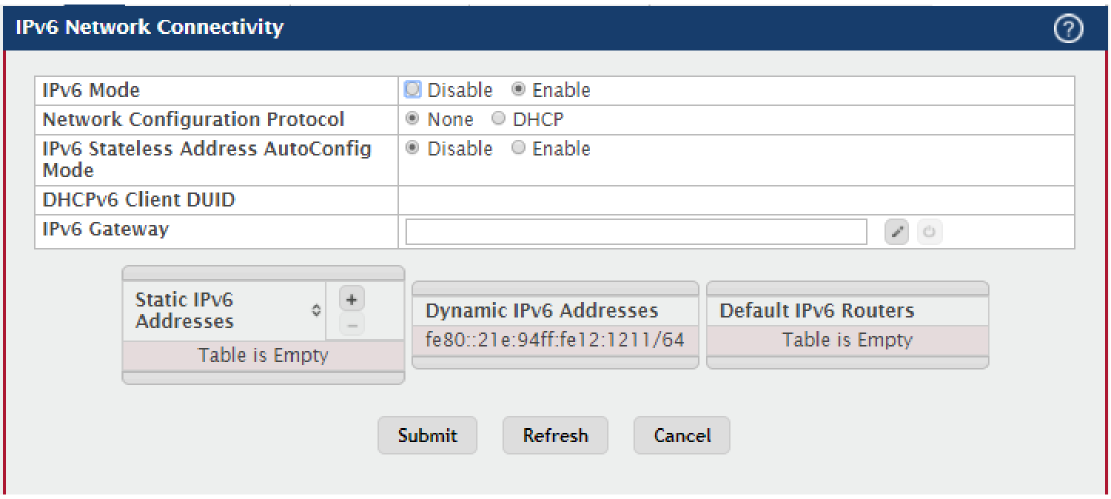
Network Configuration Protocol	● None ○ Bootp ○ DHCP
DHCP Client Identifier	□
IP Address	192.168.10.1 (x.x.x.x)
Subnet Mask	255.255.255.0 (x.x.x.x)
Default Gateway	192.168.10.254 (x.x.x.x)
MAC Address Type	● Burned In ○ Locally Administered
Burned In MAC Address	00:1E:94:12:12:11
Locally Administered MAC Address	00:00:00:00:00:00 (xx:xx:xx:xx:xx:xx)(bit format of the first byte shall be 'xxxxxx10')
Management VLAN ID	1 (1 to 4093)

Field	Description
Network Configuration Protocol	Specify how the device acquires network information on the network interface: **None** – The device does not attempt to acquire network information dynamically. Select this option to configure a static IP address, subnet mask, and default gateway. **BOOTP** – During the next boot cycle, the BOOTP client on the device broadcasts a BOOTP request in an attempt to acquire information from a BOOTP server on the network. **DHCP** – During the next boot cycle, the DHCP client on the device broadcasts a DHCP request in an attempt to acquire information from a DHCP server on the network. After this option is applied, you can use the Refresh icon at the end of the row to renew the IPv4 address learned from DHCP server.
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 interface. If the Network Configuration Protocol is None, you can manually configure a static IP address. If the Network Configuration Protocol is BOOTP or DHCP, this field displays the IP address that was dynamically acquired (if any).
Subnet Mask	The IP subnet mask for the interface. If the Network Configuration Protocol is None, you can manually configure a static subnet mask. If the Network Configuration Protocol is BOOTP or DHCP, this field displays the subnet mask that was dynamically acquired (if any).
Default Gateway	The default gateway for the IP interface. If the Network Configuration Protocol is None, you can manually configure the IP address of the default gateway. If the Network Configuration Protocol is BOOTP or DHCP, this field displays the default gateway address that was dynamically acquired (if any).
MAC Address Type	Specify whether the burned in or the locally administered MAC address should be used for in-band connectivity.
Burned In MAC Address	The burned in MAC address used for in-band connectivity if you choose not to configure a locally administered address.
Locally Administered MAC Address	You may configure 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 6 of byte 0 must be set to 1 and bit 0 to 0, i.e. byte 0 must have a value of 2, 6, A or E for its second digit.
Management VLAN ID	The VLAN ID for the management VLAN. Some network administrators use a management VLAN to isolate system management traffic from end-user data traffic.

3.1.5.2 IPv6

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



IPv6 Network Connectivity

IPv6 Mode	○ Disable ● Enable
Network Configuration Protocol	● None ○ DHCP
IPv6 Stateless Address AutoConfig Mode	● Disable ○ Enable
DHCPv6 Client DUID	
IPv6 Gateway	

Static IPv6 Addresses
Table is Empty

Dynamic IPv6 Addresses
fe80::21e:94ff:fe12:1211/64

Default IPv6 Routers
Table is Empty

Field	Description
IPv6 Mode	Enables or disables the IPv6 administrative mode on the network interface.
Network Configuration Protocol	Specify whether the device should attempt to acquire network information from a DHCPv6 server. Selecting None disables the DHCPv6 client on the network interface.
IPv6 Stateless Address AutoConfig Mode	Sets the IPv6 stateless address autoconfiguration mode on the network interface. **Enabled** – The network interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages. **Disabled** – The network interface will not use the native IPv6 address autoconfiguration features to acquire an IPv6 address.
DHCPv6 Client DUID	The client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.
IPv6 Gateway	The default gateway for the IPv6 network interface. To configure this field, click the Edit icon in the row. To reset the field to the default value, click the Reset icon in the row.

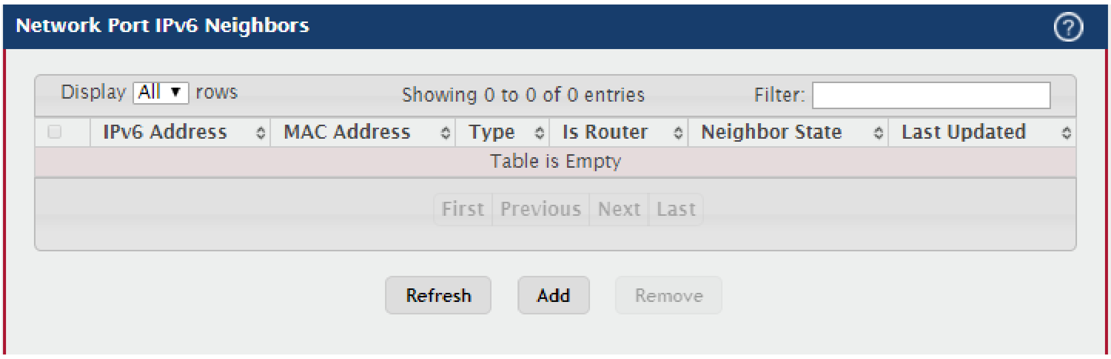
Static IPv6 Addresses	Lists the manually configured static IPv6 addresses on the network interface. Use the buttons available in this table to perform the following tasks: To add an entry to the list, click the + (plus) button to open the Add IPv6 Address dialog and provide the following: **New IPv6 Address** – Specify the IPv6 address to add to the interface. **EUI Flag** – Select this option to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or clear the option to omit the flag. To delete an entry from the list, click the – (minus) button associated with the entry to remove. To delete all entries from the list, click the – (minus) button in the heading row.
Dynamic IPv6 Addresses	Lists the IPv6 addresses on the network interface that have been dynamically configured through IPv6 autoconfiguration or DHCPv6.
Default IPv6 Routers	Lists the IPv6 address of each default router that has been automatically configured through IPv6 router discovery.

3.1.5.3 IPv6 Negihbors

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

Use the buttons to perform the following tasks:

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

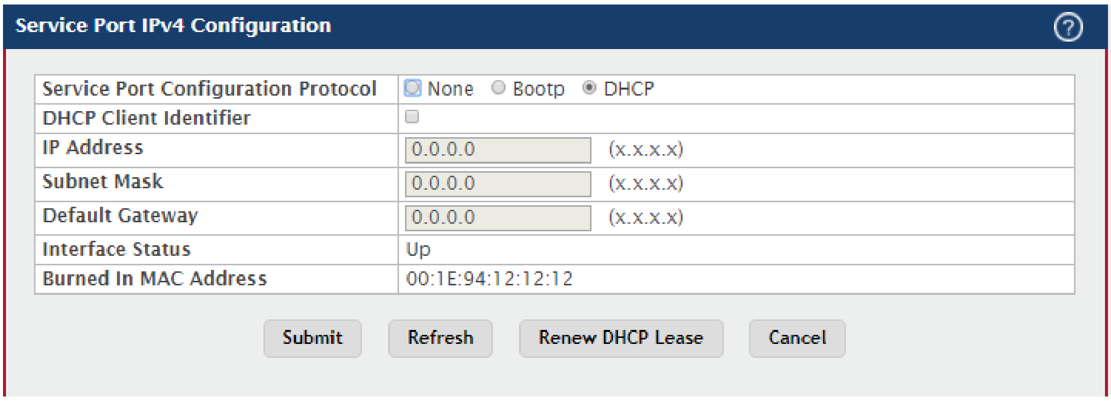


□	IPv6 Address	MAC Address	Type	Is Router	Neighbor State	Last Updated
Table is Empty						

Field	Description
IPv6 Address	The IPv6 address of a neighbor device that has been reachable on the local link through the network interface.
MAC Address	The MAC address of the neighboring device.
Type	The type of the neighbor entry, which is one of the following: **Static** – The neighbor entry is manually configured. **Dynamic** – The neighbor entry is dynamically resolved. **Local** – The neighbor entry is a local entry. **Other** – The neighbor entry is an unknown entry.
Is Router	Identifies whether the neighbor device is a router. The possible values are: **True** – The neighbor device is a router. **False** – The neighbor device is not a router.
Neighbor State	The current reachability state of the neighboring device, which is one of the following: **Reachable** – The neighbor is reachable through the network interface. **Stale** – The neighbor is not known to be reachable, and the system will begin the process to reach the neighbor. **Delay** – The neighbor is not known to be reachable, and upper-layer protocols are attempting to provide reachability information. **Probe** – The neighbor is not known to be reachable, and the device is attempting to probe for this neighbor. **Unknown** – The reachability status cannot be determined.
Last Updated	The amount of time that has passed since the neighbor entry was last updated.

3.1.5.4 Service Port IPv4

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



Service Port IPv4 Configuration

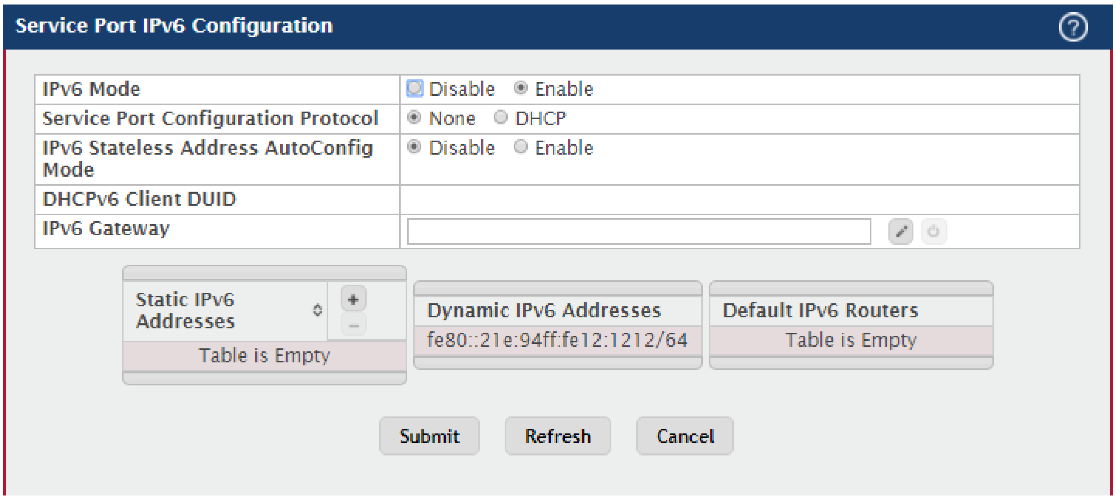
Service Port Configuration Protocol	○ None ○ Bootp ● DHCP
DHCP Client Identifier	□
IP Address	0.0.0.0 (x.x.x.x)
Subnet Mask	0.0.0.0 (x.x.x.x)
Default Gateway	0.0.0.0 (x.x.x.x)
Interface Status	Up
Burned In MAC Address	00:1E:94:12:12:12

Field	Description
Service Port Configuration Protocol	Specify how the device acquires network information on the service port: **BOOTP** – During the next boot cycle, the BOOTP client on the device broadcasts a BOOTP request in an attempt to acquire information from a BootP server on the network. **DHCP** – During the next boot cycle, the DHCP client on the device broadcasts a DHCP request in an attempt to acquire information from a DHCP server on the network. **None** – The device does not attempt to acquire network information dynamically.
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 interface. If the Service Port Configuration Protocol is None, you can manually configure a static IP address. If the Service Port Configuration Protocol is BOOTP or DHCP, this field displays the IP address that was dynamically acquired (if any).
Subnet Mask	The IP subnet mask for the interface. If the Service Port Configuration Protocol is None, you can manually configure a static subnet mask. If the Service Port Configuration Protocol is BOOTP or DHCP, this field displays the subnet mask that was dynamically acquired (if any).
Default Gateway	The default gateway for the IP interface. If the Service Port

	Configuration Protocol is None, you can manually configure the IP address of the default gateway. If the Service Port Configuration Protocol is BOOTP or DHCP, this field displays the default gateway address that was dynamically acquired (if any).
Interface Status	Indicates whether the link status is up or down.
Burned In MAC Address	The burned in MAC address used for out-of-band connectivity.

3.1.5.5 Service Port IPv6

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



Service Port IPv6 Configuration

IPv6 Mode	○ Disable ● Enable
Service Port Configuration Protocol	● None ○ DHCP
IPv6 Stateless Address AutoConfig Mode	● Disable ○ Enable
DHCPv6 Client DUID	
IPv6 Gateway	

Static IPv6 Addresses
Table is Empty

Dynamic IPv6 Addresses
fe80::21e:94ff:fe12:1212/64

Default IPv6 Routers
Table is Empty

Field	Description
IPv6 Mode	Enables or disables the IPv6 administrative mode on the service port.
Service Port Configuration Protocol	Specify whether the device should attempt to acquire network information from a DHCPv6 server. Selecting None disables the DHCPv6 client on the service port.
IPv6 Stateless Address AutoConfig Mode	Sets the IPv6 stateless address autoconfiguration mode on the service port. **Enabled** – The service port can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages. **Disabled** – The service port will not use the native IPv6 address autoconfiguration features to acquire an IPv6 address.

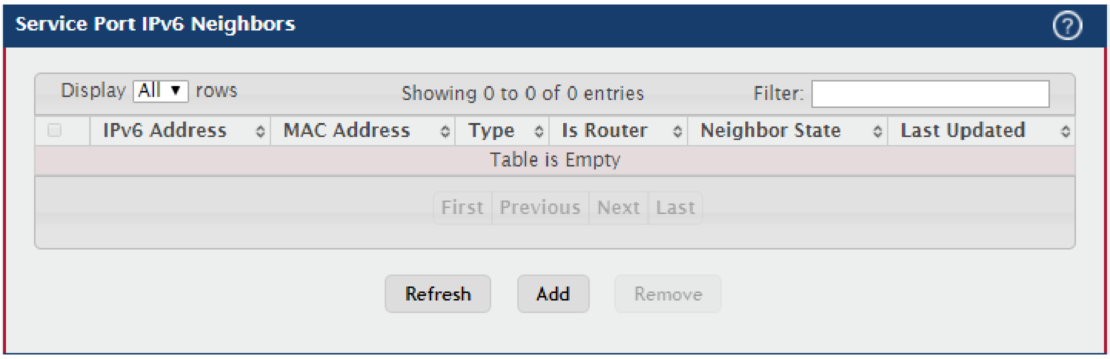
DHCPv6 Client DUID	The client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.
IPv6 Gateway	The default gateway for the IPv6 service port interface. To configure this field, click the Edit icon in the row. To reset the field to the default value, click the Reset icon in the row.
Static IPv6 Addresses	Lists the manually configured static IPv6 addresses on the service port interface. Use the buttons available in this table to perform the following tasks: To add an entry to the list, click the + (plus) button to open the Add IPv6 Address dialog and provide the following: **New IPv6 Address** – Specify the IPv6 address to add to the service port interface. **EUI Flag** – Select this option to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or clear the option to omit the flag. To delete an entry from the list, click the – (minus) button associated with the entry to remove. To delete all entries from the list, click the – (minus) button in the heading row.
Dynamic IPv6 Addresses	Lists the IPv6 addresses on the service port interface that have been dynamically configured through IPv6 autoconfiguration or DHCPv6.
Default IPv6 Routers	Lists the IPv6 address of each default router that has been automatically configured through IPv6 router discovery.

3.1.5.6 Service Port IPv6 Neighbors

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

Use the buttons to perform the following tasks:

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



Service Port IPv6 Neighbors

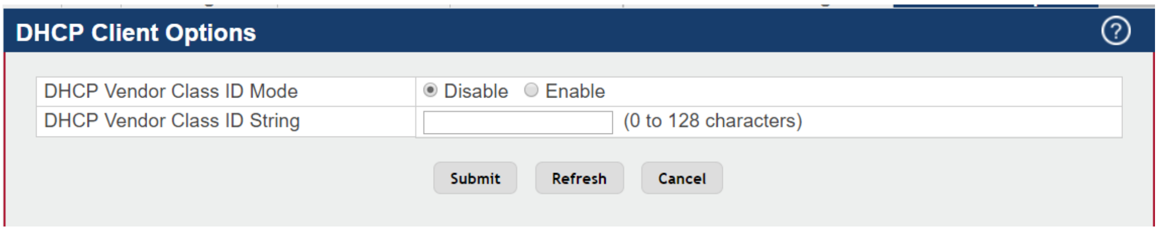
Display All rows Showing 0 to 0 of 0 entries Filter:

□	IPv6 Address	MAC Address	Type	Is Router	Neighbor State	Last Updated
Table is Empty						

Field	Description
IPv6 Addresses	The IPv6 address of a neighbor device that has been reachable on the local link through the service port.
MAC Address	The MAC address of the neighboring device.
Type	The type of the neighbor entry, which is one of the following: **Static** – The neighbor entry is manually configured. **Dynamic** – The neighbor entry is dynamically resolved. **Local** – The neighbor entry is a local entry. **Other** – The neighbor entry is an unknown entry.
Is Router	Identifies whether the neighbor device is a router. The possible values are: **True** – The neighbor device is a router. **False** – The neighbor device is not a router.
Neighbor State	The current reachability state of the neighboring device, which is one of the following: **Reachable** – The neighbor is reachable through the service port. **Stale** – The neighbor is not known to be reachable, and the system will begin the process to reach the neighbor. **Delay** – The neighbor is not known to be reachable, and upper-layer protocols are attempting to provide reachability information. **Probe** – The neighbor is not known to be reachable, and the device is attempting to probe for this neighbor. **Unknown** – The reachability status cannot be determined.
Last Updated	The amount of time that has passed since the neighbor entry was last updated.

3.1.5.7 DHCP Client Options

Use this page to set a value for DHCP option 60 in the DHCP requests that the DHCP client on the device broadcasts to network DHCP servers. Option 60, the Vendor Class Identifier (VCI), can help identify the device to the DHCP server, which allows the server to include additional information in the DHCP response.



DHCP Client Options

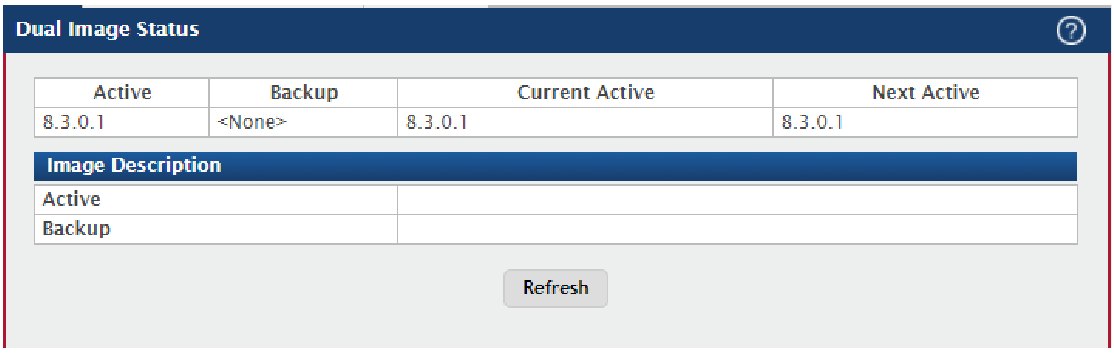
DHCP Vendor Class ID Mode	● Disable ○ Enable
DHCP Vendor Class ID String	(0 to 128 characters)

Field	Description
DHCP Vendor Class ID Mode	The VCI administrative mode. When the mode is enabled, the DHCP client includes the text configured as the DHCP Vendor Class ID String in DHCP requests.
DHCP Vendor Class ID String	The text string to add to DHCP requests as option 60, the VCI option.

3.1.6 Firmware

3.1.6.1 Status

Use this page to view information about the software images on the device. The device can store up to two software images in permanent storage. The dual image feature allows you to upgrade the device without deleting the older software image.



Dual Image Status

Active	Backup	Current Active	Next Active
8.3.0.1	<None>	8.3.0.1	8.3.0.1

Image Description

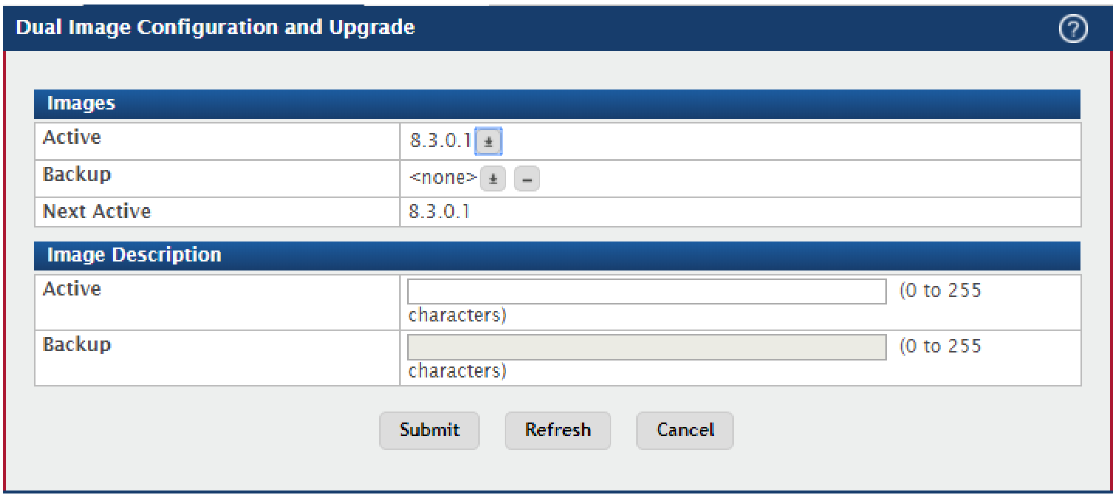
Active	
Backup	

Field	Description
Unit	The unit ID of the switch.
Active	The code file version of the active image.
Backup	The code file version of the backup image.

Current Active	The image version that is loaded and running on this unit.
Next Active	The image version to be loaded after the system reboots.
Active Description	The description associated with the active code file.
Backup Description	The description associated with the backup code file.

3.1.6.2 Configuration and Upgrade

Use this page 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.



Dual Image Configuration and Upgrade

Images

Active	8.3.0.1
Backup	<none>
Next Active	8.3.0.1

Image Description

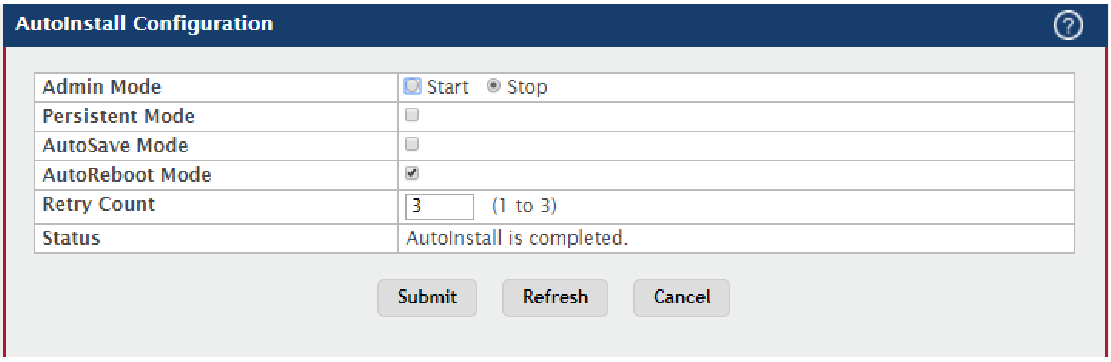
Active	(0 to 255 characters)
Backup	(0 to 255 characters)

Field	Description
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	Select the image version to load the next time this unit reboots.
Active Description	Specify a description to associate with the image that is currently the active code file.
Backup Description	Specify a description to associate with the image that is currently the backup code file.
Select File	Provides 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.

3.1.6.3 Auto Install

The AutoInstall feature can automatically obtain configuration information and install a new image when the switch boots. The process begins when the switch is initialized and no configuration file (startup-config) is found, or when the switch boots and loads a saved configuration that has AutoInstall enabled. If initiated, the AutoInstall feature allows the device to obtain an IP address from a network DHCP server and then attempts to locate the predefined configuration file from a TFTP server.



AutoInstall Configuration

Admin Mode	○ Start ● Stop
Persistent Mode	□
AutoSave Mode	□
AutoReboot Mode	☑
Retry Count	3 (1 to 3)
Status	AutoInstall is completed.

Field	Description
Admin Mode	The current administrative mode of the AutoInstall feature: **Start** — AutoInstall is enabled, and the feature will attempt to automatically configure the device during the next boot cycle. **Stop** — AutoInstall is disabled. The automatic process will begin only if no configuration file is located during the next boot cycle.
Persistent Mode	If this option is selected, the settings you configure on this page are

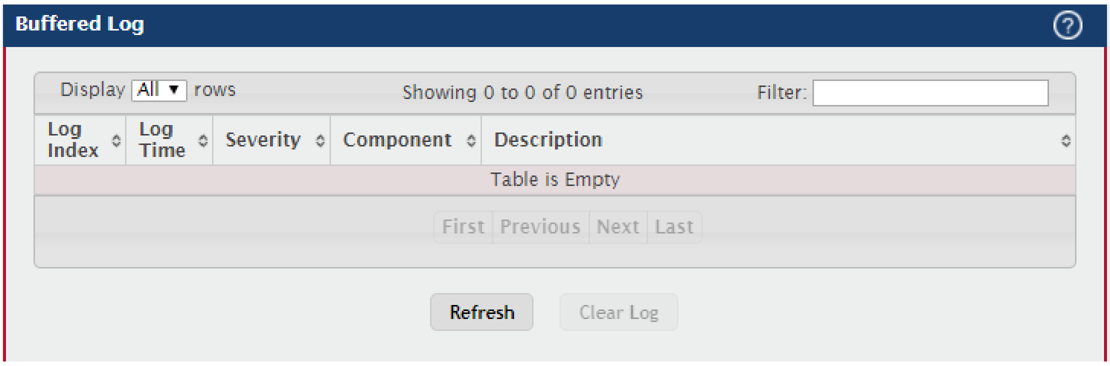
	automatically saved to persistent memory in the startup-config file when you apply the changes. If this option is not selected, the device treats these settings like any other applied changes (i.e. the changes are not retained across a reboot unless you save the configuration).
AutoSave Mode	If this option is selected, the downloaded configuration is automatically saved to persistent storage. If this option is not selected, you must explicitly save the downloaded configuration in non-volatile memory for the configuration to be available for the next reboot.
AutoReboot Mode	If this option is selected, the switch automatically reboots after a new image is successfully downloaded and makes the downloaded image the active image. If this option is not selected, the device continues to boot with the current image. The downloaded image will not become the active image until the device reboots.
Retry Count	When attempting to retrieve the DHCP-specified configuration file, this value represents the number of times the TFTP client on the device tries to use unicast requests before reverting to broadcast requests.
Status	The current status of the AutoInstall process.

3.1.7 Log

3.1.7.1 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.

Use the Buffered Log page to view information about the log messages stored in RAM.



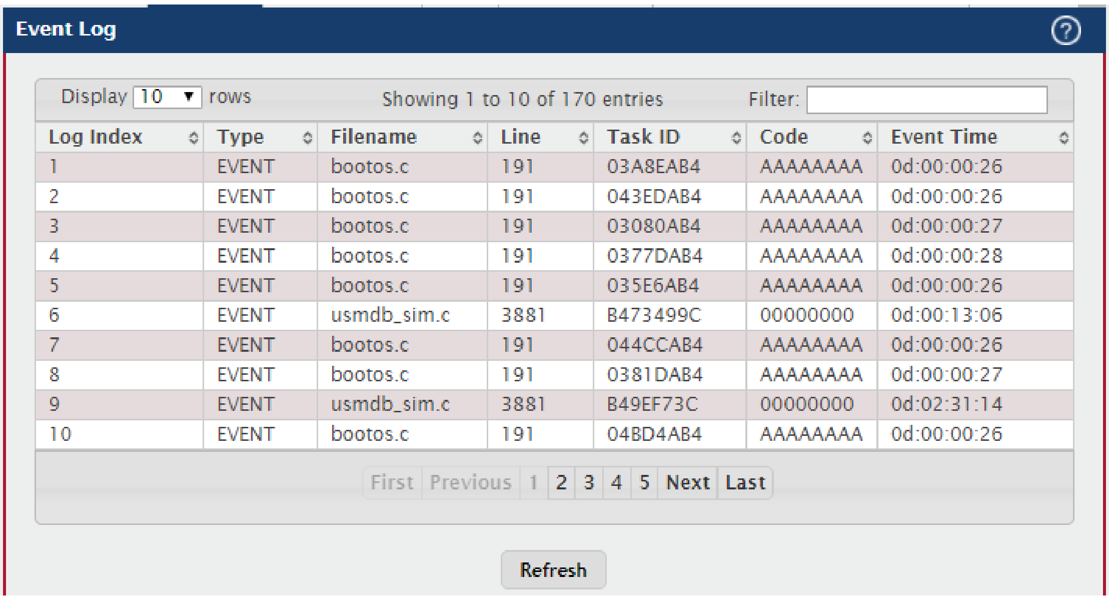
Log Index	Log Time	Severity	Component	Description
Table is Empty				

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.
Clear Log (Button)	Clears the buffered log messages and resets the counters. The buffered log will be repopulated with new entries as they occur on the system.

3.1.7.2 Event Log

The event log contains error messages which result from catastrophic events that occur during system operation. At least two thousand (2,000) entries can be stored in the event log, although the actual number depends on the specific device hardware and operating system in use.

The event log is preserved across system resets, but the log file is automatically erased whenever an attempt is made to write a new entry when the log is at capacity. The system automatically resets after a new event is logged and the updated log file is saved to non-volatile memory.



Event Log

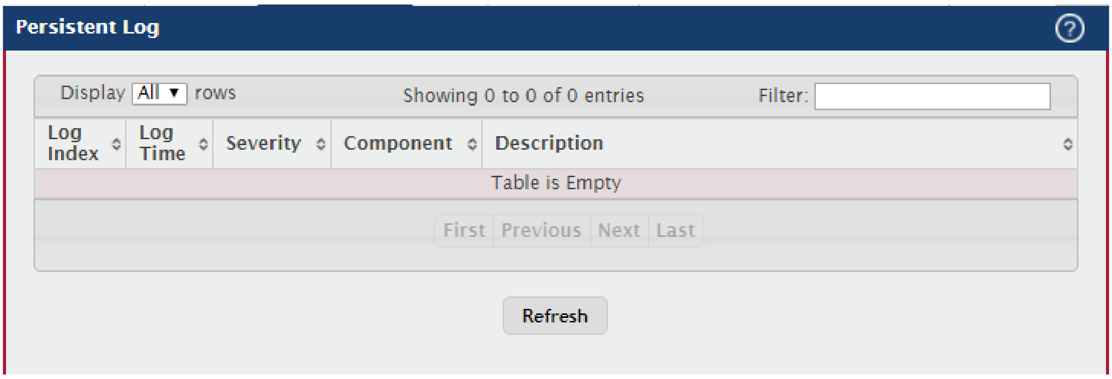
Display 10 ▼ rows Showing 1 to 10 of 170 entries Filter:

Log Index	Type	Filename	Line	Task ID	Code	Event Time
1	EVENT	bootos.c	191	03A8EAB4	AAAAAAAA	0d:00:00:26
2	EVENT	bootos.c	191	043EDAB4	AAAAAAAA	0d:00:00:26
3	EVENT	bootos.c	191	03080AB4	AAAAAAAA	0d:00:00:27
4	EVENT	bootos.c	191	0377DAB4	AAAAAAAA	0d:00:00:28
5	EVENT	bootos.c	191	035E6AB4	AAAAAAAA	0d:00:00:26
6	EVENT	usmdb_sim.c	3881	B473499C	00000000	0d:00:13:06
7	EVENT	bootos.c	191	044CCAB4	AAAAAAAA	0d:00:00:26
8	EVENT	bootos.c	191	0381DAB4	AAAAAAAA	0d:00:00:27
9	EVENT	usmdb_sim.c	3881	B49EF73C	00000000	0d:02:31:14
10	EVENT	bootos.c	191	04BD4AB4	AAAAAAAA	0d:00:00:26

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

3.1.7.3 Persistent Log

Persistent log messages are stored in persistent storage so that they survive across device reboots. Two types of log files exist in flash (persistent) memory: the system startup log and the system operation logs. The system startup log stores the first 32 messages received after system reboot. The log file stops when it is full. The system operation log stores the last 32 messages received during system operation. The oldest messages are overwritten when the file is full.



Persistent Log

Display All rows Showing 0 to 0 of 0 entries Filter:

Log Index	Log Time	Severity	Component	Description
Table is Empty				

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 has issued the log entry.
Description	The text description for the log entry.

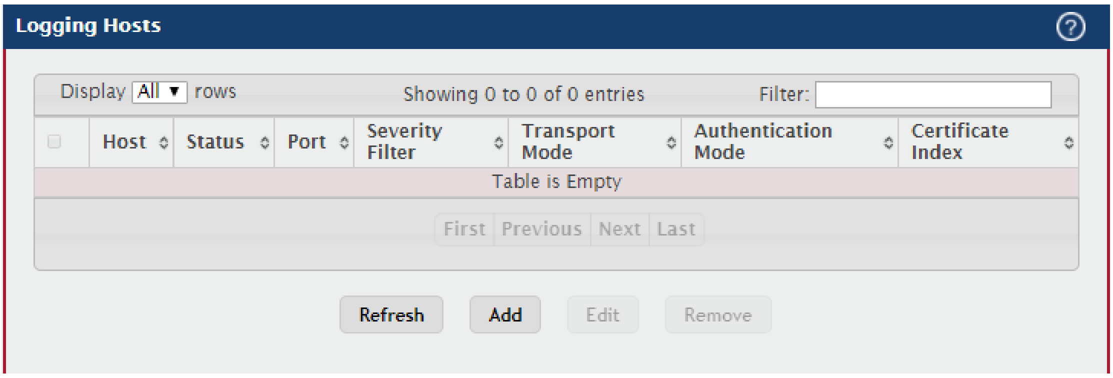
3.1.7.4 Hosts

Use this page to add, edit, and remove information about one or more remote syslog servers that receive system log messages sent from the device. The log messages are sent to the logging host for viewing, analysis, and storage.

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.**



Logging Hosts

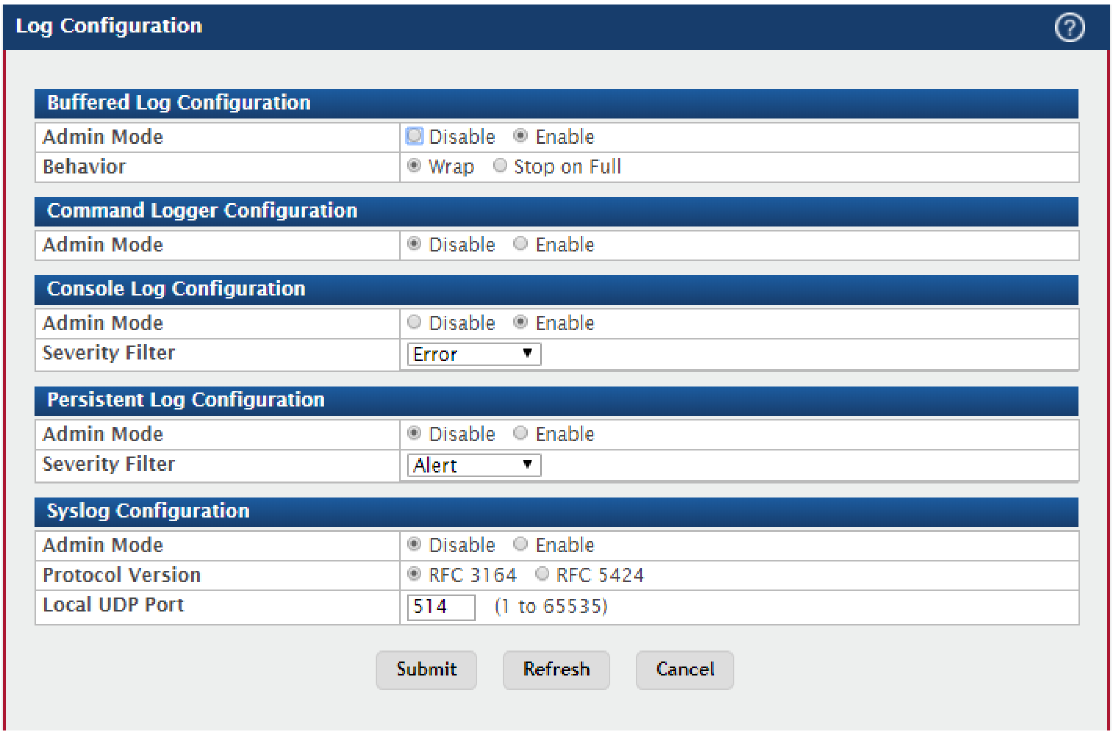
Display All rows Showing 0 to 0 of 0 entries Filter:

□	Host	Status	Port	Severity Filter	Transport Mode	Authentication Mode	Certificate Index
Table is Empty							

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.

3.1.7.5 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.



Log Configuration

Buffered Log Configuration

Admin Mode	○ Disable ● Enable
Behavior	● Wrap ○ Stop on Full

Command Logger Configuration

Admin Mode	● Disable ○ Enable

Console Log Configuration

Admin Mode	○ Disable ● Enable
Severity Filter	Error

Persistent Log Configuration

Admin Mode	● Disable ○ Enable
Severity Filter	Alert

Syslog Configuration

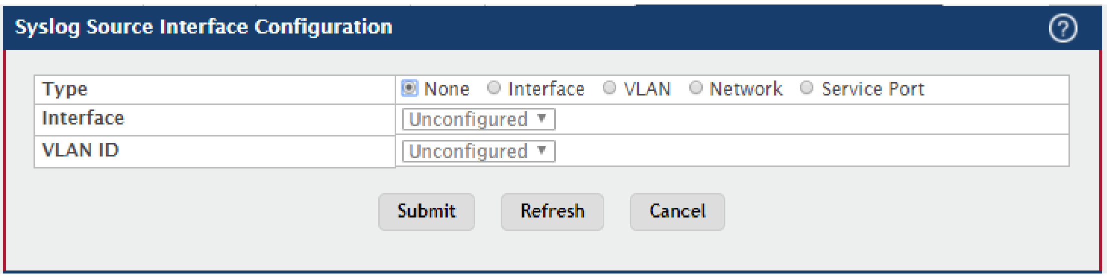
Admin Mode	● Disable ○ Enable
Protocol Version	● RFC 3164 ○ RFC 5424
Local UDP Port	514 (1 to 65535)

Field	Description
Buffered Log Configuration	Admin Mode: Enable or disable logging to the buffered (RAM) log file. Behavior: Specify what the device should do when the buffered log is full. It can either overwrite the oldest messages (Wrap) or stop writing new messages to the buffer (Stop on Full).
Command Logger Configuration	Admin Mode: Enable or disable logging of the command-line interface (CLI) commands issued on the device.
Console Log Configuration	Admin Mode: Enable or disable logging to any serial device attached to the host. Severity Filter: Select the severity of the messages to be logged. All messages at and above the selected threshold are logged to the console. The severity can be one of the following: 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.
Persistent Log Configuration	Admin Mode: Enable or disable logging to the persistent log. These messages are not deleted when the device reboots. Severity Filter: Select the severity of the messages to be logged. All messages at and above the selected threshold are logged to the console. See the previous severity filter description for more information about each severity level.
Syslog Configuration	Admin Mode: Enable or disable logging to configured syslog hosts. When the syslog admin mode is disabled the device does not relay logs to syslog hosts, and no messages will be sent to any collector/relay. When the syslog admin mode is enabled, messages will be sent to configured collectors/relays using the values configured for each collector/relay. Protocol Version: The RFC version of the syslog protocol. Local UDP Port: The UDP port on the local host from which syslog messages are sent.

3.1.7.6 Source Interface Configuration

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



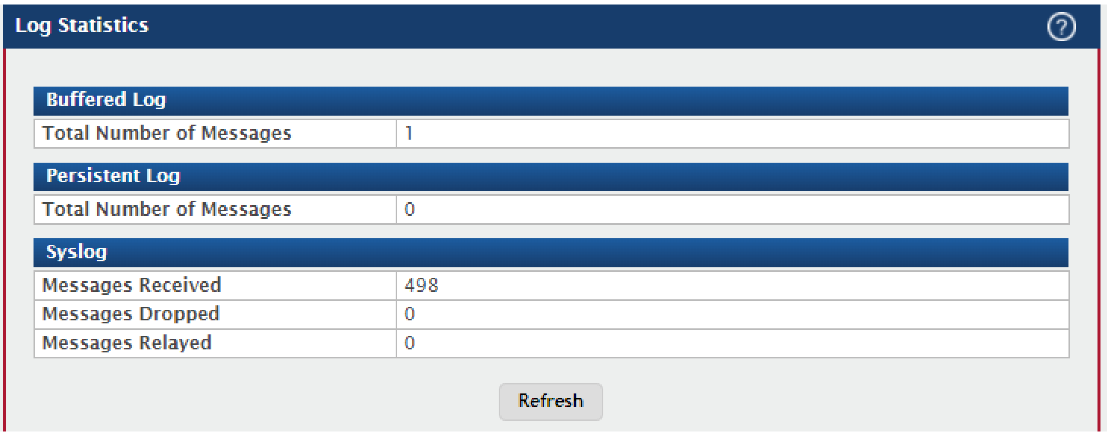
Syslog Source Interface Configuration

Type	● None ○ Interface ○ VLAN ○ Network ○ Service Port
Interface	Unconfigured
VLAN ID	Unconfigured

Field	Description
Type	The type of interface to use as the source interface: **None** – The primary IP address of the originating (outbound) interface is used as the source address. **Interface** – The primary IP address of a physical port is used as the source address. **VLAN** – The primary IP address of a VLAN routing interface is used as the source address. **Network** – The network source IP is used as the source address. **Service Port** – The management port source IP is used as the source address.
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.

3.1.7.7 Statistics

This page displays summary information about the number of messages logged to the buffered, persistent, or syslog file. It also displays the number of messages that were successfully or unsuccessfully relayed to any remote syslog servers configured on the device.



Log Statistics

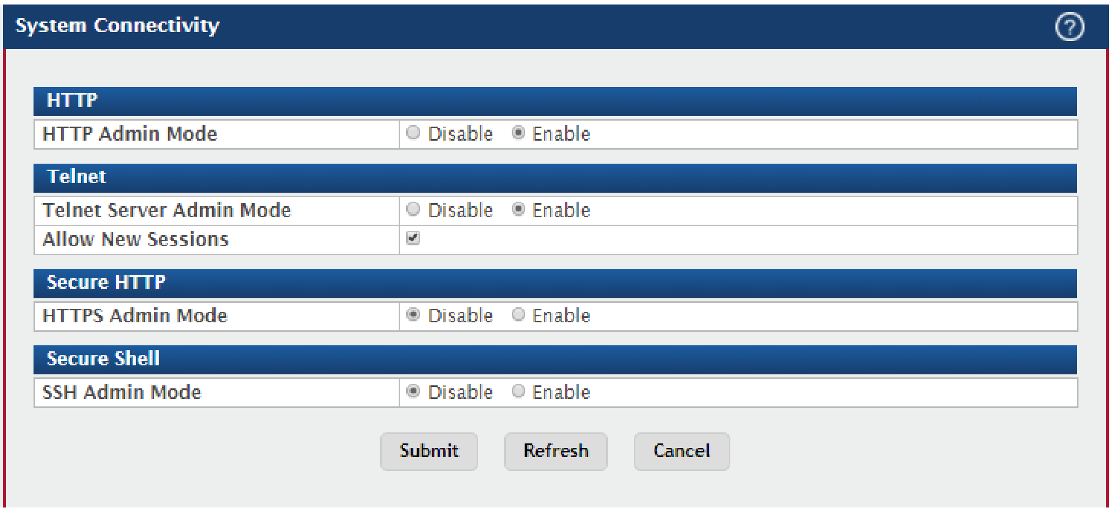
Buffered Log	
Total Number of Messages	1
Persistent Log	
Total Number of Messages	0
Syslog	
Messages Received	498
Messages Dropped	0
Messages Relayed	0

Field	Description
Buffered Log	Total Number of Messages: The number of log messages currently stored in RAM.
Persistent Log	Total Number of Messages: The number of log messages currently stored in persistent storage.
Syslog	Messages Received: The total number of messages received by the log process. This includes messages that are dropped or ignored. The number includes messages of all severity levels. Messages Dropped: The number of messages that failed to be relayed to a remote syslog server. The configured syslog server might be unreachable, misconfigured, or out of storage space. Messages Relayed: The number of log messages successfully relayed to a remote syslog server. Messages forwarded to multiple hosts are counted once for each host.

3.1.8 Management Access

3.1.8.1 System

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



System Connectivity

HTTP

HTTP Admin Mode	○ Disable ● Enable

Telnet

Telnet Server Admin Mode	○ Disable ● Enable
Allow New Sessions	☑

Secure HTTP

HTTPS Admin Mode	● Disable ○ Enable

Secure Shell

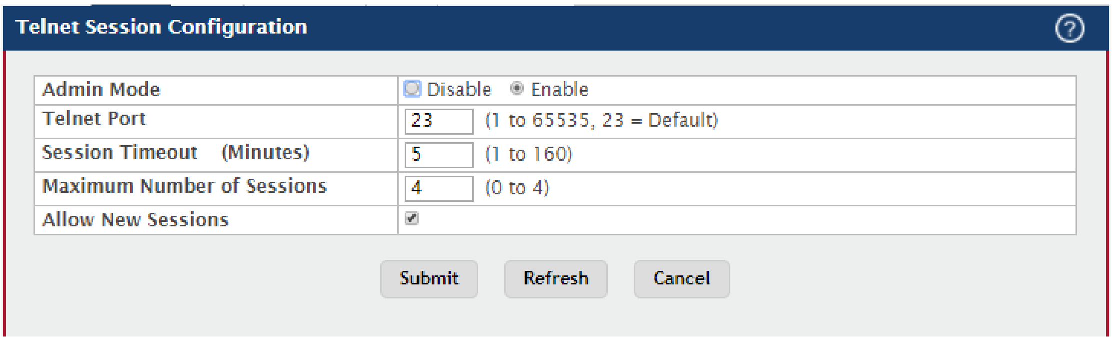
SSH Admin Mode	● Disable ○ Enable

Field	Description
HTTP	**HTTP Admin Mode** Enables or disables the HTTP administrative mode. When this mode

	is enabled, the device management interface can be accessed through a web browser using the HTTP protocol.
Telnet	**Telnet Server Admin Mode** Enables or disables the telnet administrative mode. When this mode is enabled, the device command-line interface (CLI) can be accessed through the telnet port. Disabling this mode disconnects all existing telnet connections and shuts down the telnet port in the device. **Allow New Sessions** Enables or disables new telnet sessions. When this option is disabled, the system does not accept any new telnet sessions, but existing telnet sessions are unaffected.
Secure HTTP	**HTTPS Admin Mode** Enables or disables the administrative mode of secure HTTP. When this mode is enabled, the device management interface can be accessed through a web browser using the HTTPS protocol.
Secure Shell	**SSH Admin Mode** Enables or disables the administrative mode of SSH. When this mode is disabled, all existing SSH connections remain connected until timed-out or logged out, but new SSH connections cannot be established.

3.1.8.2 Telnet

This page displays the current value of the telnet configuration parameters for the device. A user having sufficient privilege level may change the values shown on this page.



Telnet Session Configuration

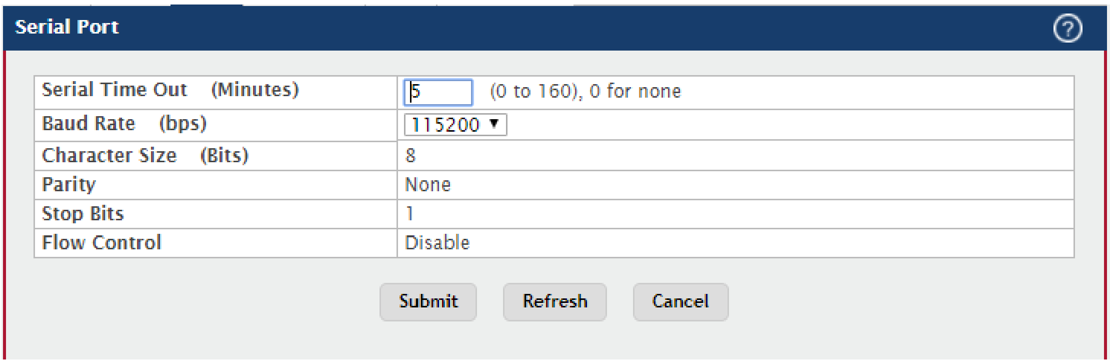
Admin Mode	○ Disable ● Enable
Telnet Port	23 (1 to 65535, 23 = Default)
Session Timeout (Minutes)	5 (1 to 160)
Maximum Number of Sessions	4 (0 to 4)
Allow New Sessions	☑

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

Telnet Port	The TCP port number on which the telnet server listens for requests. Existing telnet login sessions are not affected by a change in this value, although establishment of any new telnet sessions must use the new port number. Note: Before changing this value, check your system (e.g. using netstat) to make sure the desired port number is not currently being used by any other service.
Session Timeout	The telnet session inactivity timeout value, in minutes. A connected user that does not exhibit any telnet activity for this amount of time is automatically disconnected from the device.
Maximum Number of Sessions	The maximum number of telnet sessions that may be connected to the device simultaneously.
Allow New Sessions	Controls whether new telnet sessions are allowed. Setting this value to Disable disallows any new telnet sessions from starting (although existing telnet sessions are unaffected).

3.1.8.3 Serial

The Serial Port page displays the serial (console) port settings for the device. If you connect a terminal or PC to the device through the serial port, configure the terminal or terminal-emulation software with the settings that are displayed on this page to access the device command-line interface (CLI).



Serial Port

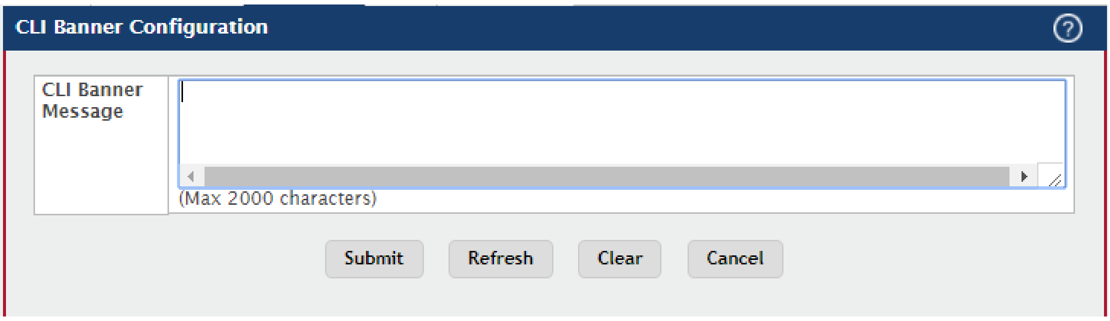
Serial Time Out (Minutes)	5 (0 to 160), 0 for none
Baud Rate (bps)	115200 ▼
Character Size (Bits)	8
Parity	None
Stop Bits	1
Flow Control	Disable

Field	Description
Serial Time Out	Serial port inactivity timeout value, in minutes. A logged-in user who does not exhibit any CLI activity through the serial port connection for this amount of time is automatically logged out of the device.
Baud Rate	The number of signals per second transmitted over the physical medium, measured in bits per second.
Character Size	The number of bits in a character. This value is always 8.

Parity	The parity method used on the serial port.
Stop Bits	The number of stop bits per character.
Flow Control	Indicates whether hardware flow control is enabled or disabled on the serial port.

3.1.8.4 CLI Banner

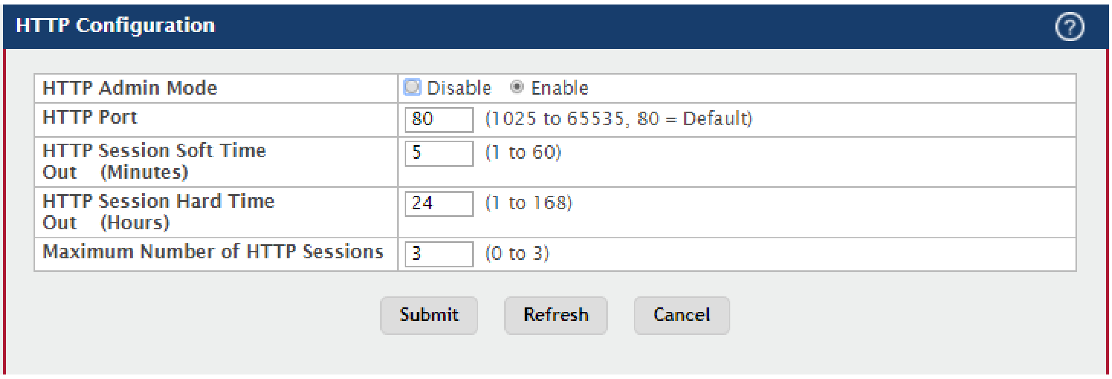
Use this page to configure the command-line interface (CLI) banner message that displays when a user connects to the device using a serial, telnet, or SSH session.



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

3.1.8.5 HTTP

Use this page to view and modify the HTTP settings on the device. HTTP allows web-based management access to the device from an administrative system.



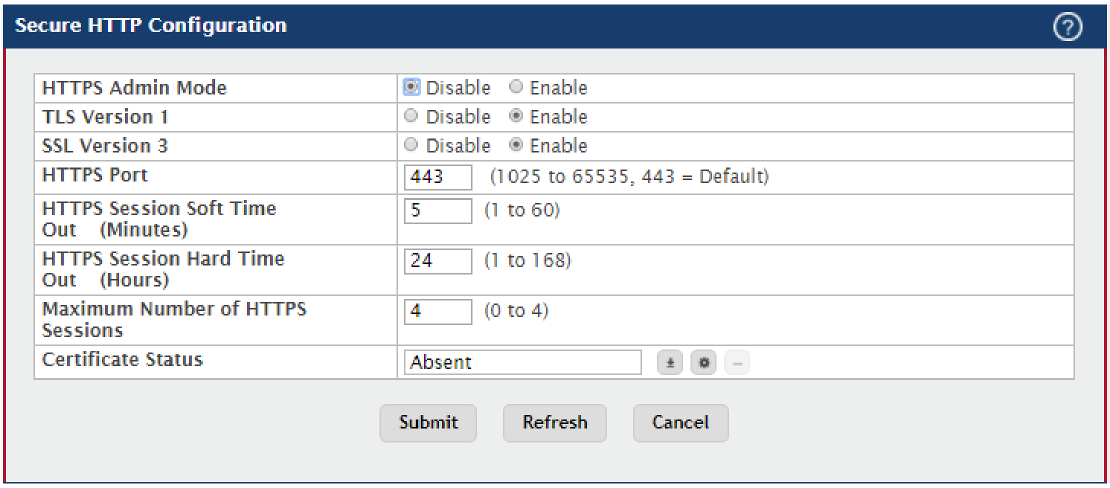
HTTP Configuration

HTTP Admin Mode	○ Disable ● Enable
HTTP Port	80 (1025 to 65535, 80 = Default)
HTTP Session Soft Time Out (Minutes)	5 (1 to 60)
HTTP Session Hard Time Out (Hours)	24 (1 to 168)
Maximum Number of HTTP Sessions	3 (0 to 3)

Field	Description
HTTP Admin Mode	Enables or disables the HTTP administrative mode. When enabled, the device can be accessed through a web browser using the HTTP protocol.
HTTP Port	The TCP port number on which the HTTP server listens for requests. Existing HTTP login sessions are closed whenever this value is changed. All new HTTP sessions must use the new port number. Note: Before changing this value, check your system (e.g. using netstat) to make sure the desired port number is not currently being used by any other service.
HTTP Session Soft Time Out (Minutes)	HTTP session inactivity timeout value. A logged-in user that does not exhibit any HTTP activity for this amount of time is automatically logged out of the HTTP session.
HTTP Session Hard Time Out (Hours)	HTTP session hard timeout value. A user connected to the device via an HTTP session is automatically logged out after this amount of time regardless of the amount of HTTP activity that occurs.
Maximum Number of HTTP Sessions	The maximum number of HTTP sessions that may be connected to the device simultaneously.

3.1.8.6 HTTPS

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



Secure HTTP Configuration

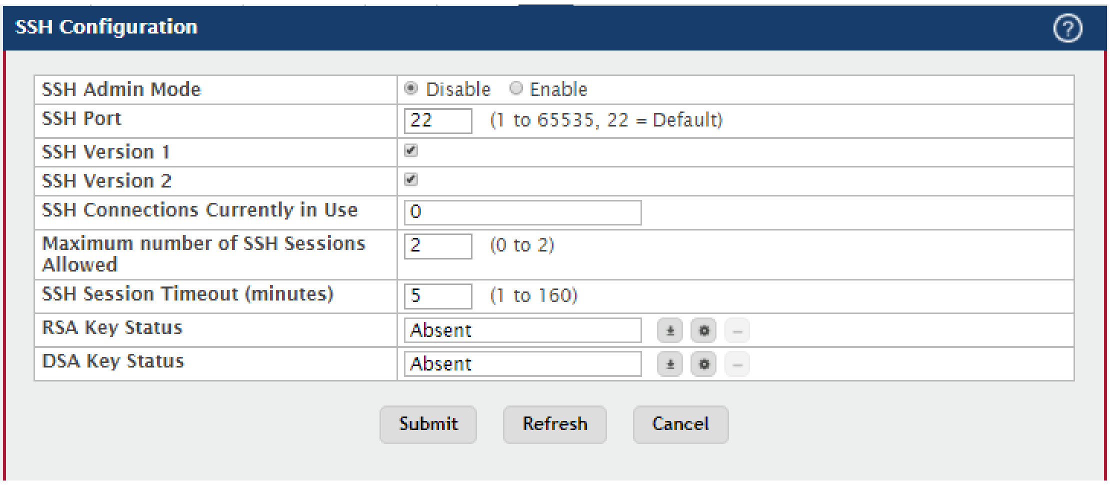
HTTPS Admin Mode	● Disable ○ Enable
TLS Version 1	○ Disable ● Enable
SSL Version 3	○ Disable ● Enable
HTTPS Port	443 (1025 to 65535, 443 = Default)
HTTPS Session Soft Time Out (Minutes)	5 (1 to 60)
HTTPS Session Hard Time Out (Hours)	24 (1 to 168)
Maximum Number of HTTPS Sessions	4 (0 to 4)
Certificate Status	Absent

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

Certificate Status	The status of the SSL certificate generation process. Present – The certificate has been generated and is present on the device Absent – Certificate is not available on the device Generation In Progress – An SSL certificate is currently being generated.
Download Certificates (Button)	Allows you to download an SSL certificate file from a remote system to the device. Note that to download SSL certificate files, SSL must be administratively disabled.
Generate Certificate (Button)	Generates an SSL certificate to use for secure communication between the web browser and the embedded web server on the device.
Delete Certificates (Button)	Deletes the SSL certificate. This button is available only if an SSL certificate is present on the device.
File Type	Specify the type of file to transfer from the device to a remote system.
Select File	Provides option to browse to the directory where the file is located and select the file to transfer to the device.
Status	Provides information about the status of the file transfer.

3.1.8.7 SSH

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



SSH Admin Mode	● Disable ○ Enable
SSH Port	22 (1 to 65535, 22 = Default)
SSH Version 1	☑
SSH Version 2	☑
SSH Connections Currently in Use	0
Maximum number of SSH Sessions Allowed	2 (0 to 2)
SSH Session Timeout (minutes)	5 (1 to 160)
RSA Key Status	Absent
DSA Key Status	Absent

Field	Description
SSH Admin Mode	Enables or disables the SSH server administrative mode. When this mode is enabled, the device can be accessed by using an SSH client on a remote system.
SSH Port	The TCP port number on which the SSH server listens for requests. Existing SSH login sessions are not affected by a change in this value, although establishment of any new SSH sessions must use the new port number. Note: Before changing this value, check your system (e.g. using netstat) to make sure the desired port number is not currently being used by any other service.
SSH Version 1	When this option is selected, the SSH server on the device can accept connections from an SSH client using SSH-1 protocol. If the option is clear, the device does not allow connections from clients using the SSH-1 protocol.
SSH Version 2	When this option is selected, the SSH server on the device can accept connections from an SSH client using SSH-2 protocol. If the option is clear, the device does not allow connections from clients using the SSH-2 protocol.
SSH Connections Currently in Use	The number of active SSH sessions between remote SSH clients and the SSH server on the device.
Maximum number of SSH Sessions Allowed	The maximum number of SSH sessions that may be connected to the device simultaneously.
SSH Session Timeout (minutes)	The SSH session inactivity timeout value. A connected user that does not exhibit any SSH activity for this amount of time is automatically disconnected from the device.
RSA Key Status	The status of the SSH-1 Rivest-Shamir-Adleman (RSA) key file or SSH-2 RSA key file (PEM Encoded) on the device, which might be Present, Absent, or Generation in Progress.
DSA Key Status	The status of the SSH-2 Digital Signature Algorithm (DSA) key file (PEM Encoded) on the device, which might be Present, Absent, or Generation in Progress.
Download Certificates (Button)	Use this button to download an SSH-1 RSA, SSH-2 RSA, or SSH-2 DSA key file from a remote system to the device. After you click the button, a Download Certificates window opens. Select the file type to download, browse to the location on the remote system, and select

	the file to upload. Then, click Begin Transfer. The Status field provides information about the file transfer.
Generate Certificate (Button)	Use this button to manually generate an RSA key or DSA key on the device.
Delete Certificates (Button)	Use this button to delete an RSA key or DSA key that has been downloaded to the device or manually generated on the device.
File Type	Specify the type of file to transfer from the device to a remote system.
Select File	Provides option to browse to the directory where the file is located and select the file to transfer to the device.
Status	Provides information about the status of the file transfer.

3.1.9 Management Security

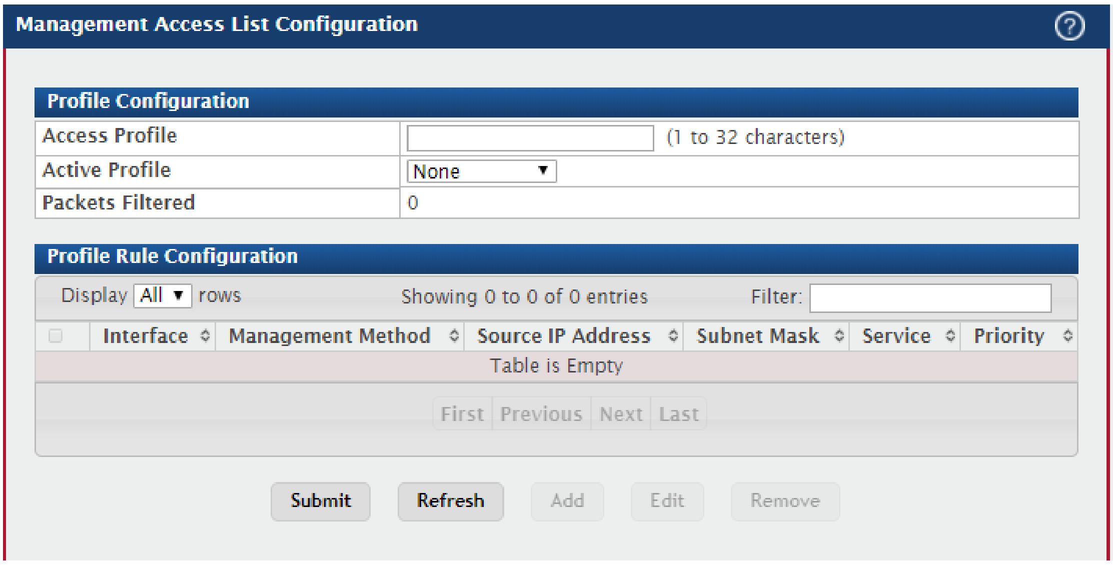
3.1.9.1 Access Profile

The administrator may elect to configure a management access control list. The Management Access Control and Administration List (ACAL) component is used to ensure that only known and trusted devices are allowed to remotely manage the switch via TCP/IP.

To configure The Management Access Control and Administration List, use the following buttons to perform the tasks:

- Use **Submit** button to edit the Profile Configuration.
- Use **Add** button to add Profile Rules to the Management Access Control list.
- Use **Edit** button to modify Profile Rules for the Management Access Control list.
- Use **Remove** button to remove Profile Rules.

NOTE: Profile rules cannot be added or modified when a profile is active.



Management Access List Configuration

Profile Configuration

Access Profile	(1 to 32 characters)
Active Profile	None ▾
Packets Filtered	0

Profile Rule Configuration

Display All ▾ rows Showing 0 to 0 of 0 entries Filter:

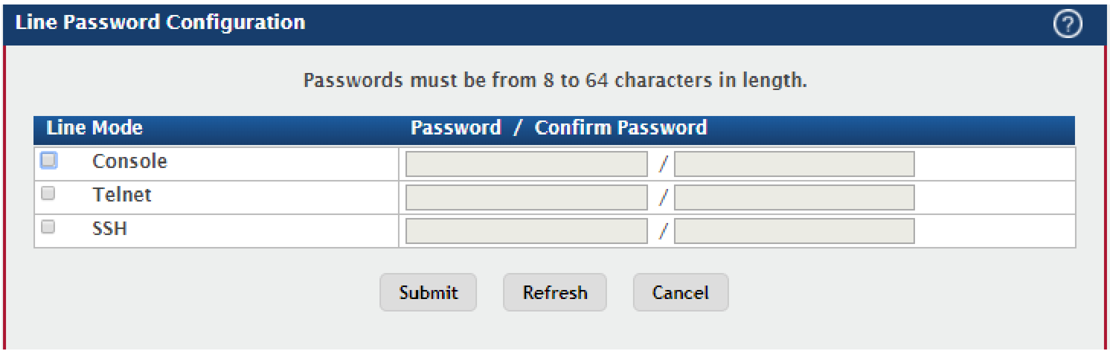
□	Interface	Management Method	Source IP Address	Subnet Mask	Service	Priority
Table is Empty						

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.
Interface	The port/interface or trunk ID.
Management Method	Below are 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.
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	Vlan number.
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	Indicates service type. Can be one of the following. ANY TELNET HTTP HTTPS SNMP SSH TFTP

	SNTP
Priority	Priority for the rule. Duplicates are not allowed.

3.1.10 Passwords

3.1.10.1 Line Password



Line Password Configuration

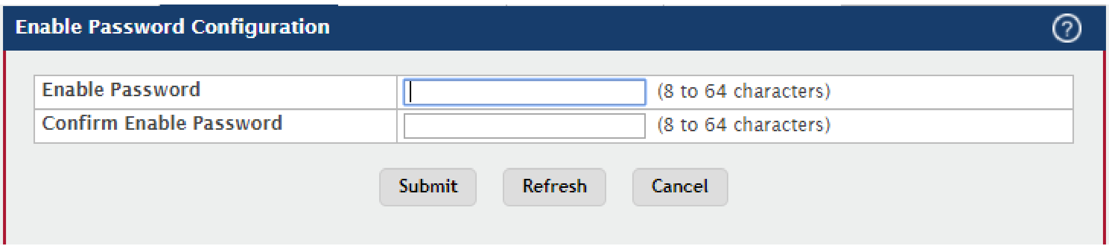
Passwords must be from 8 to 64 characters in length.

Line Mode	Password / Confirm Password
□ Console	/
□ Telnet	/
□ SSH	/

Field	Description
Line Mode	Any or all of the following passwords may be changed on this page by checking the box that precedes it: Console Telnet SSH
Password	Enter the new password for the corresponding Line Mode in this field. Be sure the password conforms to the allowed number of characters. The password characters are not displayed on the page, but are disguised in a browser-specific manner.
Confirm Password	Re-enter the new password for the corresponding Line Mode in this field. This must be the same value entered in the Password field. Be sure the password conforms to the allowed number of characters. The password characters are not displayed on the page, but are disguised in a browser-specific manner.

3.1.10.2 Enable Password

Use this page to set a local password to control CLI access to privileged levels.



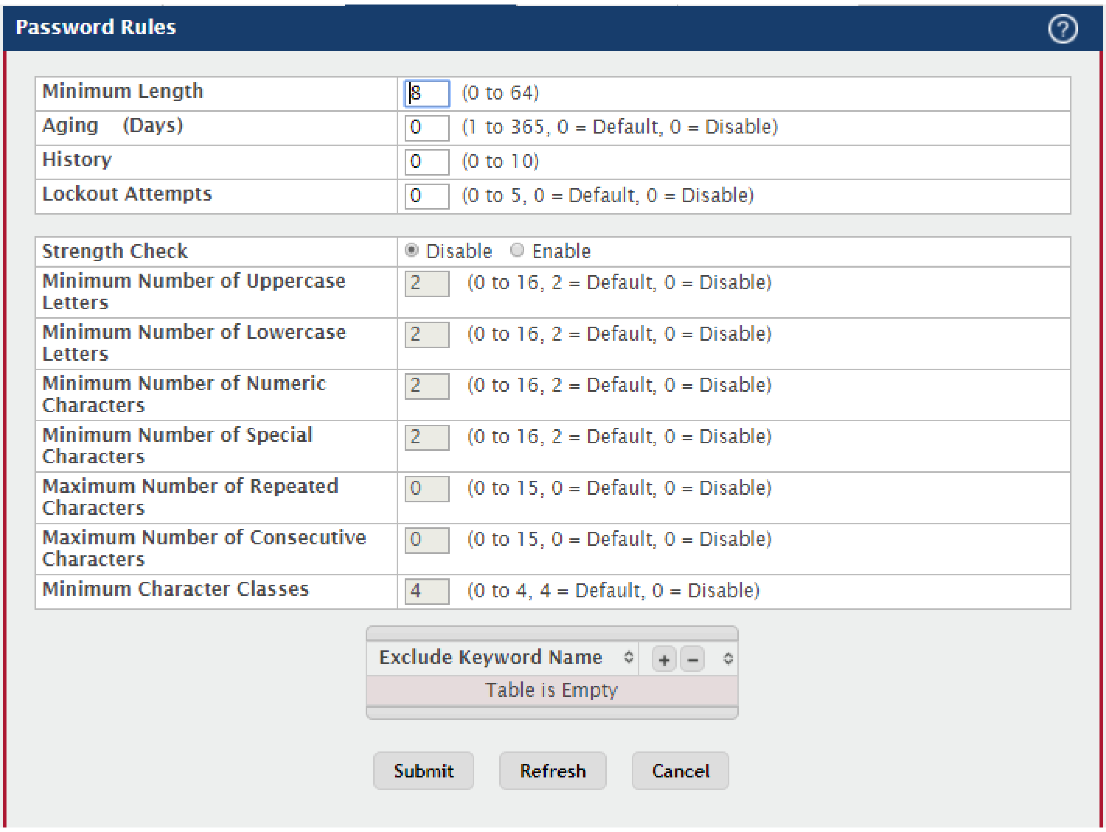
Enable Password Configuration

Enable Password		(8 to 64 characters)
Confirm Enable Password		(8 to 64 characters)

Field	Description
Enable Password	Specify the password all users must enter after executing the enable command at the CLI prompt.
Confirm Enable Password	Type the password again to confirm that you have entered it correctly.

3.1.10.3 Password Rules

Use this page to configure rules for locally-administered passwords. The rules you set determine the strength of local passwords that device users can associate with their usernames. The strength of a password is a function of length, complexity, and randomness.



Password Rules

Minimum Length	8	(0 to 64)
Aging (Days)	0	(1 to 365, 0 = Default, 0 = Disable)
History	0	(0 to 10)
Lockout Attempts	0	(0 to 5, 0 = Default, 0 = Disable)

Strength Check	● Disable ○ Enable	
Minimum Number of Uppercase Letters	2	(0 to 16, 2 = Default, 0 = Disable)
Minimum Number of Lowercase Letters	2	(0 to 16, 2 = Default, 0 = Disable)
Minimum Number of Numeric Characters	2	(0 to 16, 2 = Default, 0 = Disable)
Minimum Number of Special Characters	2	(0 to 16, 2 = Default, 0 = Disable)
Maximum Number of Repeated Characters	0	(0 to 15, 0 = Default, 0 = Disable)
Maximum Number of Consecutive Characters	0	(0 to 15, 0 = Default, 0 = Disable)
Minimum Character Classes	4	(0 to 4, 4 = Default, 0 = Disable)

Exclude Keyword Name
Table is Empty

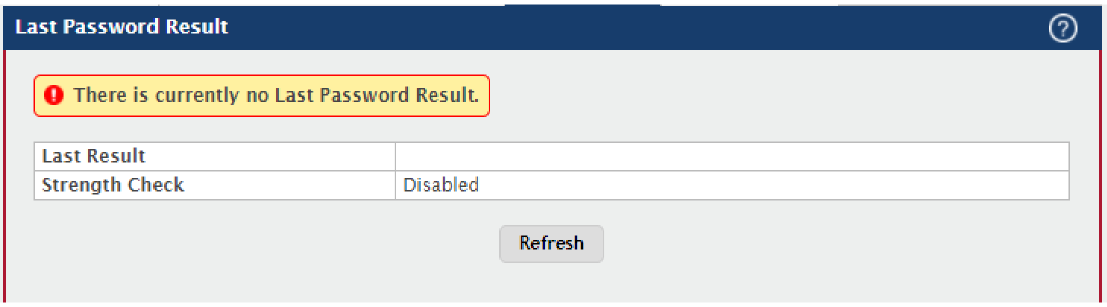
Field	Description
Minimum Length	The minimum number of characters required for a valid password.

Aging	The number of days that a user password is valid from the time the password is set. Once a password expires, the user is required to enter a new password at the next login.
History	The number of previous passwords that are retained to prevent password reuse. This helps to ensure that a user does not attempt to reuse the same password too often.
Lockout Attempts	The number of local authentication attempts that are allowed to fail before the user account is automatically locked.
Strength Check	Enables or disables the password strength checking feature. Enabling this feature forces the user to configure passwords that comply with the various strong password configuration parameters that are defined on this page.
Minimum Number of Uppercase Letters	The minimum number of upper-case letters that a valid password must contain.
Minimum Number of Lowercase Letters	The minimum number of lower-case letters that a valid password must contain.
Minimum Number of Numeric Characters	The minimum number of numeric characters that a valid password must contain.
Minimum Number of Special Characters	The minimum number of special characters (such as the keyboard symbols @, $, &) that a valid password must contain.
Maximum Number of Repeated Characters	The maximum number of characters of any type that are allowed to repeat in a valid password. Repetition is defined as the same character occurring in succession anywhere within the password, such as "11" or "%%%" or "EEEE".
Maximum Number of Consecutive Characters	The maximum number of characters belonging to a sequence that are allowed to occur in a valid password. Consecutive characters are defined as a sequential pattern of case-sensitive alphabetic or numeric characters, such as "2345" or "def" or "YZ".
Minimum Character Classes	This minimum number of character classes, defined as the various password strength categories listed above, that must be met in order for a password to be considered valid. It is permissible, therefore, to define strength checking criteria for each of the different types of conditions, but only require a valid password to meet some of them.

	The number of these character classes that must be met is specified by this value.
Exclude Keyword Name	The list of keywords that a valid password must not contain. Excluded keyword checking is case-insensitive. Additionally, a password cannot contain the backwards version of an excluded keyword. For example, if pass is an excluded keyword, passwords such as 23passA2c, ssapword, and PAsSwoRD are prohibited. Use the plus and minus buttons to perform the following tasks: To add a keyword to the list, click the + (plus) button, type the word to exclude in the Exclude Keyword Name field, and click Submit. To remove a keyword from the list, click the – (minus) button associated with the keyword to remove and confirm the action. To remove all keywords from the list, click the – (minus) button in the header row and confirm the action.

3.1.10.4 Last Password

Use this page to view information about the most recent result of a password change operation. These operations include setting the password for a user, setting the password for access to the device CLI (line password,) or enabling and setting the CLI privileged mode password.



Last Password Result

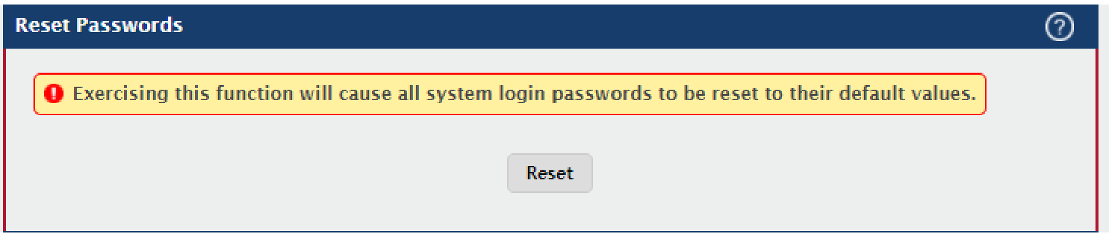
There is currently no Last Password Result.

Last Result	
Strength Check	Disabled

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

3.1.10.5 Reset Password

Initiates a reset of all login passwords to their factory default setting after displaying a confirmation message. The login password of every defined user is affected by this action.



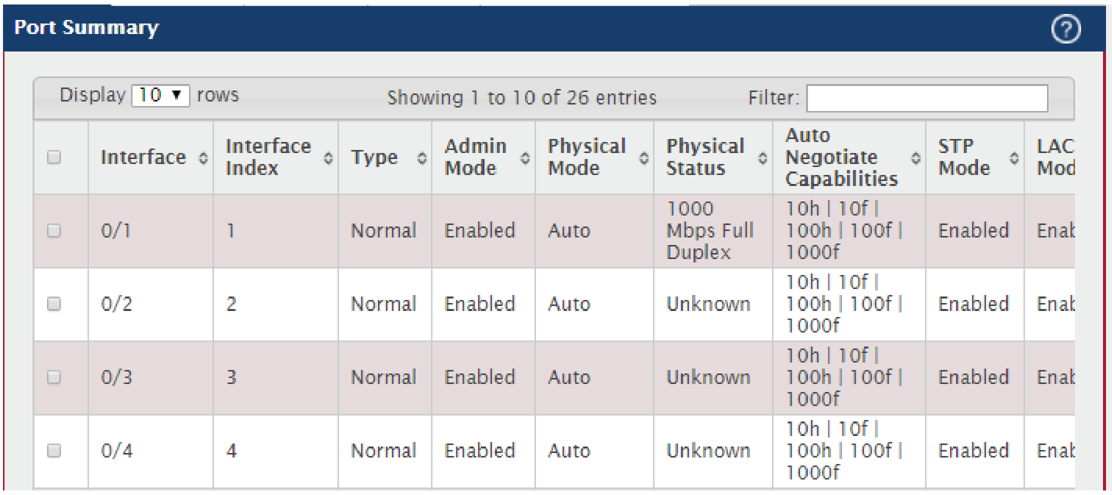
Reset Passwords

Exercising this function will cause all system login passwords to be reset to their default values.

3.1.11 Port

3.1.11.1 Summary

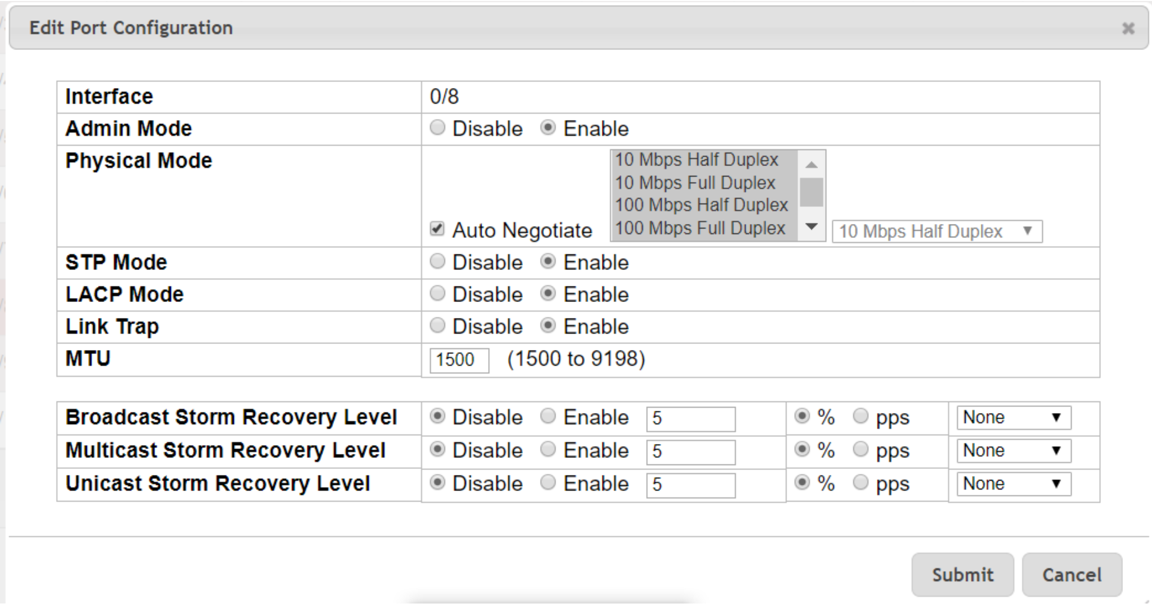
Use this page to view and configure information about all physical ports and Link Aggregation Groups (LAGs) on the device. LAGs are also known as port channels.



Port Summary

Display 10 rows Showing 1 to 10 of 26 entries Filter:

□	Interface	Interface Index	Type	Admin Mode	Physical Mode	Physical Status	Auto Negotiate Capabilities	STP Mode	LAC Mod
□	0/1	1	Normal	Enabled	Auto	1000 Mbps Full Duplex	10h | 10f | 100h | 100f | 1000f	Enabled	Enat
□	0/2	2	Normal	Enabled	Auto	Unknown	10h | 10f | 100h | 100f | 1000f	Enabled	Enat
□	0/3	3	Normal	Enabled	Auto	Unknown	10h | 10f | 100h | 100f | 1000f	Enabled	Enat
□	0/4	4	Normal	Enabled	Auto	Unknown	10h | 10f | 100h | 100f | 1000f	Enabled	Enat



Edit Port Configuration

Interface	0/8
Admin Mode	○ Disable ● Enable
Physical Mode	☑ Auto Negotiate 10 Mbps Half Duplex 10 Mbps Full Duplex 100 Mbps Half Duplex 100 Mbps Full Duplex 10 Mbps Half Duplex ▼
STP Mode	○ Disable ● Enable
LACP Mode	○ Disable ● Enable
Link Trap	○ Disable ● Enable
MTU	1500 (1500 to 9198)

Broadcast Storm Recovery Level	● Disable ○ Enable 5	● % ○ pps	None ▼
Multicast Storm Recovery Level	● Disable ○ Enable 5	● % ○ pps	None ▼
Unicast Storm Recovery Level	● Disable ○ Enable 5	● % ○ pps	None ▼

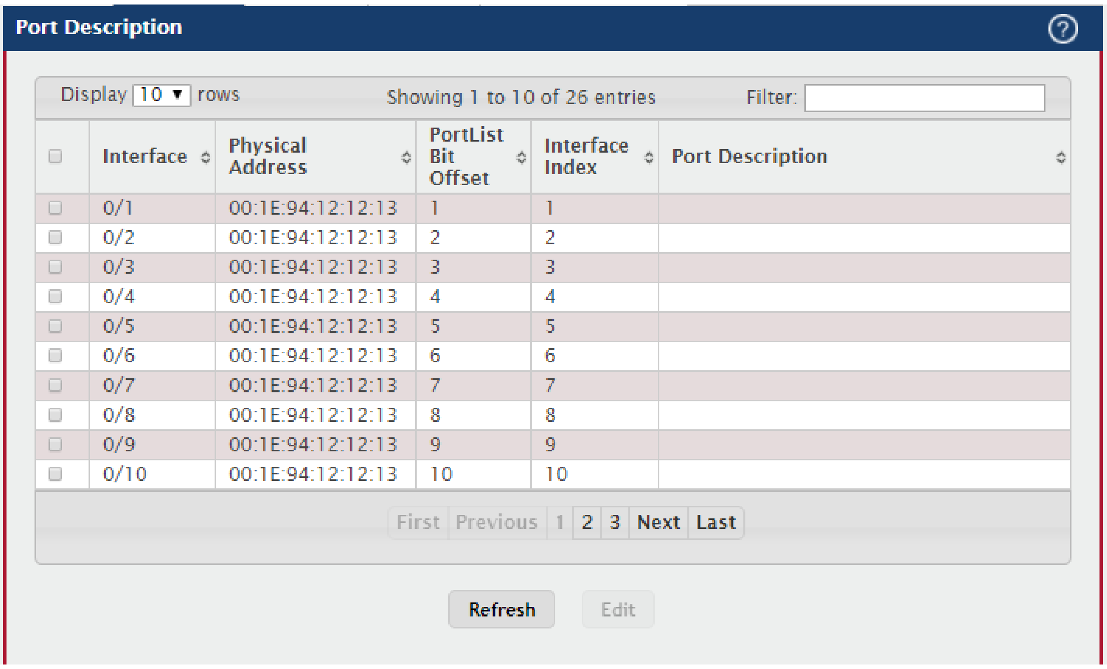
Field	Description
Interface	Identifies the port or LAG.
Interface Index	The interface index object value assigned by the IF-MIB. This value is used to identify the interface when managing the device by using SNMP.
Type	The interface type, which is one of the following: Normal - The port is a normal port, which means it is not a LAG member or configured for port mirroring. Trunk Member - The port is a member of a LAG. Mirrored - The port is configured to mirror its traffic (ingress, egress, or both) to another port (the probe port). Probe - The port is configured to receive mirrored traffic from one or more source ports.
Admin Mode	The administrative mode of the interface. If a port or LAG is administratively disabled, it cannot forward traffic.
Physical Mode	Indicates the port speed and duplex mode for physical interfaces. 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	Shows the administrative mode of the Link Aggregation Control Protocol (LACP), which is one of the following: Enabled - The port uses LACP for dynamic LAG configuration. When LACP is enabled, the port sends and receives LACP PDUs with its link partner to confirm that the external switch is also configured for link aggregation. Disabled - The port supports static LAG configuration only. This mode might be used when the port is connected to a device that does not support LACP. When a port is added to a LAG as a static member, it neither transmits nor receives LACP PDUs. N/A - For LAG ports.
Link Status	Indicates whether the link is up or down. The link is the physical connection between the port or LAG and the interface on another device.
Link Trap	Indicates whether the port will send an SNMP trap when link status changes.
Broadcast Storm Recovery Level	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 option "trap" sends trap messages at approximately every 30 seconds until broadcast storm control recovers.
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 option "trap" sends trap messages at approximately every 30 seconds until unicast storm control recovers.
MTU	Indicates MTU (Maximum Transmit Unit) of the interface. The actual frame size is calculated by adding ethernet header size in MTU.

3.1.11.2 Description

Use this page to view information that helps identify each interface. Also, the description field associated with the port(s) or LAG(s) on the device can be edited.



Port Description

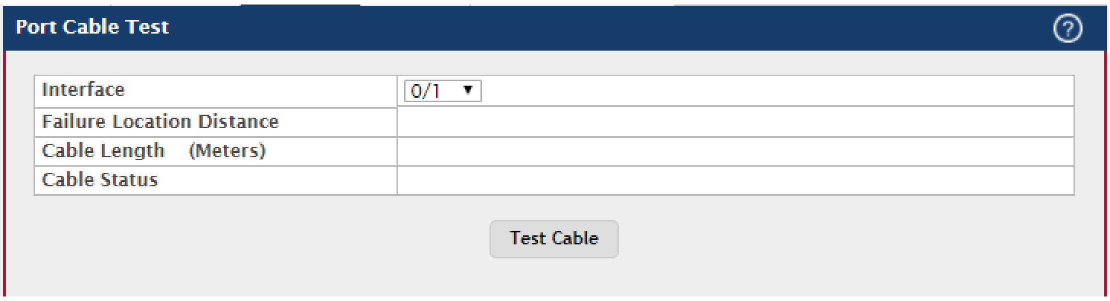
Display 10 ▾ rows   Showing 1 to 10 of 26 entries   Filter:

□	Interface	Physical Address	PortList Bit Offset	Interface Index	Port Description
□	0/1	00:1E:94:12:12:13	1	1	
□	0/2	00:1E:94:12:12:13	2	2	
□	0/3	00:1E:94:12:12:13	3	3	
□	0/4	00:1E:94:12:12:13	4	4	
□	0/5	00:1E:94:12:12:13	5	5	
□	0/6	00:1E:94:12:12:13	6	6	
□	0/7	00:1E:94:12:12:13	7	7	
□	0/8	00:1E:94:12:12:13	8	8	
□	0/9	00:1E:94:12:12:13	9	9	
□	0/10	00:1E:94:12:12:13	10	10	

Field	Description
Interface	Identifies the port or LAG.
Physical Address	The MAC address of the interface.
PortList Bit Offset	The bit offset value that corresponds to the interface when the MIB object type Port List is used when managing the device by using 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	The current description, if any, associated with the interface to help identify it.

3.1.11.3 Cable Test

Use this page to test the cable connected to a port on the device. The cable test uses Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested.



Port Cable Test

Interface	0/1 ▼
Failure Location Distance	
Cable Length (Meters)	
Cable Status	

Field	Description
Interface	Select the port with the connected cable to test.
Cable Status	Displays the cable status as one of the following: 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.
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 Distance	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.
Test Cable (Button)	Perform a cable test on the selected interface. The cable test may take up to 2 seconds to complete. If the port has an active link, the link is not taken down, and the Cable Status always indicates Normal. The test returns a cable length estimate if this feature is supported by the PHY for the current link speed. Note: If the link is down and a cable is attached to a 10/100 Ethernet adapter, the Cable Status may indicate Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded.

3.1.11.4 Mirroring

Use this page to configure port mirroring on the device. Port mirroring is used to monitor the network traffic that one or more ports or the ports within a VLAN send and receive. The Port Mirroring feature creates a copy of the traffic that the source interface handles and sends it to a destination port or a Remote Switched Port Analyzer (RSPAN) VLAN. All traffic from the source can be mirrored and sent toward the destination, or you can specify that only traffic flows that match the criteria in an ACL are mirrored. The source is the port or VLAN that is being monitored. The destination is where the packets from the source port are sent. When the destination is a port on the local device, a network protocol analyzer is typically connected to the port.

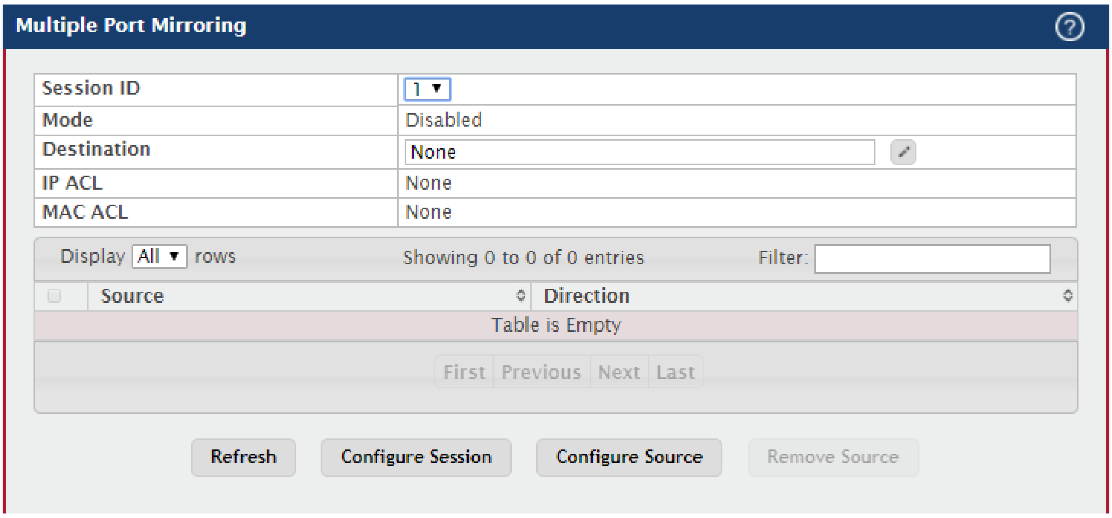
Use the buttons to perform the following tasks:

To configure the administrative mode for a port mirroring session or to select an ACL for flow-based mirroring, click Configure Session and configure the desired settings.

To configure one or more source ports or a VLAN 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.

To configure the destination for the mirrored traffic, click the Edit icon in the Destination field.



Multiple Port Mirroring

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

Display All ▾ rows Showing 0 to 0 of 0 entries Filter:

□	Source	Direction
Table is Empty		

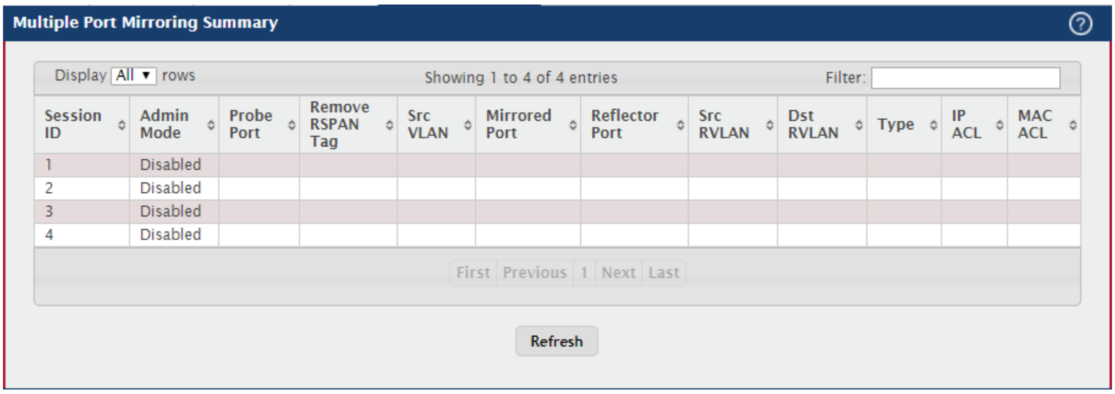
Field	Description
Session ID	The port mirroring session ID. The number of sessions allowed is platform specific.
Mode	The administrative mode for the selected port mirroring session. If the mode is disabled, the configured source is not mirroring traffic to the destination.
Destination	The interface that receives traffic from all configured source ports. After you click the Edit icon, the Destination Configuration window opens. The following information describes the additional fields available in this window. **Type** The type of interface to use as the destination, which is one of the following: **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.
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.
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 (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. After you click Configure Source, the Source Configuration window opens. The following information describes the additional fields that appear in this window. **Type** The type of interface to use as the source, which is one of the following: **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.

3.1.11.5 Mirroring Summary

Use this page to view port mirroring summary.



Multiple Port Mirroring Summary

Display All rows   Showing 1 to 4 of 4 entries   Filter:

Session ID	Admin Mode	Probe Port	Remove RSPAN Tag	Src VLAN	Mirrored Port	Reflector Port	Src RVLAN	Dst RVLAN	Type	IP ACL	MAC ACL
1	Disabled										
2	Disabled										
3	Disabled										
4	Disabled										

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 RSPAN destination port are double tagged. Enable this option to remove RSPAN VLAN ID tag for 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.
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.

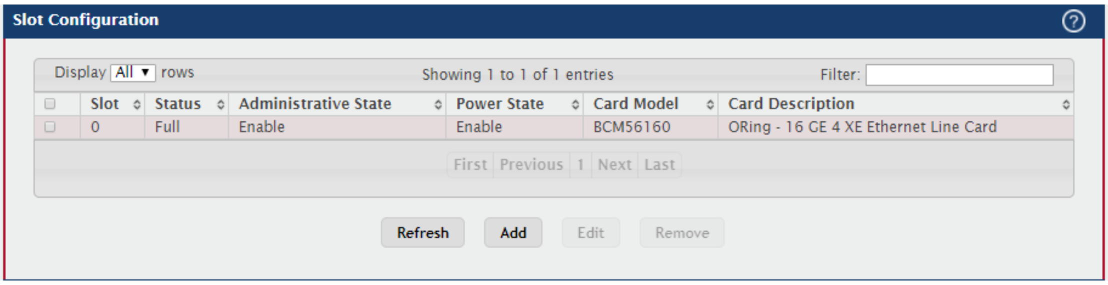
3.1.12 Slot

3.1.12.1 Configuration

Use this page to view information about the cards installed in the device's slots and to configure settings for the slots available on the device. Support for adding cards to a slot or changing the slot configuration is platform dependent.

Use the buttons to perform the following tasks:

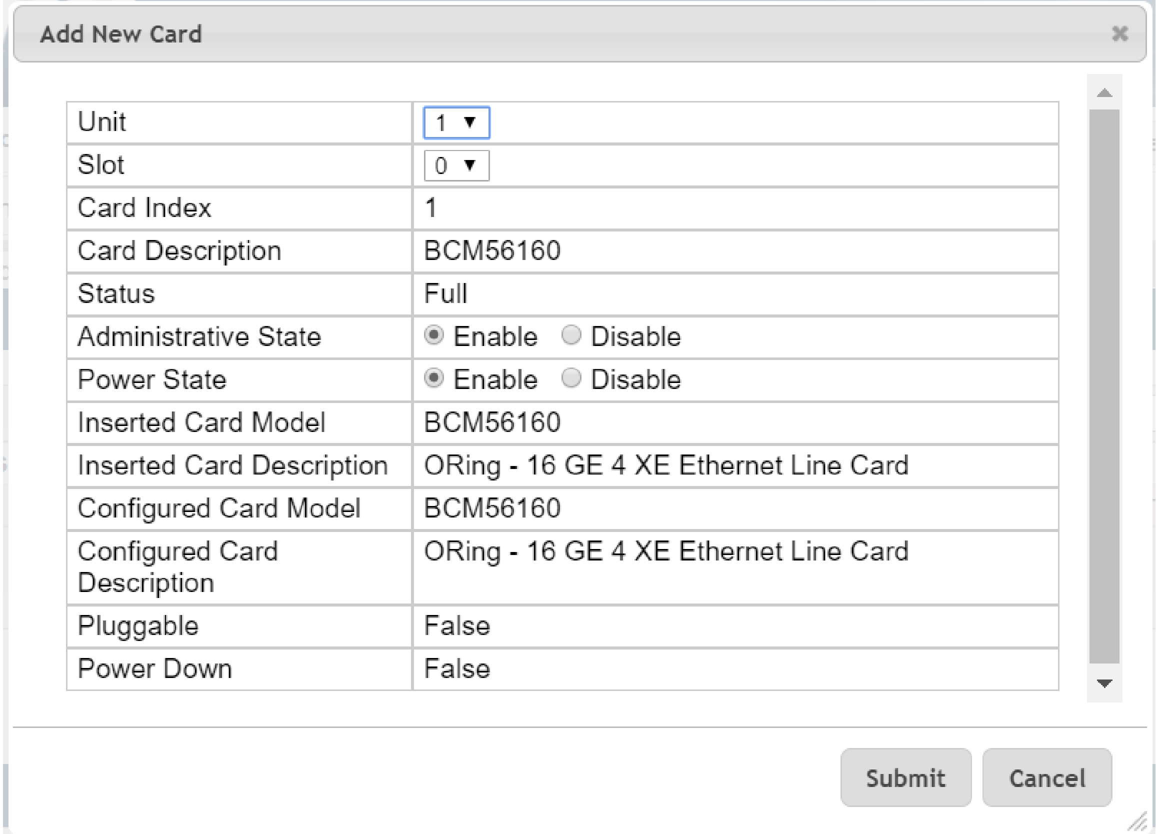
To preconfigure a card before adding it to a slot, click Add and configure the desired settings.
To change slot or card settings, select the check box associated with the entry and click Edit.
To delete a slot configuration entry from the list, select the check box associated with each entry to delete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



Slot Configuration

Display All rows   Showing 1 to 1 of 1 entries   Filter:

□	Slot	Status	Administrative State	Power State	Card Model	Card Description
□	0	Full	Enable	Enable	BCM56160	ORing - 16 GE 4 XE Ethernet Line Card



Add New Card

Unit	1
Slot	0
Card Index	1
Card Description	BCM56160
Status	Full
Administrative State	● Enable ○ Disable
Power State	● Enable ○ Disable
Inserted Card Model	BCM56160
Inserted Card Description	ORing - 16 GE 4 XE Ethernet Line Card
Configured Card Model	BCM56160
Configured Card Description	ORing - 16 GE 4 XE Ethernet Line Card
Pluggable	False
Power Down	False

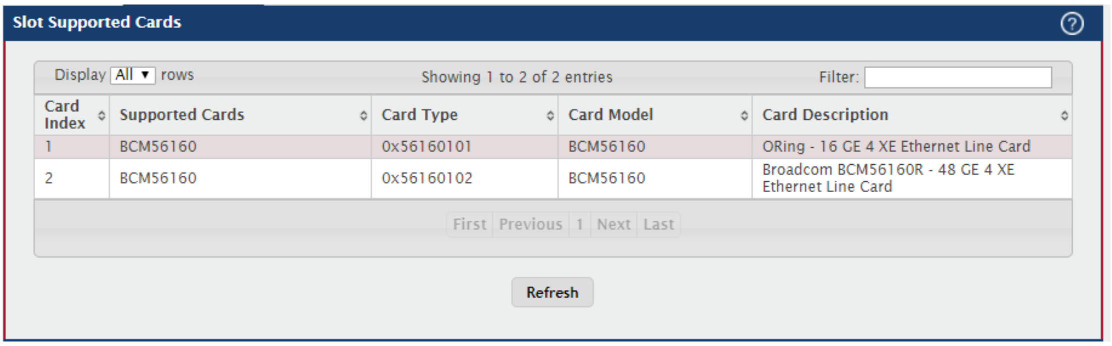
Field	Description
Slot	Identifies the slot number.
Status	Indicates whether the slot is empty or full.
Administrative State	Indicates whether the slot is administratively enabled or disabled. For some devices, you can change the Administrative State when you add or edit slot information.
Power State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

In addition to the fields described above, the following non-configurable information is available in the dialog box used for adding or editing slot information.

Field	Description
Unit	Identifies the unit number of the device (in the stack of devices) on which to add the new card.
Card Index	Identifies the index number assigned to the card. This value is helpful when configuring the system by using SNMP.
Inserted Card Model	The model ID of the card plugged into the slot.
Inserted Card Description	The description of the card plugged into the slot.
Configured Card Model	The model ID of the card configured for the slot.
Configured Card Description	The description of the card configured for the slot.
Pluggable	If the value is True, the card can be administratively enabled or disabled. If the value is False, the Administrative State cannot be configured.
Power Down	If the value is True, the Power State can be administratively enabled or disabled. If the value is False, the Power State cannot be configured.

3.1.12.2 Supported Cards

This page displays information about the cards the device supports.



Slot Supported Cards

Display All ▾ rows   Showing 1 to 2 of 2 entries   Filter:

Card Index	Supported Cards	Card Type	Card Model	Card Description
1	BCM56160	0x56160101	BCM56160	ORing - 16 GE 4 XE Ethernet Line Card
2	BCM56160	0x56160102	BCM56160	Broadcom BCM56160R - 48 GE 4 XE Ethernet Line Card

Field	Description
Card Index	The index assigned to the card type.
Supported Cards	The model of the card that can be supported.
Card Type	The hardware type of the supported card, which is assigned by the manufacturer.

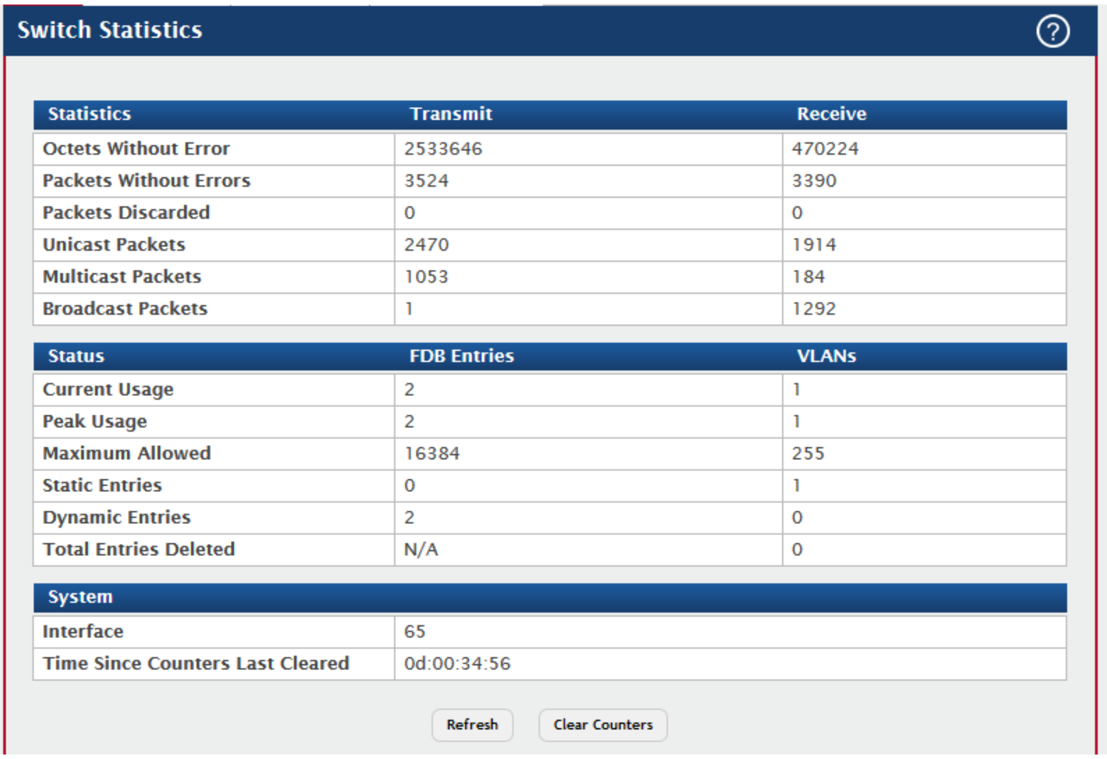
Card Model	Similar to the Supported Cards information, this field identifies the model of the supported card.
Card Description	Description of the supported card, which might include the manufacturer's product number and information about number and speed of the supported interfaces.

3.1.13 Statistics

3.1.13.1 System

3.1.13.1.1 Switch

This page shows summary information about traffic transmitted and received on the device, entries in the MAC address table, and Virtual Local Area Networks (VLANs) that exist on the device.



Switch Statistics

Statistics	Transmit	Receive
Octets Without Error	2533646	470224
Packets Without Errors	3524	3390
Packets Discarded	0	0
Unicast Packets	2470	1914
Multicast Packets	1053	184
Broadcast Packets	1	1292

Status	FDB Entries	VLANs
Current Usage	2	1
Peak Usage	2	1
Maximum Allowed	16384	255
Static Entries	0	1
Dynamic Entries	2	0
Total Entries Deleted	N/A	0

System	
Interface	65
Time Since Counters Last Cleared	0d:00:34:56

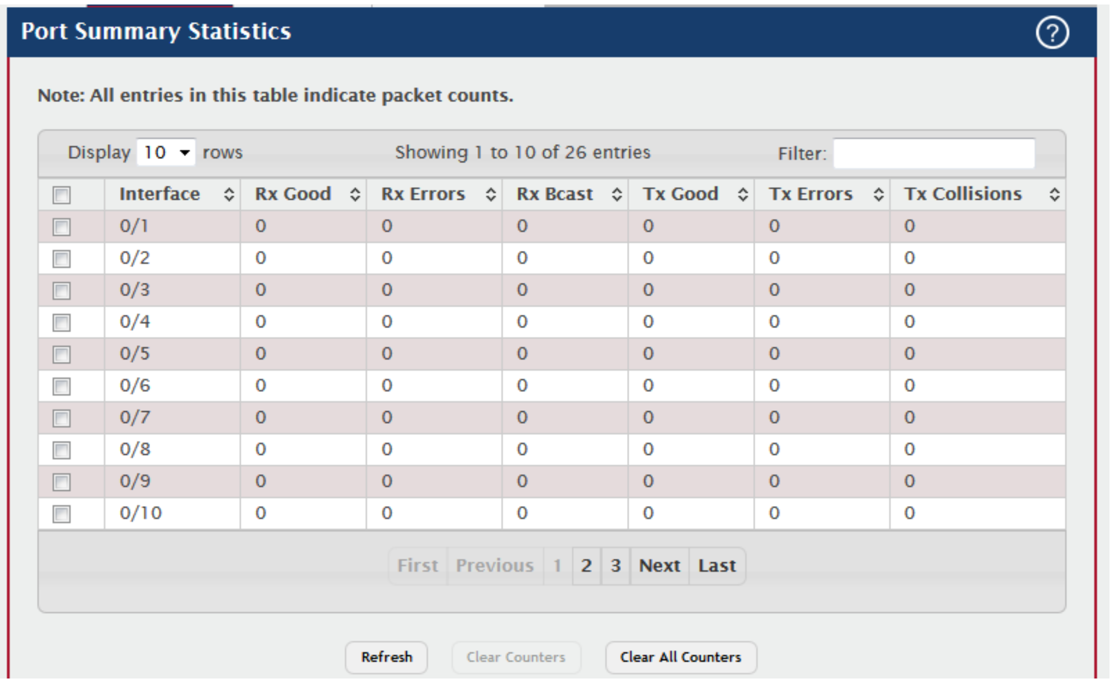
Field	Description
Statistics	
Octets Without Error	The total number of octets (bytes) of data successfully transmitted or received by the processor (excluding framing bits but including FCS octets).
Packets Without Errors	The total number of packets including unicast, broadcast, and multicast packets, 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.
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	The amount of time in days, hours, minutes, and seconds, that has passed since the statistics for this device were last reset.

Cleared	
Clear Counters (Button)	Reset all switch summary and detailed statistics values on this page to the default values. The discarded packets count cannot be cleared.

3.1.13.1.2 Port Summary

This page shows statistical information about the packets received and transmitted by each port and LAG.



Port Summary Statistics

Note: All entries in this table indicate packet counts.

Display 10 rows   Showing 1 to 10 of 26 entries   Filter:

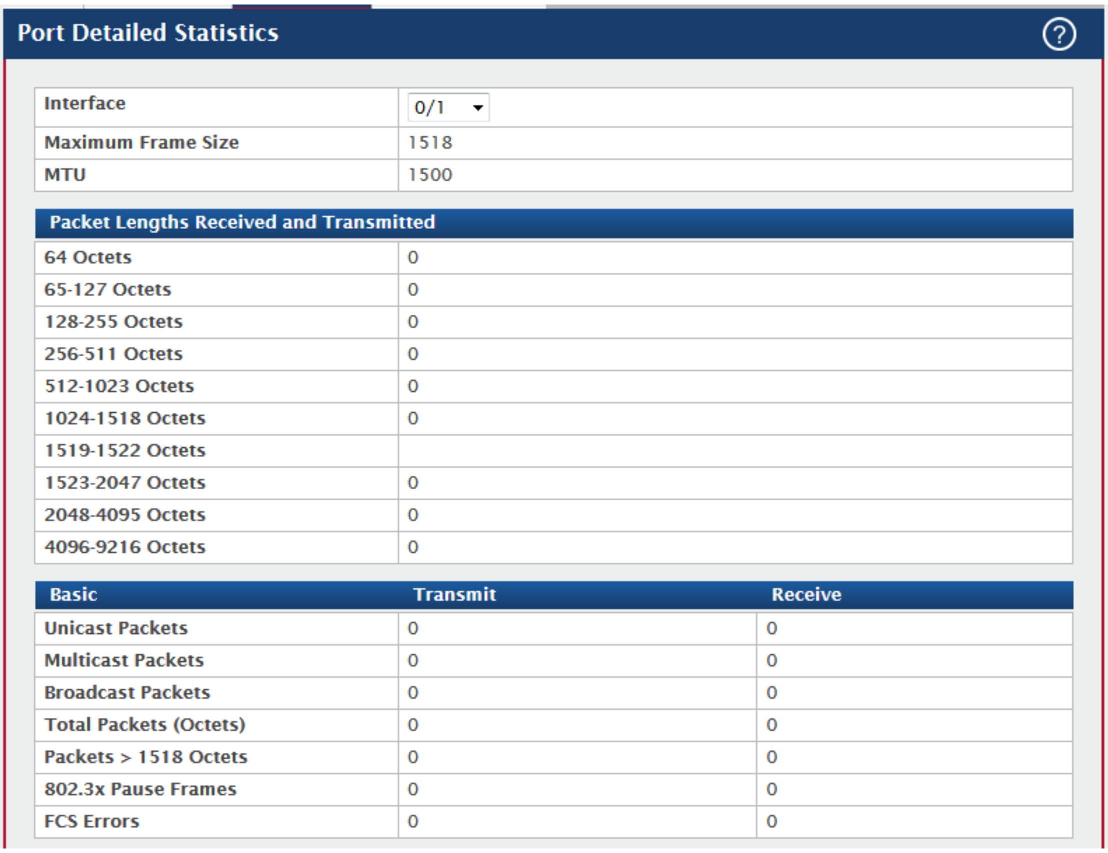
□	Interface	Rx Good	Rx Errors	Rx Bcast	Tx Good	Tx Errors	Tx Collisions
□	0/1	0	0	0	0	0	0
□	0/2	0	0	0	0	0	0
□	0/3	0	0	0	0	0	0
□	0/4	0	0	0	0	0	0
□	0/5	0	0	0	0	0	0
□	0/6	0	0	0	0	0	0
□	0/7	0	0	0	0	0	0
□	0/8	0	0	0	0	0	0
□	0/9	0	0	0	0	0	0
□	0/10	0	0	0	0	0	0

Field	Description
Interface	Identifies the port or LAG.
Rx Good	The total number of inbound packets received by the interface without errors.
Rx Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Rx Bcast	The total number of good packets received that were directed to the broadcast address. 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.

3.1.13.1.3 Port Detailed

This page shows detailed information about the traffic transmitted and received by each interface.

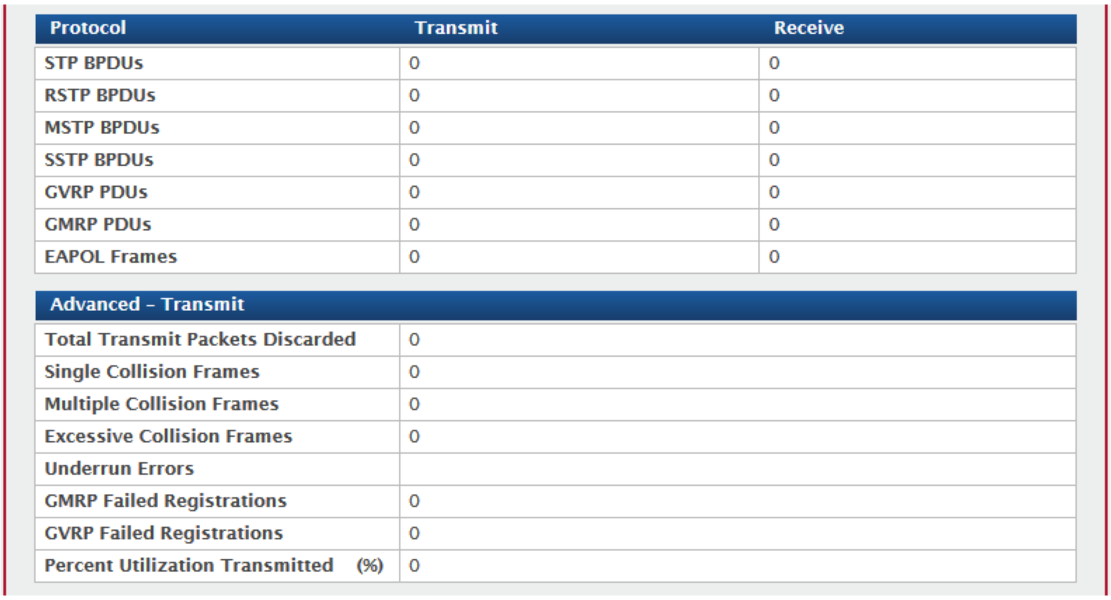


Port Detailed Statistics

Interface	0/1
Maximum Frame Size	1518
MTU	1500

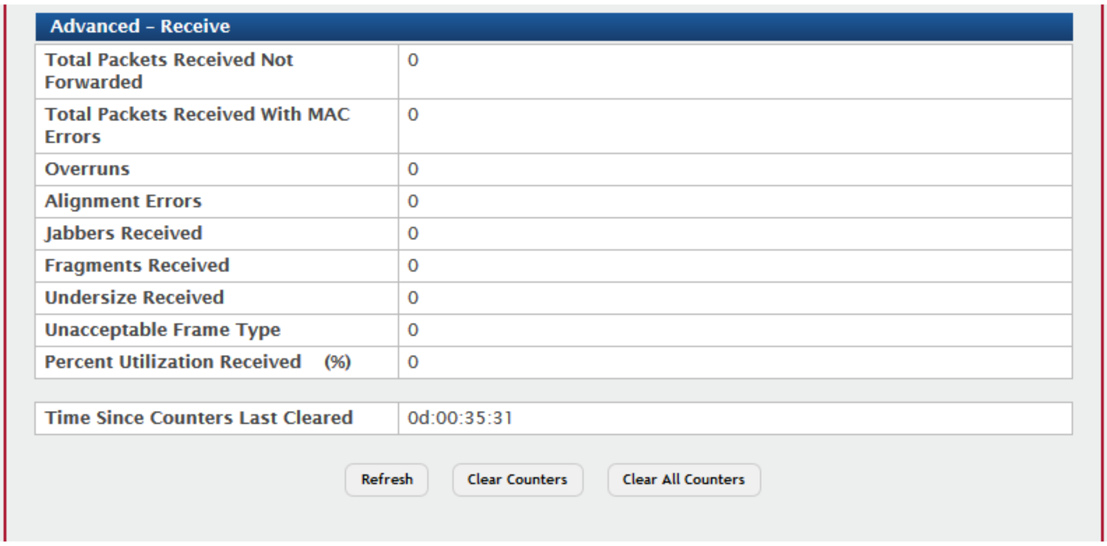
Packet Lengths Received and Transmitted	
64 Octets	0
65-127 Octets	0
128-255 Octets	0
256-511 Octets	0
512-1023 Octets	0
1024-1518 Octets	0
1519-1522 Octets	
1523-2047 Octets	0
2048-4095 Octets	0
4096-9216 Octets	0

Basic	Transmit	Receive
Unicast Packets	0	0
Multicast Packets	0	0
Broadcast Packets	0	0
Total Packets (Octets)	0	0
Packets > 1518 Octets	0	0
802.3x Pause Frames	0	0
FCS Errors	0	0



Protocol	Transmit	Receive
STP BPDUs	0	0
RSTP BPDUs	0	0
MSTP BPDUs	0	0
SSTP BPDUs	0	0
GVRP PDUs	0	0
GMRP PDUs	0	0
EAPOL Frames	0	0

Advanced - Transmit	
Total Transmit Packets Discarded	0
Single Collision Frames	0
Multiple Collision Frames	0
Excessive Collision Frames	0
Underrun Errors	
GMRP Failed Registrations	0
GVRP Failed Registrations	0
Percent Utilization Transmitted (%)	0



Advanced – Receive

Total Packets Received Not Forwarded	0
Total Packets Received With MAC Errors	0
Overruns	0
Alignment Errors	0
Jabbers Received	0
Fragments Received	0
Undersize Received	0
Unacceptable Frame Type	0
Percent Utilization Received (%)	0

Time Since Counters Last Cleared	0d:00:35:31

Field	Description
Interface	Identifies the port or LAG. To view the statistics for a specific interface, select the interface number from the drop-down menu. The page automatically refreshes with the statistics for the selected interface.
Maximum Frame Size	The maximum Ethernet frame size the interface supports or is configured to support. The maximum frame size includes the Ethernet header, CRC, and payload.
MTU	Indicates MTU (Maximum Transmit Unit) of the interface. The actual frame size is calculated by adding ethernet header size in MTU.
Packet Lengths Received and Transmitted	
64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
1519-1522 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
1523-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Basic	
Unicast Packets	The Transmit column shows the total number of packets that higher-level protocols requested be transmitted to a subnetwork unicast address, including those that were discarded or not sent. The Receive column shows the number of subnetwork unicast packets delivered to a higher-layer protocol.
Multicast Packets	The Transmit column shows the total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent. The Receive column shows the number of multicast packets delivered to a higher-layer protocol.
Broadcast Packets	The Transmit column shows the total number of packets that higher-level protocols requested be transmitted to a broadcast address, including those that were discarded or not sent. The Receive column shows the number of broadcast packets delivered to a higher-layer protocol.
Total Packets (Octets)	The total number of octets of data (including those in bad packets) transmitted or received on the interface (excluding framing bits but including FCS octets). This object can be used as a reasonable

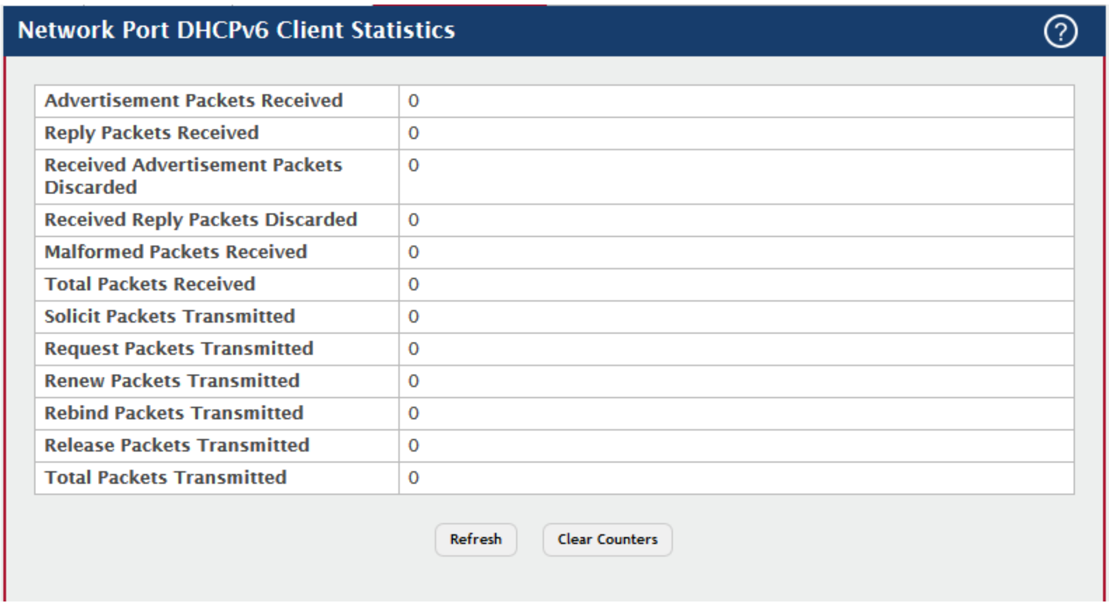
	estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets > 1518 Octets	The total number of packets transmitted or received by this interface that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. This counter has a maximum increment rate of 815 counts per sec at 10 Mb/s.
802.3x Pause Frames	The number of MAC Control frames transmitted or received by this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
FCS Errors	The total number of packets transmitted or received by this interface that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.
Protocol	
STP BPDUs	The number of Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) transmitted or received by the interface.
RSTP BPDUs	The number of Rapid STP BPDUs transmitted or received by the interface.
MSTP BPDUs	The number of Multiple STP BPDUs transmitted or received by the interface.
SSTP BPDUs	The number of Shared Spanning Tree Protocol (SSTP) Bridge Protocol Data Units (BPDUs) transmitted or received by the interface.
GVRP PDUs	The number of Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) PDUs transmitted or received by the interface.
GMRP PDUs	The number of GARP Multicast Registration Protocol (GMRP) PDUs transmitted or received by the interface.
EAPOL Frames	The number of Extensible Authentication Protocol (EAP) over LAN (EAPOL) frames transmitted or received by the interface for IEEE 802.1X port-based network access control.
Advanced - Transmit	
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one

	collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Underrun Errors	The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.
GMRP Failed Registrations	The number of times attempted GMRP registrations could not be completed.
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed.
Percent Utilization Transmitted	The value of link utilization in percentage representation for TX line.
Advanced - Receive	
Total Packets Received Not Forwarded	The number of inbound packets which were chosen to be discarded to prevent them from being delivered to a higher-layer protocol, even though no errors had been detected. One possible reason for discarding such a packet is to free up buffer space.
Total Packets Received With MAC Errors	The total number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
Unacceptable Frame Type	The number of frames discarded from this interface due to being a frame type that the interface cannot accept.
Percent Utilization Received	The value of link utilization in percentage representation for RX line.
Time Since Counters Last Cleared	The amount of time in days, hours, minutes, and seconds, that has passed since the statistics for this interface were last reset.
Clear Counters (Button)	Reset the detailed statistics for the selected interface to the default values.
Clear All Counters (Button)	Reset the detailed statistics for all interfaces to the default values.

3.1.13.1.4 Network DHCPv6

This page displays the DHCPv6 client statistics values for the network interface. The DHCPv6 client on the device exchanges several different types of UDP messages with one or more network DHCPv6 servers during the process of acquiring address, prefix, or other relevant network configuration information from the server. The values indicate the various counts that have accumulated since they were last cleared.



Network Port DHCPv6 Client Statistics

Advertisement Packets Received	0
Reply Packets Received	0
Received Advertisement Packets Discarded	0
Received Reply Packets Discarded	0
Malformed Packets Received	0
Total Packets Received	0
Solicit Packets Transmitted	0
Request Packets Transmitted	0
Renew Packets Transmitted	0
Rebind Packets Transmitted	0
Release Packets Transmitted	0
Total Packets Transmitted	0

Field	Description
Advertisement Packets Received	Number of DHCPv6 advertisement messages received from one or more DHCPv6 servers in response to the client's solicit message.
Reply Packets Received	Number of DHCPv6 reply messages received from one or more DHCPv6 servers in response to the client's request message.
Received Advertisement Packets Discarded	Number of DHCPv6 advertisement messages received from one or more DHCPv6 servers to which the client did not respond.
Received Reply Packets Discarded	Number of DHCPv6 reply messages received from one or more DHCPv6 servers to which the client did not respond.
Malformed Packets Received	Number of messages received from one or more DHCPv6 servers that were improperly formatted.
Total Packets Received	Total number of messages received from all DHCPv6 servers.
Solicit Packets Transmitted	Number of DHCPv6 solicit messages the client sent to begin the process of acquiring network information from a DHCPv6 server.
Request Packets Transmitted	Number of DHCPv6 request messages the client sent in response to a DHCPv6 server's advertisement message.
Renew Packets Transmitted	Number of renew messages the DHCPv6 client has sent to the server to request an extension of the lifetime of the information provided by the server. This message is sent to the DHCPv6 server that originally assigned the addresses and configuration information.
Rebind Packets Transmitted	Number of rebind messages the DHCPv6 client has sent to any available DHCPv6 server to request an extension of its addresses and an update to any other relevant information. This message is sent only if the client does not receive a response to the renew message.
Release Packets Transmitted	Number of release messages the DHCPv6 client has sent to the server to indicate that it no longer needs one or more of the assigned addresses.
Total Packets Transmitted	Total number of messages sent to all DHCPv6 servers.
Clear Counters (Button)	Clears all of the statistics displayed on this page by resetting them to their default values.

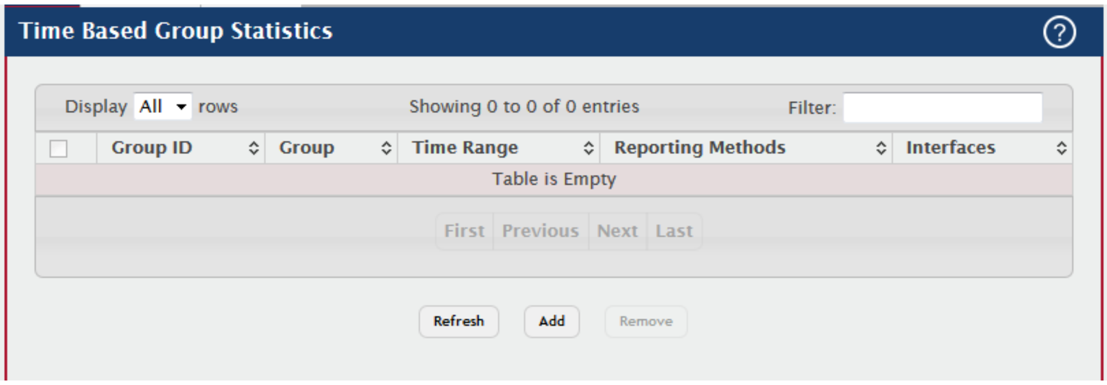
3.1.13.2 Time Based Group Statistics

3.1.13.2.1 Group

Use this page to define criteria for collecting time-based statistics for interface traffic. The time-based statistics can be useful for troubleshooting and diagnostics purposes. The statistics application uses the system clock for time-based reporting, so it is important to configure the system clock (manually or through SNTP) before using this feature.

Use the buttons to perform the following tasks:

- To add a set of time-based traffic group statistics to collect, click **Add** and configure the desired settings.
- To delete one or more time-based statistics groups, select each entry to delete and click **Remove**.



Field	Description
Group	The type of traffic statistics to collect for the group, which is one of the following: Received – The number of packets received on the interfaces within the group. Received Errors – The number of packets received with errors on the interfaces within the group. Transmitted – The number of packets transmitted by the interfaces within the group. Received Transmitted – The number of packets received and transmitted by the interfaces within the group. Port Utilization – The percentage of total bandwidth used by the port within the specified time period. Congestion – The percentage of time within the specified time range

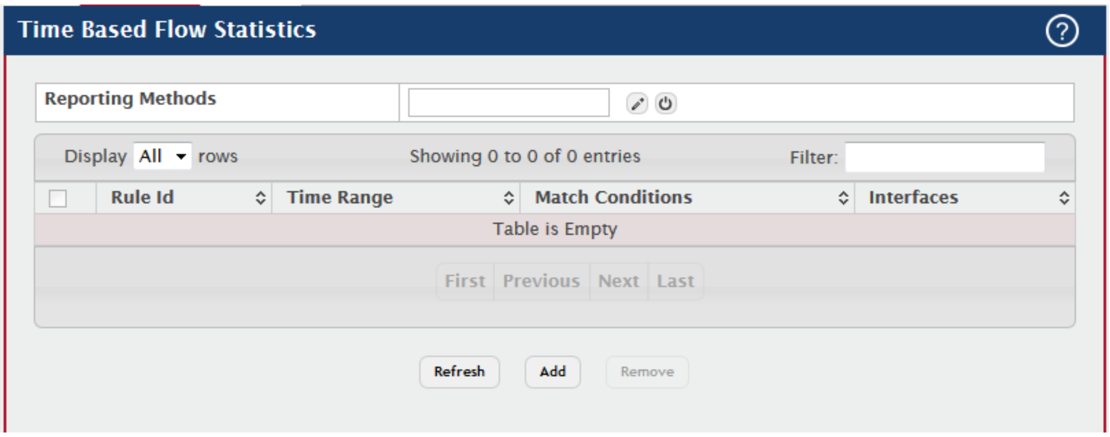
	that the ports experienced congestion.
Time Range	The name of the periodic or absolute time range to use for data collection. The time range is configured by using the Time Range Summary and Time Range Entry Summary pages. The time range must be configured on the system before the time-based statistics can be collected.
Reporting Methods	The methods for reporting the collected statistics at the end of every configured time range interval. The available options are: None – The statistics are not reported to the console or an external server. They can be viewed only by using the web interface or by issuing a CLI command. Console – The statistics are displayed on the console. E-Mail – The statistics are sent to an e-mail address. The SNTP server and e-mail address information is configured by using the appropriate Email Alerts pages. Syslog – The statistics are sent to a remote syslog server. The syslog server information is configured on the Logging Hosts page.
Interfaces	The interface or interfaces on which data is collected. To select multiple interfaces when adding a new group, CTRL + click each interface to include in the group.

3.1.13.2.2 Flow Based

Use this page to define criteria for collecting time-based statistics for specific traffic flows. The statistics include a per-interface hit count based on traffic that meets the match criteria configured in a rule for the interfaces included in the rule. The hit count statistics are collected only during the specified time range. The statistics application uses the system clock for time-based reporting. Configure the system clock (manually or through SNTP) before using the time-based statistics feature.

Use the buttons to perform the following tasks:

- To add a rule and define criteria for flow-based statistics that are collected within a time range, click **Add** and configure the desired settings.
- To delete one or more flow-based rules for time-based statistics, select each entry to delete and click **Remove**.



Time Based Flow Statistics

Reporting Methods

Display All rows Showing 0 to 0 of 0 entries Filter:

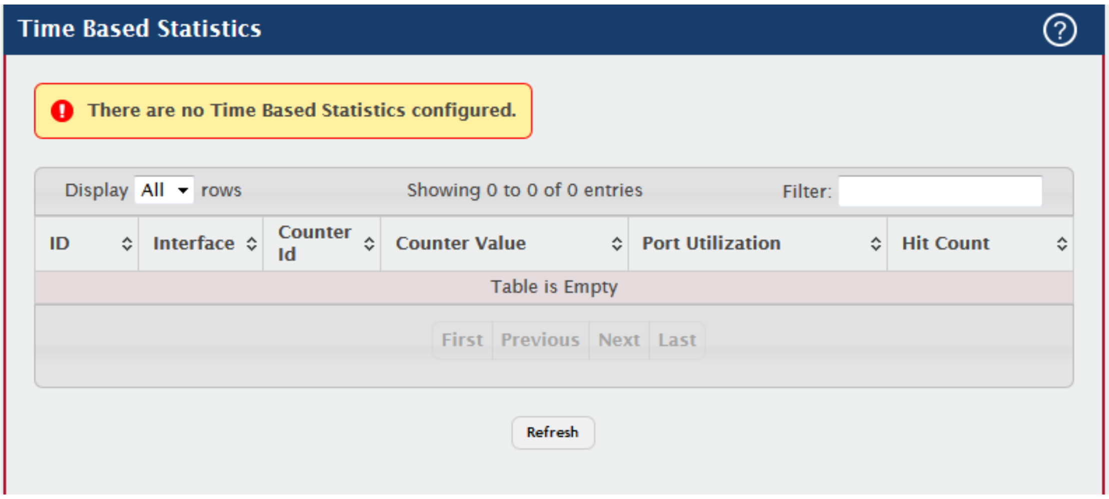
□	Rule Id	Time Range	Match Conditions	Interfaces
Table is Empty				

Field	Description
Reporting Methods	The methods for reporting the collected statistics at the end of every configured interval. To change the reporting methods for all flow-based statistics rules, click the Edit icon and select one or more methods. To reset the field to the default value, click the Reset icon. The available reporting methods are: **None** – The statistics are not reported to the console or an external server. They can be viewed only by using the web interface or by issuing a CLI command. **Console** – The statistics are displayed on the console. **E-Mail** – The statistics are sent to an e-mail address. The SNTP server and e-mail address information is configured by using the appropriate Email Alerts pages. **Syslog** – The statistics are sent to a remote syslog server. The syslog server information is configured on the Logging Hosts page.
Rule Id	The number that identifies the flow-based statistics collection rule.
Time Range	The name of the periodic or absolute time range to use for data collection. The time range is configured by using the Time Range Summary and Time Range Entry Summary pages. The time range must be configured on the system before the time-based statistics can be collected.
Match Conditions	The criteria a packet must meet to match the rule.
Interfaces	The interface or interfaces on which the flow-based rule is applied. Only traffic on the specified interfaces is checked against the rule. After you click Add, the Time Based Flow Configuration window opens and allows you to configure a rule for traffic flow statistics. The match conditions are optional, but the rule must specify at least one match

	condition. The following information describes the match criteria fields that are available in this window.
Match All	Select this option to indicate that all traffic matches the rule and is counted in the statistics. This option is exclusive to all other match criteria, so if Match All is selected, no other match criteria can be configured.
Source IP	The source IP address to match in the IPv4 packet header.
Destination IP	The destination IP address to match in the IPv4 packet header.
Source MAC	The source MAC address to match in the ingress frame header.
Destination MAC	The destination MAC address to match in the ingress frame header.
Source TCP Port	The TCP source port to match in the TCP header.
Destination TCP Port	The TCP destination port to match in the TCP header.
Source UDP Port	The UDP source port to match in the UDP header.
Destination UDP Port	The UDP destination port to match in the UDP header.

3.1.13.2.3 Statistics

Use this page to view time-based statistics collected for the configured traffic groups and flow-based rules.


Time Based Statistics

There are no Time Based Statistics configured.

Display All rows Showing 0 to 0 of 0 entries Filter:

ID	Interface	Counter Id	Counter Value	Port Utilization	Hit Count
Table is Empty					

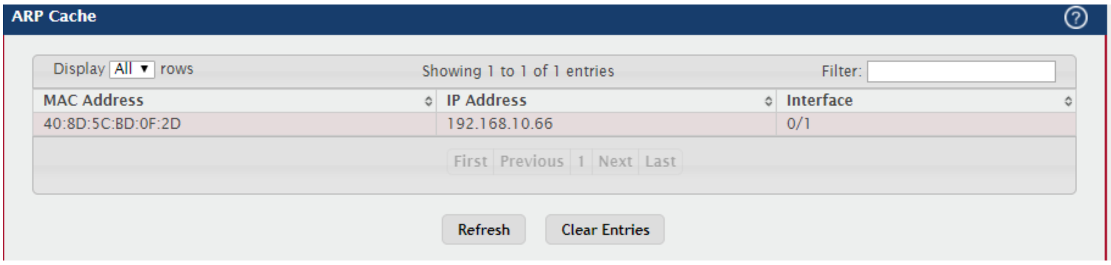
Field	Description
ID	The traffic group name or flow-based rule ID associated with the rest of the statistics in the row.
Interface	The interface on which the statistics were reported.

Counter Id	For traffic group statistics, this field identifies the type of traffic.
Counter Value	For traffic group statistics, this field shows the number of packets of the type identified by the Counter Id field that were reported on the interface during the time range.
Port Utilization	For a port utilization traffic group, this field reports the percentage of the total available bandwidth used on the interface during the time range.
Hit Count	For flow-based statistics, this field reports the number of packets that matched the flow-based rule criteria during the time range.

3.1.14 Status

3.1.14.1 ARP Cache

The Address Resolution Protocol (ARP) dynamically maps physical (MAC) addresses to Internet (IP) addresses. This page shows the current contents of the system-wide ARP cache, listed as a table of connections, that are used when managing the device.


ARP Cache

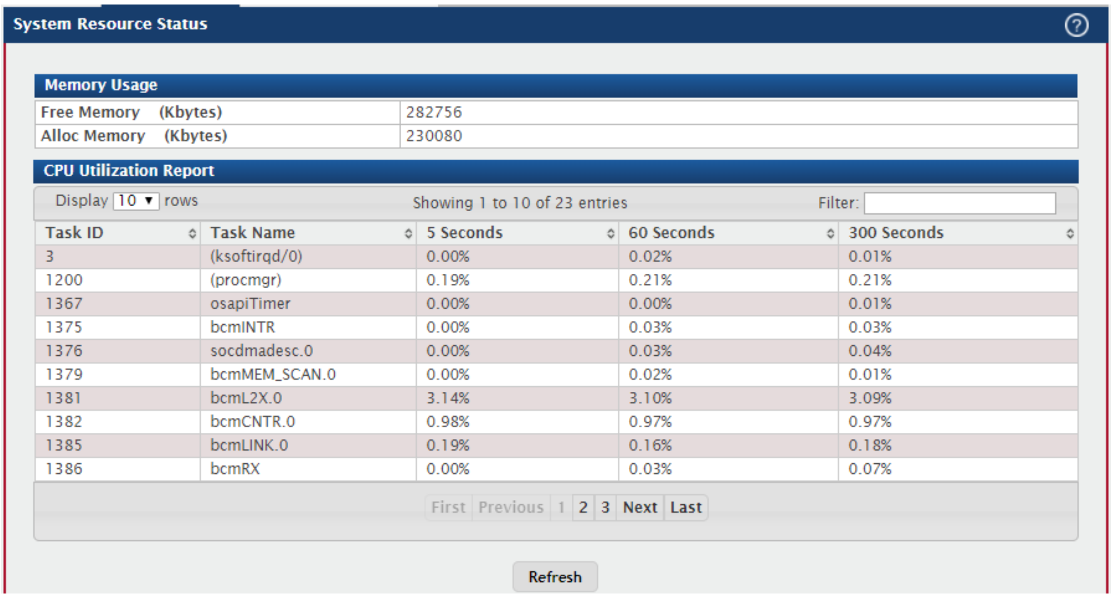
Display All rows Showing 1 to 1 of 1 entries Filter:

MAC Address	IP Address	Interface
40:8D:5C:BD:0F:2D	192.168.10.66	0/1

Field	Description
MAC Address	The physical (MAC) address associated with the IP address of the connection.
IP Address	The Internet (IP) address of the connection.
Interface	Shows the switch port through which the connection was established, or displays as Management if the connection occurred via a non-network port interface (if applicable).
Clear Entries (Button)	Clears all entries from the system ARP Cache.

3.1.14.2 Resource Status

This web page displays status information indicating the CPU utilization and free memory in the system.



System Resource Status

Memory Usage

Free Memory (Kbytes)	282756
Alloc Memory (Kbytes)	230080

CPU Utilization Report

Display 10 rows   Showing 1 to 10 of 23 entries   Filter:

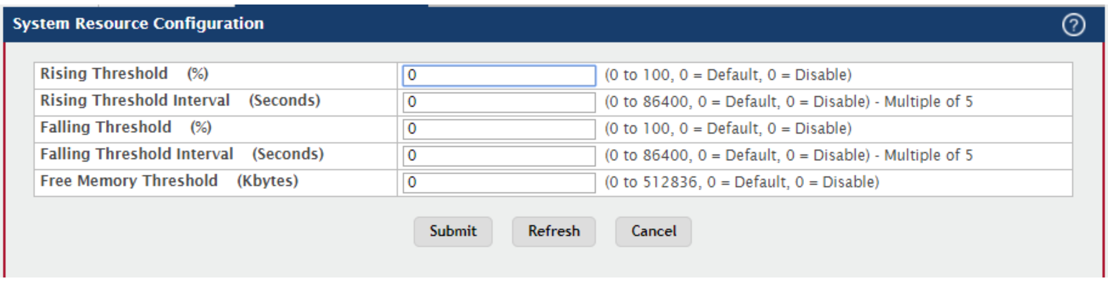
Task ID	Task Name	5 Seconds	60 Seconds	300 Seconds
3	(ksoftirqd/0)	0.00%	0.02%	0.01%
1200	(procmgr)	0.19%	0.21%	0.21%
1367	osapiTimer	0.00%	0.00%	0.01%
1375	bcmINTR	0.00%	0.03%	0.03%
1376	socdmadesc.0	0.00%	0.03%	0.04%
1379	bcmMEM_SCAN.0	0.00%	0.02%	0.01%
1381	bcmL2X.0	3.14%	3.10%	3.09%
1382	bcmCNTR.0	0.98%	0.97%	0.97%
1385	bcmLINK.0	0.19%	0.16%	0.18%
1386	bcmRX	0.00%	0.03%	0.07%

Field	Description
Free Memory	The amount of system memory that is currently available for allocation, specified in kilobytes.
Alloc Memory	The amount of system memory that is currently allocated for use, specified in kilobytes.
Task ID	System task identifier. The entry named Total represents the total CPU utilization, expressed as a percentage, that is used by the entire system for each of the specified time intervals.
Task Name	System task name.
5 Seconds	The percentage amount of CPU utilization consumed by the corresponding task in the last 5 seconds.
60 Seconds	The percentage amount of CPU utilization consumed by the corresponding task in the last 60 seconds.
300 Seconds	The percentage amount of CPU utilization consumed by the corresponding task in the last 300 seconds.

An additional column is shown in the table corresponding to the Rising Threshold Period, in seconds, if this has been configured to a value other than zero.

3.1.14.3 Resource Configuration

Use this page to configure the threshold parameters for monitoring CPU utilization and the amount of free memory in the system.



System Resource Configuration

Rising Threshold (%)	0	(0 to 100, 0 = Default, 0 = Disable)
Rising Threshold Interval (Seconds)	0	(0 to 86400, 0 = Default, 0 = Disable) - Multiple of 5
Falling Threshold (%)	0	(0 to 100, 0 = Default, 0 = Disable)
Falling Threshold Interval (Seconds)	0	(0 to 86400, 0 = Default, 0 = Disable) - Multiple of 5
Free Memory Threshold (Kbytes)	0	(0 to 512836, 0 = Default, 0 = Disable)

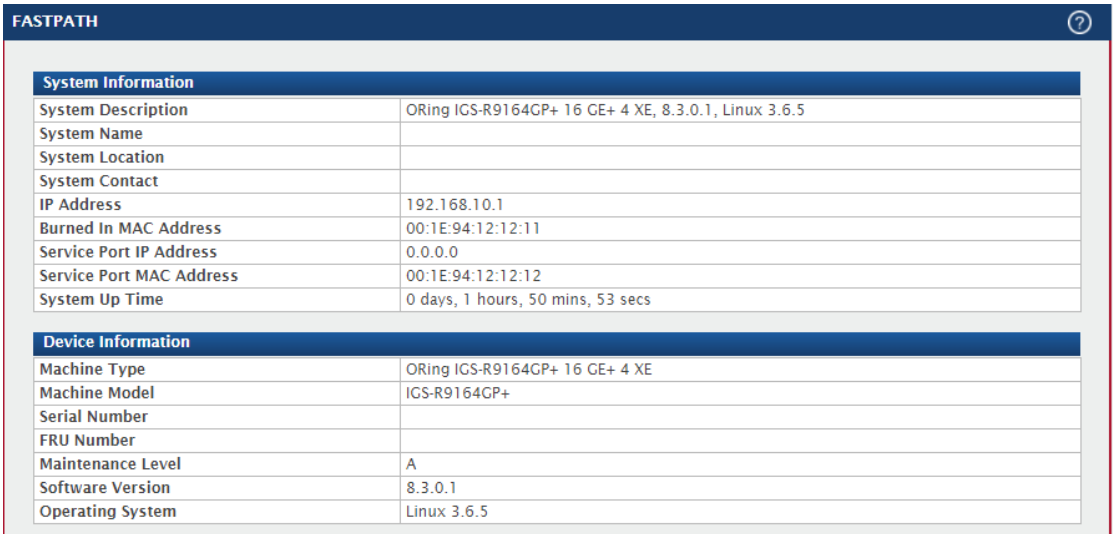
Field	Description
Rising Threshold	The CPU utilization rising threshold, expressed as a percentage. When the CPU utilization is increasing, an event is signaled when it reaches or exceeds this level.
Rising Threshold Interval	The CPU utilization rising threshold interval in seconds. This represents how often the current CPU utilization is checked against the configured rising threshold value.
Falling Threshold	The CPU utilization falling threshold, expressed as a percentage. When the CPU utilization is decreasing, an event is signaled when it reaches or falls below this level.
Falling Threshold Interval	The CPU utilization falling threshold interval in seconds. This represents how often the current CPU utilization is checked against the configured falling threshold value.
Free Memory Threshold	The free memory threshold in kilobytes. If enabled, an event is signaled when the amount of free memory in the system falls below this value.

Note: Setting any these configuration values to zero disables monitoring of that particular item and suppresses its corresponding event notification.

3.1.15 Summary

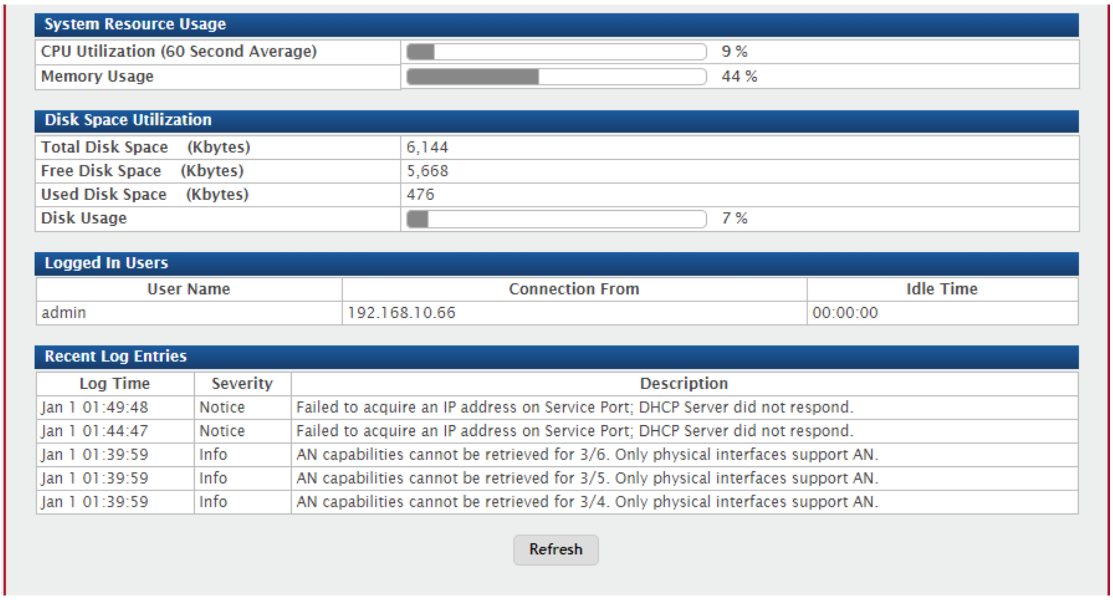
3.1.15.1 Dashboard

This page provides a brief overview of the system and serves as the home page upon successful login to the device.



System Information	
System Description	ORing IGS-R9164GP+ 16 GE+ 4 XE, 8.3.0.1, Linux 3.6.5
System Name	
System Location	
System Contact	
IP Address	192.168.10.1
Burned In MAC Address	00:1E:94:12:12:11
Service Port IP Address	0.0.0.0
Service Port MAC Address	00:1E:94:12:12:12
System Up Time	0 days, 1 hours, 50 mins, 53 secs

Device Information	
Machine Type	ORing IGS-R9164GP+ 16 GE+ 4 XE
Machine Model	IGS-R9164GP+
Serial Number	
FRU Number	
Maintenance Level	A
Software Version	8.3.0.1
Operating System	Linux 3.6.5



System Resource Usage	
CPU Utilization (60 Second Average)	9 %
Memory Usage	44 %

Disk Space Utilization	
Total Disk Space (Kbytes)	6,144
Free Disk Space (Kbytes)	5,668
Used Disk Space (Kbytes)	476
Disk Usage	7 %

Logged In Users

User Name	Connection From	Idle Time
admin	192.168.10.66	00:00:00

Recent Log Entries

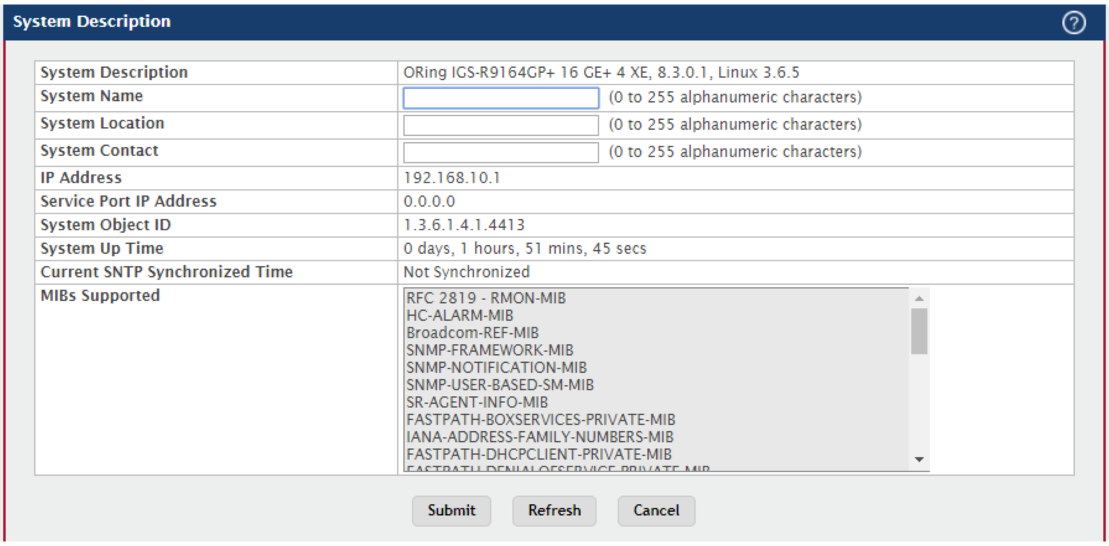
Log Time	Severity	Description
Jan 1 01:49:48	Notice	Failed to acquire an IP address on Service Port; DHCP Server did not respond.
Jan 1 01:44:47	Notice	Failed to acquire an IP address on Service Port; DHCP Server did not respond.
Jan 1 01:39:59	Info	AN capabilities cannot be retrieved for 3/6. Only physical interfaces support AN.
Jan 1 01:39:59	Info	AN capabilities cannot be retrieved for 3/5. Only physical interfaces support AN.
Jan 1 01:39:59	Info	AN capabilities cannot be retrieved for 3/4. Only physical interfaces support AN.

Field	Description
System Description	The product name of this device.
System Name	The configured name used to identify this device.
System Location	The configured location of this device.
System Contact	The configured contact person for this device.
IP Address	The IP address assigned to the network interface. The network

	interface is the logical interface that allows remote management of the device via any of the front-panel switch ports.
Burned In MAC Address	The device burned-in universally-administered media access control (MAC) address of the base system.
Service Port IP Address	The IP address assigned to the service port. The service port provides remote management access to the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.
Service Port MAC Address	The device burned-in universally-administered media access control (MAC) address of the service port.
System Up Time	The time in days, hours, minutes and seconds since the system was last reset.
Machine Type	The device hardware type or product family.
Machine Model	The model identifier, which is usually related to the Machine Type.
Serial Number	The unique device serial number.
FRU Number	The field replaceable unit number.
Maintenance Level	The device hardware change level identifier.
Software Version	The release.version.maintenance number of the software currently running on the device. For example, if the release is 1, the version is 2 and the maintenance number is 4, this version number is displayed as 1.2.4.
Operating System	The device operating system type and version identification information.
CPU Utilization (60 Second Average)	The percentage of CPU utilization for the entire system averaged over the past 60 seconds.
Memory Usage	The percentage of total available system memory (RAM) that is currently in use.
Disk Usage	The percentage of total available disk space that is currently in use.
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.

3.1.15.2 Description

Use the System Description page to view and configure basic information about the device. This page contains information that is useful for administrators who manage the device by using a Network Management System (NMS) that communicates with the Simple Network Manage Protocol (SNMP) agent on the device.



System Description

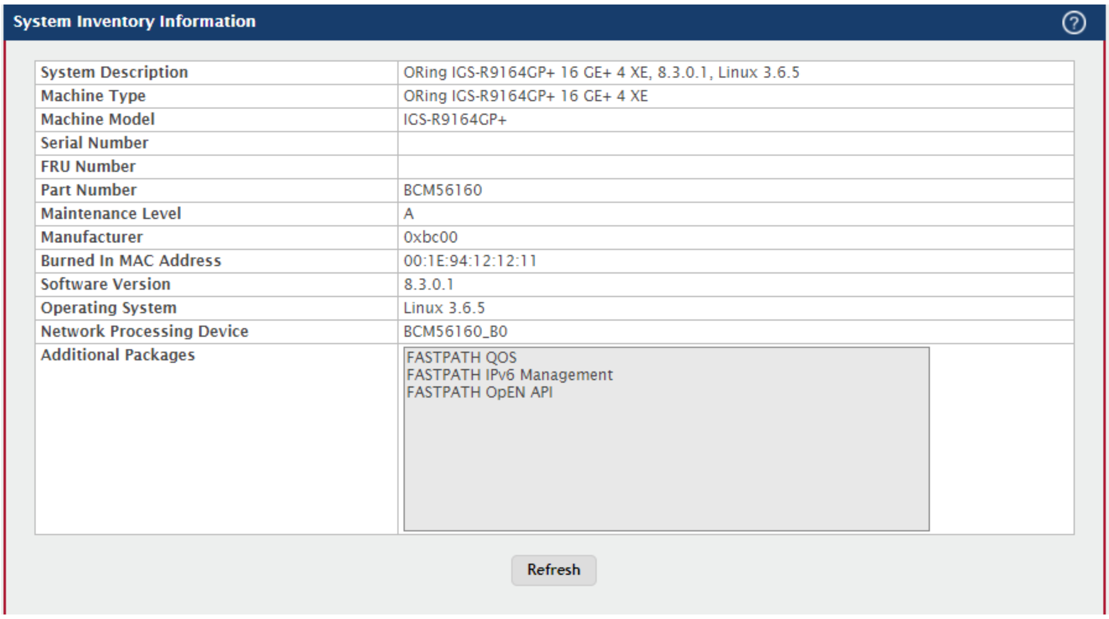
System Description	ORing IGS-R9164GP+ 16 GE+ 4 XE, 8.3.0.1, Linux 3.6.5
System Name	(0 to 255 alphanumeric characters)
System Location	(0 to 255 alphanumeric characters)
System Contact	(0 to 255 alphanumeric characters)
IP Address	192.168.10.1
Service Port IP Address	0.0.0.0
System Object ID	1.3.6.1.4.1.4413
System Up Time	0 days, 1 hours, 51 mins, 45 secs
Current SNTP Synchronized Time	Not Synchronized
MIBs Supported	RFC 2819 - RMON-MIB HC-ALARM-MIB Broadcom-REF-MIB SNMP-FRAMEWORK-MIB SNMP-NOTIFICATION-MIB SNMP-USER-BASED-SM-MIB SR-AGENT-INFO-MIB FASTPATH-BOXSERVICES-PRIVATE-MIB IANA-ADDRESS-FAMILY-NUMBERS-MIB FASTPATH-DHCPCLIENT-PRIVATE-MIB

Field	Description
System Description	The product name of this device.
System Name	The name used to identify this device. The factory default is blank.
System Location	The location of this device. The factory default is blank.
System Contact	The contact person for this device. The factory default is blank.
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.
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 device's enterprise MIB. This ID is used for SNMP-based management of the device.
System Up Time	The time in days, hours, minutes, and seconds since the last device reboot.
Current SNTP Synchronized	Displays the currently synchronized SNTP time in UTC. If the time is not synchronized with an SNTP server, it displays "Not

Time	Synchronized."
MIBs Supported	The list of MIBs supported by the SNMP agent running on this device.

3.1.15.3 Inventory

This page displays information about the system hardware and software.



System Inventory Information

System Description	ORing IGS-R9164GP+ 16 GE+ 4 XE, 8.3.0.1, Linux 3.6.5
Machine Type	ORing IGS-R9164GP+ 16 GE+ 4 XE
Machine Model	IGS-R9164GP+
Serial Number	
FRU Number	
Part Number	BCM56160
Maintenance Level	A
Manufacturer	0xbc00
Burned In MAC Address	00:1E:94:12:12:11
Software Version	8.3.0.1
Operating System	Linux 3.6.5
Network Processing Device	BCM56160_B0
Additional Packages	FASTPATH QOS FASTPATH IPv6 Management FASTPATH OpEN API

Field	Description
System Description	The product name of this device.
Machine Type	The hardware platform of this device.
Machine Model	The product model number.
Serial Number	The unique serial number used to identify the device.
FRU Number	The field replaceable unit number.
Part Number	The manufacturing part number.
Maintenance Level	The device hardware change level identifier.
Manufacturer	The two-octet code that identifies the manufacturer.
Burned In MAC Address	The device burned-in universally-administered media access control (MAC) address.
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 device.
Network Processing Device	Identifies the network processor hardware.

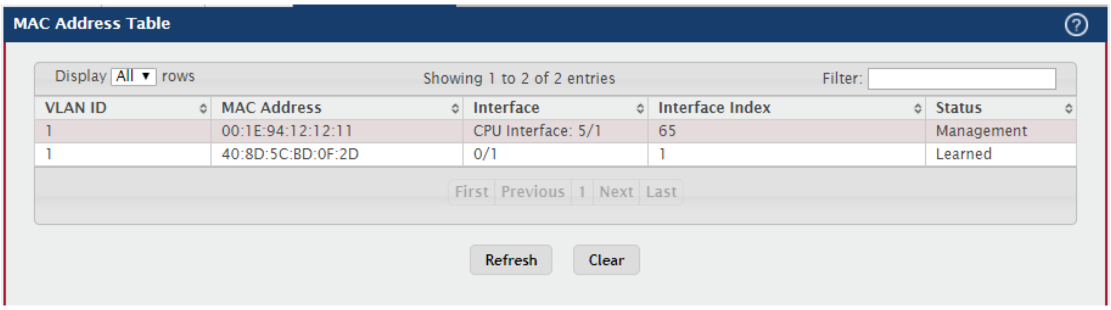
Additional Packages	A list of the optional software packages installed on the device, if any. For example, QoS.

3.1.15.4 MAC Address Table

The MAC address table keeps track of the Media Access Control (MAC) addresses that are associated with each port. This table allows the device to forward unicast traffic through the appropriate port. The MAC address table is sometimes called the bridge table or the forwarding database.

Use this page to display information about entries in the MAC address table. The transparent bridging function uses these entries to determine how to forward a received frame.

To remove dynamically learned FDB table entries, use the Clear button. The user is allowed to clear either all the learned entries at once, the entries for a specific interface or VLAN, or the range of entries that match the MAC address and mask combination.



MAC Address Table

Display All rows Showing 1 to 2 of 2 entries Filter:

VLAN ID	MAC Address	Interface	Interface Index	Status
1	00:1E:94:12:12:11	CPU Interface: 5/1	65	Management
1	40:8D:5C:BD:0F:2D	0/1	1	Learned

Field	Description
VLAN ID	The VLAN with which the MAC address is associated. A MAC address can be associated with multiple VLANs.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.
Interface	The port where this address was learned. The port identified in this field is the port through which the MAC address can be reached.
Interface Index	The Interface Index of the MIB interface table entry associated with the source port. This value helps identify an interface when using SNMP to manage the device.
Status	Provides information about the entry and why it is in the table, which can be one of the following: Static: The address has been manually configured and does not age

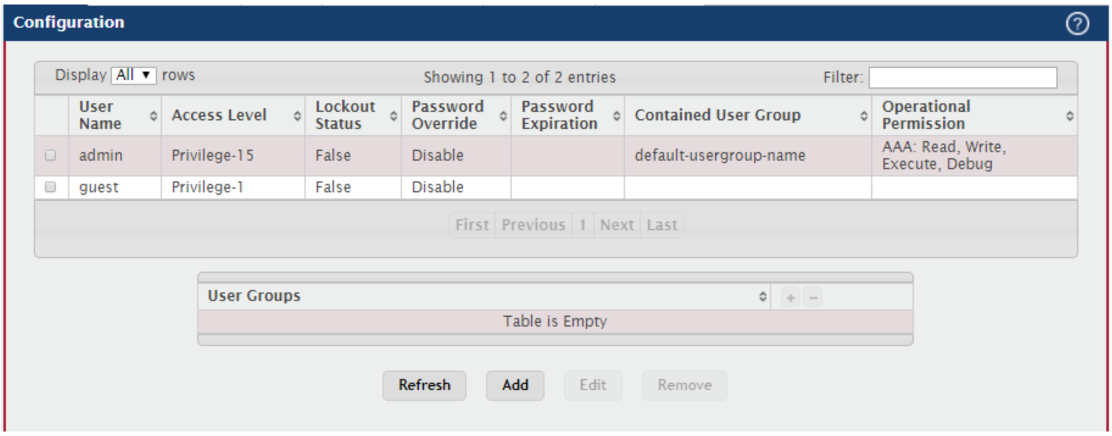
	out. Learned: The address has been automatically learned by the device and can age out when it is not in use. Dynamic addresses are learned by examining information in incoming Ethernet frames. Management: The burned-in MAC address of the device. Self: The MAC address belongs to one of the device's physical interfaces. GMRP Learned: The address was added dynamically by the GARP Multicast Registration Protocol (GMRP). Other: The address was added dynamically through an unidentified protocol or method. Unknown: The device is unable to determine the status of the entry.

3.1.16 Users

3.1.16.1 Accounts

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

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



Configuration

Display All rows   Showing 1 to 2 of 2 entries   Filter:

	User Name	Access Level	Lockout Status	Password Override	Password Expiration	Contained User Group	Operational Permission
□	admin	Privilege-15	False	Disable		default-usergroup-name	AAA: Read, Write, Execute, Debug
□	guest	Privilege-1	False	Disable			

User Groups
Table is Empty

Field	Description
User Name	A unique ID or name used to identify this user account.

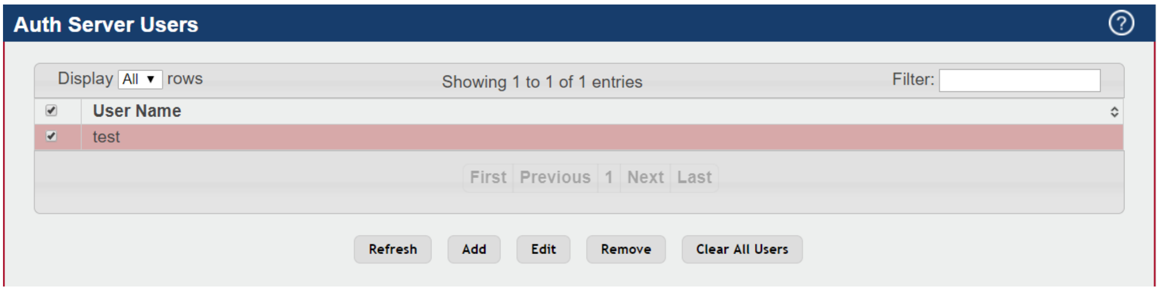
Access Level	The access or privilege level for this user. The options are: **Privilege-15** - The user can view and modify the configuration. **Privilege-1** - The user can view the configuration but cannot modify any fields. **Privilege-0** - The user exists but is not permitted to log on to the device.
Lockout Status	Provides the current lockout status for this user. If the lockout status is True, the user cannot access the management interface even if the correct username and password are provided. The user has been locked out of the system due to a failure to supply the correct password within the configured number of login attempts.
Password Override	Identifies the password override complexity status for this user. **Enable** - The system does not check the strength of the password. **Disable** - When configuring a password, it is checked against the Strength Check rules configured for passwords.
Password Expiration	Indicates the current expiration date (if any) of the password.
Contained User Group	The associated user groups for the user.
Operational Permission	The operational task permissions for the user. In addition to the fields described above, the User Groups table will be populated when you click on each row. To configure this user group, click the Add icon in the header row. To remove the user group, click the Reset icon in the row.
User Groups	The associated user group or groups for the user. In addition to the fields described above, the following fields are available when you click Add or Edit
Password	The password assigned to this user.
Confirm	Re-enter the password to confirm that you have entered it correctly.
Unlock User Account	Specifies the locked status of the user.
Password Strength	Shows the status of password strength check.
Encrypted Password	Specifies the password encryption.

3.1.16.2 Auth Sever User

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

Use the buttons to perform the following tasks:

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



Auth Server Users

Display All rows Showing 1 to 1 of 1 entries Filter:

☑	User Name
☑	test

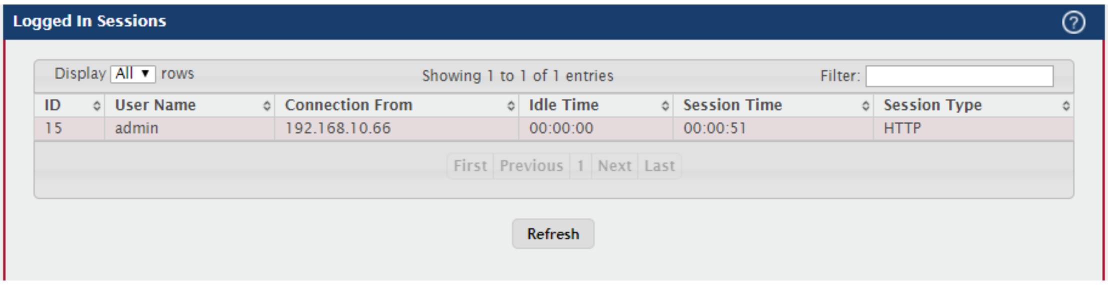
Field	Description
User Name	A unique name used to identify this user account. You configure the User Name when you add a new user.

When you add a new user or edit an existing user, a new window opens to allow you to configure the user information. In addition to the User Name field, the following fields are available on the modal page for adding and editing users.

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

3.1.16.3 Sessions

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

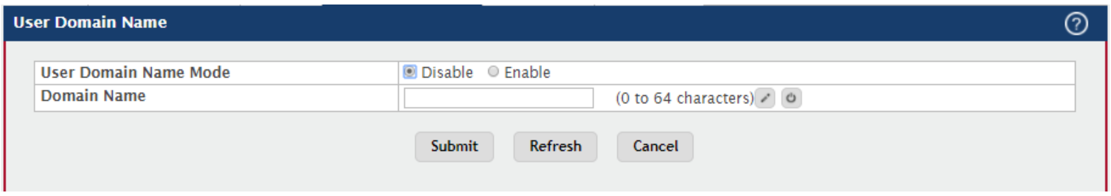


ID	User Name	Connection From	Idle Time	Session Time	Session Type
15	admin	192.168.10.66	00:00:00	00:00:51	HTTP

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

3.1.16.4 User Domain Name

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



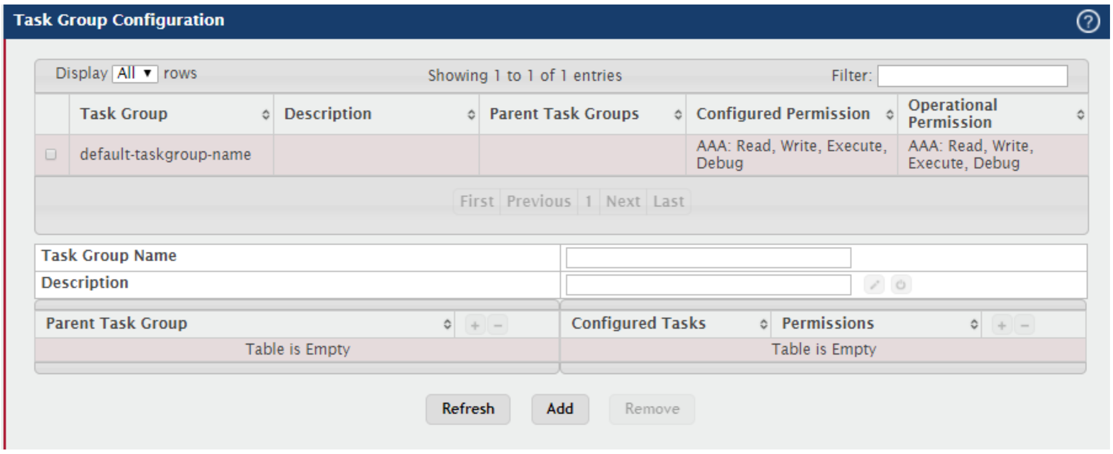
User Domain Name Mode	● Disable ○ Enable
Domain Name	(0 to 64 characters)

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

3.1.16.5 Task Groups

This page provides the capability to add, edit, and remove task groups.

- To add a task group, click **Add**. The **Add** new dialog box opens. Specify the new task group information in the available fields.
- To remove a task group, select one or more table entries and click **Remove** to delete the selected entries.



Task Group Configuration

Display All rows Showing 1 to 1 of 1 entries Filter:

	Task Group	Description	Parent Task Groups	Configured Permission	Operational Permission
□	default-taskgroup-name			AAA: Read, Write, Execute, Debug	AAA: Read, Write, Execute, Debug

First Previous 1 Next Last

Task Group Name	
Description	

Parent Task Group
Table is Empty

Configured Tasks	Permissions
Table is Empty	

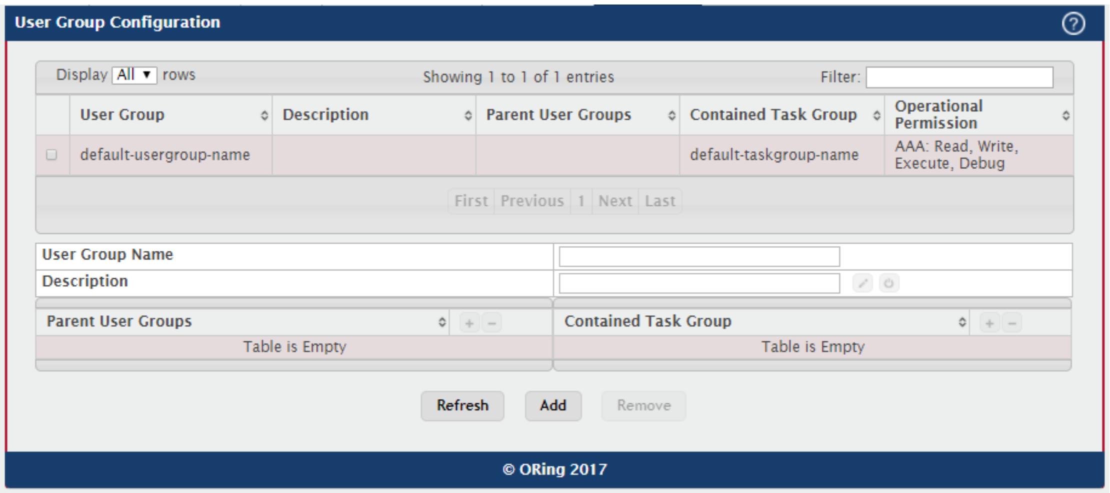
Field	Description
Task Group	The task group name.
Description	The associated description for task group name.

Parent Task Groups	The associated parent task groups for task group name. To configure this parent task group, click the Add icon in the header row. To remove the parent task group, click the Reset icon in the row.
Configured Permission	The configured task permissions for task group.
Operational Permission	The operational task permissions for task group.
Configured Tasks	The list of task names. To configure this task, click the Add icon in the header row. To remove the task, click the Reset icon in the row. AAA
Permissions	The task permissions. Read Write Debug Execute

3.1.16.6 User Group

This page provides the capability to add, edit, and remove user groups.

- To add a user group, click **Add**. The **Add** new dialog box opens. Specify the new user group information in the available fields.
- To remove a user group, select one or more table entries and click **Remove** to delete the selected entries.



User Group Configuration

Display All rows Showing 1 to 1 of 1 entries Filter:

	User Group	Description	Parent User Groups	Contained Task Group	Operational Permission
□	default-usergroup-name			default-taskgroup-name	AAA: Read, Write, Execute, Debug

User Group Name	
Description	

Parent User Groups
Table is Empty

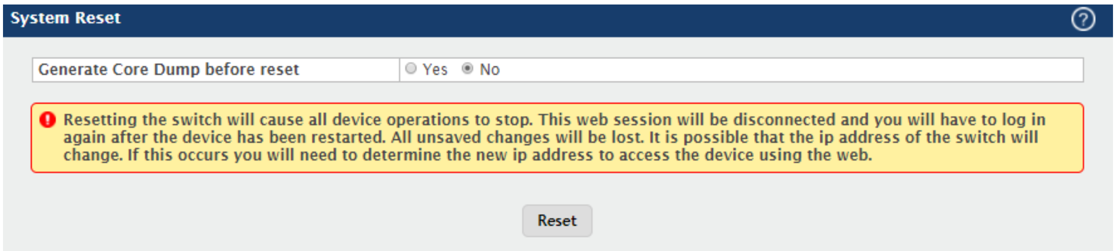
Contained Task Group
Table is Empty

Field	Description
User Group	The user group name.
Description	The associated description for user group name.
Parent User Groups	The associated parent user groups for user group. To configure this parent user group, click the Add icon in the header row. To remove the parent user group, click the Reset icon in the row.
Contained Task Group	The associated task groups for user group. To configure this task group, click the Add icon in the header row. To remove the task group, click the Reset icon in the row.
Operational Permission	The operational task permissions for user group.

3.1.17 Utilities

3.1.17.1 System Reset

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.



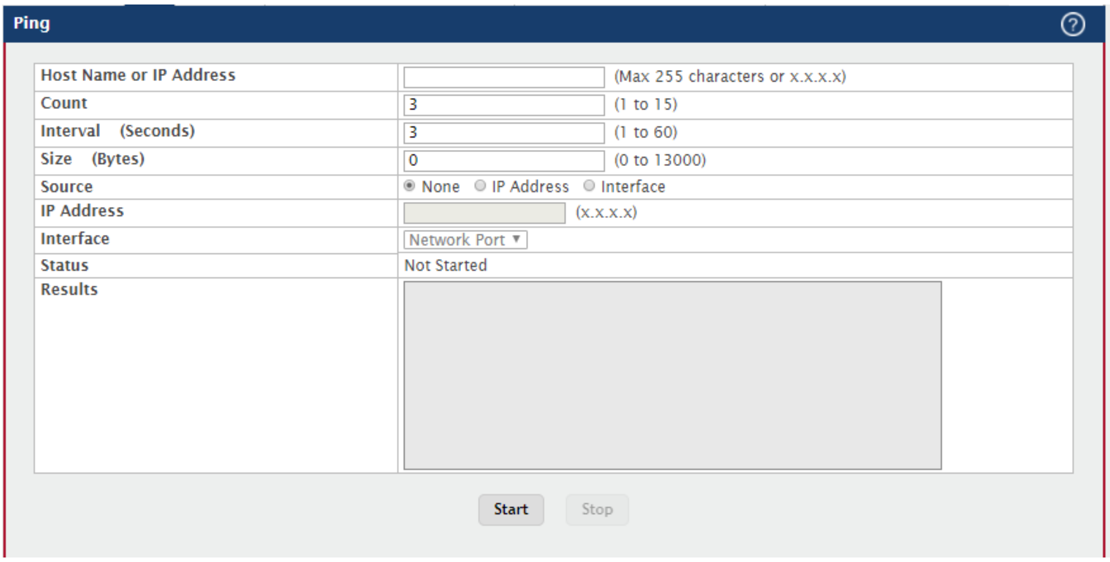
System Reset

Generate Core Dump before reset	○ Yes ● No

Resetting the switch will cause all device operations to stop. This web session will be disconnected and you will have to log in again after the device has been restarted. All unsaved changes will be lost. It is possible that the ip address of the switch will change. If this occurs you will need to determine the new ip address to access the device using the web.

3.1.17.2 Ping

Use this page to tell the device to send one or more ping requests to a specified host. You can use the ping request to check whether the device can communicate with a particular host on an IP network. A ping request is an Internet Control Message Protocol (ICMP) echo request packet. The information you enter on this page is not saved as part of the device configuration.



Ping

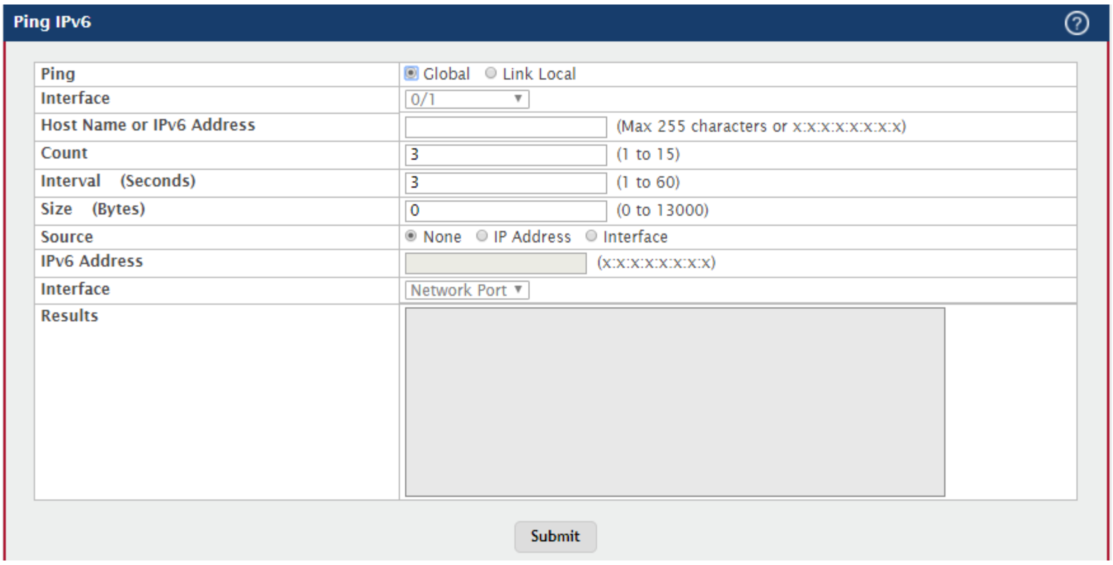
Host Name or IP Address		(Max 255 characters or x.x.x.x)
Count	3	(1 to 15)
Interval (Seconds)	3	(1 to 60)
Size (Bytes)	0	(0 to 13000)
Source	● None ○ IP Address ○ Interface	
IP Address		(x.x.x.x)
Interface	Network Port ▾	
Status	Not Started	
Results		

Field	Description
Host Name or IP Address	The DNS-resolvable hostname or IP address of the system to ping.
Count	Enter the number of ICMP echo request packets to send to the host.
Interval	Enter the number of seconds to wait between sending ping packets.
Size	The size of the ping packet, in bytes. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes, such as large or very large packets.
Source	The source IP address or interface to use when sending the echo request packets. If source is not required, select None as source option.
IP Address	The source IP address to use when sending the Echo requests packets. This field is enabled when IP Address is selected as source option.
Interface	The interface to use when sending the Echo requests packets. This field is enabled when Interface is selected as source option.
Status	The current status of the ping test, which can be: Not Started – The ping test has not been initiated since viewing the page. In Progress – The ping test has been initiated and is running. Stopped – The ping test was interrupted by clicking the Stop button. Done – The test has completed, and information about the test is displayed in the Results area.
Results	The results of the ping test, which includes information about the reply

	(if any) received from the host.
Start (Button)	Starts the ping test. The device sends the specified number of ping packets to the host.
Stop (Button)	Interrupts the current ping test.

3.1.17.3 Ping IPv6

Use this page to tell the device to send one or more ping requests to a specified IPv6 host. You can use the ping request to check whether the device can communicate with a particular host on an IPv6 network. A ping request is an Internet Control Message Protocol version 6 (ICMPv6) echo request packet. The information you enter on this page is not saved as part of the device configuration.



Ping IPv6

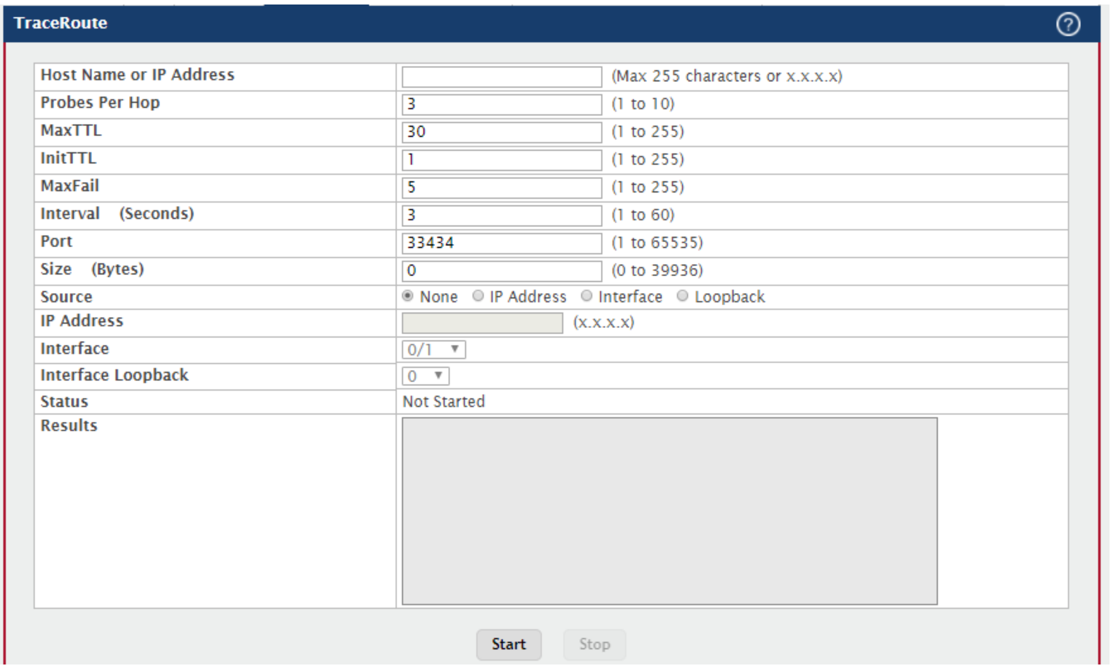
Ping	● Global ○ Link Local
Interface	0/1 ▼
Host Name or IPv6 Address	(Max 255 characters or x:x:x:x:x:x:x:x)
Count	3 (1 to 15)
Interval (Seconds)	3 (1 to 60)
Size (Bytes)	0 (0 to 13000)
Source	● None ○ IP Address ○ Interface
IPv6 Address	(x:x:x:x:x:x:x:x)
Interface	Network Port ▼
Results	

Field	Description
Ping	Select either a global IPv6 address or a link local address to ping. A global address is routable over the Internet, while a link-local address is intended for communication only within the local network. Link local addresses have a prefix of fe80::/64.
Interface	Select the interface on which to issue the Link Local ping request.
Host Name or IPv6 Address	Enter the global or link-local IPv6 address, or the DNS-resolvable host name of the station to ping. If the ping type is Link Local, you must enter a link-local address and cannot enter a host name.
Count	Enter the number of ICMP echo request packets to send to the host.
Interval	Enter the number of seconds to wait between sending ping packets.
Size	The size of the ping packet, in bytes. Changing the size allows you to

	troubleshoot connectivity issues with a variety of packet sizes, such as large or very large packets.
Source	The source IP address or interface to use when sending the echo request packets. If source is not required, select None as source option.
IPv6 Address	The source IPv6 address to use when sending the Echo requests packets. This field is enabled when IP Address is selected as source option.
Interface	The interface to use when sending the Echo requests packets. This field is enabled when Interface is selected as source option.
Results	The results of the ping test, which includes information about the reply (if any) received from the host.

3.1.17.4 Trace Route

Use this page to determine the layer 3 path a packet takes from the device to a specific IP address or hostname. When you initiate the TraceRoute command by clicking the Start button, the device sends a series of TraceRoute probes toward the destination. The results list the IP address of each layer 3 device a probe passes through until it reaches its destination - or fails to reach its destination and is discarded. The information you enter on this page is not saved as part of the device configuration.



TraceRoute

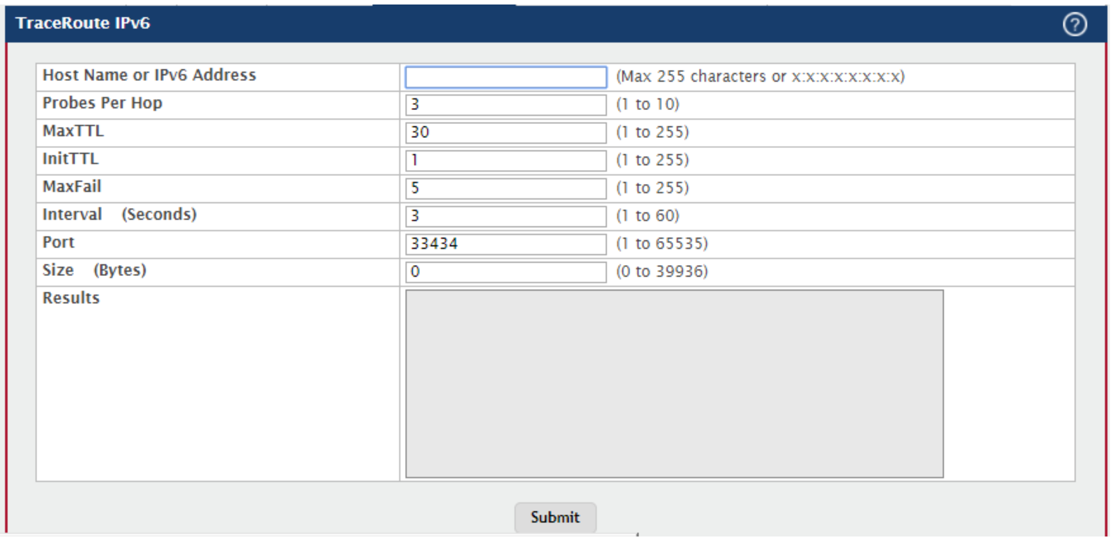
Host Name or IP Address		(Max 255 characters or x.x.x.x)
Probes Per Hop	3	(1 to 10)
MaxTTL	30	(1 to 255)
InitTTL	1	(1 to 255)
MaxFail	5	(1 to 255)
Interval (Seconds)	3	(1 to 60)
Port	33434	(1 to 65535)
Size (Bytes)	0	(0 to 39936)
Source	● None ○ IP Address ○ Interface ○ Loopback	
IP Address		(x.x.x.x)
Interface	0/1 ▼	
Interface Loopback	0 ▼	
Status	Not Started	
Results		

Field	Description
Host Name or IP Address	The DNS-resolvable hostname or IP address of the system to attempt to reach.
Probes Per Hop	TraceRoute works by sending UDP packets with increasing Time-To-Live (TTL) values. Specify the number of probes sent with each TTL.
MaxTTL	The maximum Time-To-Live (TTL). The TraceRoute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the TraceRoute will not reach it.
InitTTL	The initial Time-To-Live (TTL). This value controls the maximum number of layer 3 hops that the first set of probes may travel.
MaxFail	The number of consecutive failures that terminate the TraceRoute. If the device fails to receive a response for this number of consecutive probes, the TraceRoute terminates.
Interval	The number of Seconds to wait between sending probes.
Port	The UDP destination port number to be used in probe packets. The port number should be a port that the target host is not listening on, so that when the probe reaches the destination, it responds with an ICMP Port Unreachable message.
Size	The size of probe payload in bytes.
Status	The current status of the TraceRoute, which can be: Not Started – The TraceRoute has not been initiated since viewing the page. In Progress – The TraceRoute has been initiated and is running. Stopped – The TraceRoute was interrupted by clicking the Stop button. Done – The TraceRoute has completed, and information about the TraceRoute is displayed in the Results area.
Results	The results of the TraceRoute, which are displayed in the following format: 1 10.20.24.1 0 ms 0 ms 0 ms 2 66.20.17.9 10 ms 0 ms 10 ms 3 66.20.246.82 10 ms 20 ms 10 ms 4 129.20.4.4 20 ms 10 ms 40 ms 5 129.20.3.55 80 ms 80 ms 90 ms 6 129.20.5.246 80 ms 80 ms 80 ms

	7 198.20.90.26 70 ms 70 ms 70 ms 8 216.20.255.105 90 ms 70 ms 80 ms 9 63.20.216.155 80 ms 80 ms 90 ms Hop Count = 9 Last TTL = 9 Test attempt = 27 Test Success = 27 For each TTL value probed, the results show the IP address of the router that responded to the probes and the response time for each probe. If no response is received for probes with a particular TTL, the IP address is reported as 0.0.0.0. An error code may be printed with the response time for each probe. The error codes signify that either no response was received or an ICMP Destination Unreachable message was received with error codes as follows: * no response was received to the probe P - Protocol unreachable (RFC 792) N - Network unreachable (RFC 792) H - Host unreachable (RFC 792) F - Fragmentation needed and DF set (RFC 792) S - Source route failed (RFC 792) A - Communication with Destination Network is Administratively Prohibited (RFC 1122) C - Communication with Destination Host is Administratively Prohibited (RFC 1122) The Hop Count is the number of sets of probes sent, each set of probes having a particular TTL. The Last TTL is the TTL sent in the final set of probes. The Test Attempt value shows the number of probes sent. The Test Success value shows the number of probes that received a response.
Start (Button)	Initiates the TraceRoute.
Stop (Button)	Interrupts the running TraceRoute.

3.1.17.5 Trace Route IPv6

Use this page to determine the layer 3 path a packet takes from the device to a specific IP address or hostname. When you initiate the IPv6 TraceRoute command by clicking the Submit button, the device sends a series of IPv6 TraceRoute probes toward the destination. The results list the IP address of each layer 3 device a probe passes through until it reaches its destination - or fails to reach its destination and is discarded. The information you enter on this page is not saved as part of the device configuration.



TraceRoute IPv6

Host Name or IPv6 Address		(Max 255 characters or x:x:x:x:x:x:x:x)
Probes Per Hop	3	(1 to 10)
MaxTTL	30	(1 to 255)
InitTTL	1	(1 to 255)
MaxFail	5	(1 to 255)
Interval (Seconds)	3	(1 to 60)
Port	33434	(1 to 65535)
Size (Bytes)	0	(0 to 39936)
Results		

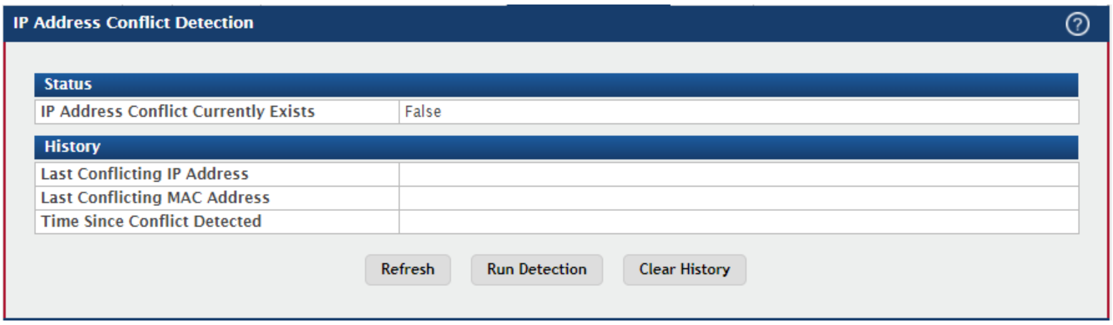
Field	Description
Host Name or IPv6 Address	The DNS-resolvable hostname or IPv6 address of the system to attempt to reach.
Probes Per Hop	IPv6 TraceRoute works by sending UDP packets with increasing Time-To-Live (TTL) values. Specify the number of probes sent with each TTL.
MaxTTL	The maximum Time-To-Live (TTL). The TraceRoute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the TraceRoute will not reach it.
InitTTL	The initial Time-To-Live (TTL). This value controls the maximum number of layer 3 hops that the first set of probes may travel.
MaxFail	The number of consecutive failures that terminate the TraceRoute. If the device fails to receive a response for this number of consecutive probes, the TraceRoute terminates.
Interval	The number of Seconds to wait between sending probes.
Port	The UDP destination port number to be used in probe packets. The port number should be a port that the target host is not listening on, so that when the probe reaches the destination, it responds with an

	ICMPv6 Port Unreachable message.
Size	The size of probe payload in bytes.
Source	The source IP address or interface to use when sending the trace route command. If source is not required, select None as source option.
IPv6 Address	The source IPv6 address to use when sending the the trace route command. This field is enabled when IP Address is selected as source option.
Interface	The interface to use when sending the trace route command. This field is enabled when Interface is selected as source option.
Results	The results of the TraceRoute, which are displayed in the following format: 1 3001::1 708 ms 41 ms 11 ms 2 4001::2 250 ms 200 ms 193 ms 3 5001::3 289 ms 313 ms 278 ms 4 6001::4 651 ms 41 ms 270 ms 5 :: * N * N * N Hop Count = 4 Last TTL = 5 Test attempt = 1 Test Success = 0 For each TTL value probed, the results show the IP address of the router that responded to the probes and the response time for each probe. If no response is received for probes with a particular TTL, the IP address is reported as 0.0.0.0. An error code may be printed with the response time for each probe. The error codes signify that either no response was received or an ICMP Destination Unreachable message was received with error codes as follows: * no response was received to the probe P - Protocol unreachable (RFC 792) N - Network unreachable (RFC 792) H - Host unreachable (RFC 792) F - Fragmentation needed and DF set (RFC 792) S - Source route failed (RFC 792) A - Communication with Destination Network is Administratively

	Prohibited (RFC 1122) C - Communication with Destination Host is Administratively Prohibited (RFC 1122) The Hop Count is the number of sets of probes sent, each set of probes having a particular TTL. The Last TTL is the TTL sent in the final set of probes. The Test Attempt value shows the number of probes sent. The Test Success value shows the number of probes that received a response.

3.1.17.6 IP Address Conflict

Use this page to determine whether the IP address configured on the device is the same as the IP address of another device on the same LAN (or on the Internet, for a routable IP address) and to help you resolve any existing conflicts. An IP address conflict can make both this system and the system with the same IP address unusable for network operation.



IP Address Conflict Detection

Status

IP Address Conflict Currently Exists	False

History

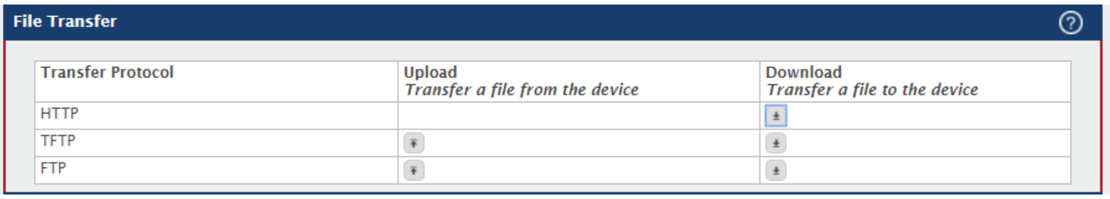
Last Conflicting IP Address	
Last Conflicting MAC Address	
Time Since Conflict Detected	

Field	Description
IP Address Conflict Currently Exists	Indicates whether a conflicting IP address has been detected since this status was last reset. False – No conflict detected (the subsequent fields on this page display as N/A). True – Conflict was detected (the subsequent fields on this page show the relevant information).
Last Conflicting IP Address	The device interface IP address that is in conflict. If multiple conflicts were detected, only the most recent occurrence is displayed.
Last Conflicting MAC Address	The MAC address of the remote host associated with the IP address that is in conflict. If multiple conflicts are detected, only the most recent occurrence is displayed.
Time Since Conflict Detected	The elapsed time (displayed in days, hours, minutes, and seconds) since the last address conflict was detected, provided the Clear History button has not yet been pressed.

Run Detection (Button)	Activates the IP address conflict detection operation in the system.
Clear History (Button)	Resets the IP address conflict detection status information that was last seen by the device.

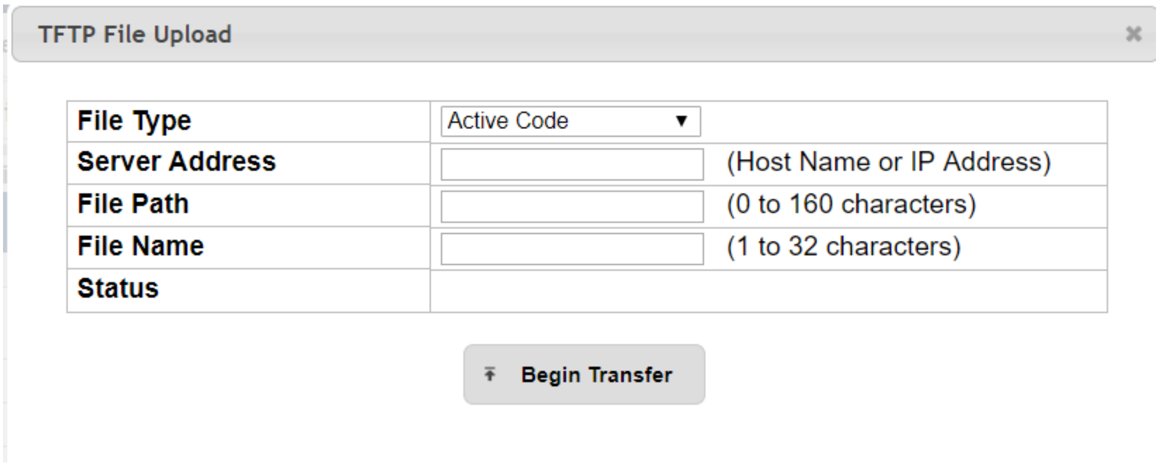
3.1.17.7 Transfer

Use this page to upload files from the device to a remote system and to download files from a remote system to the device.



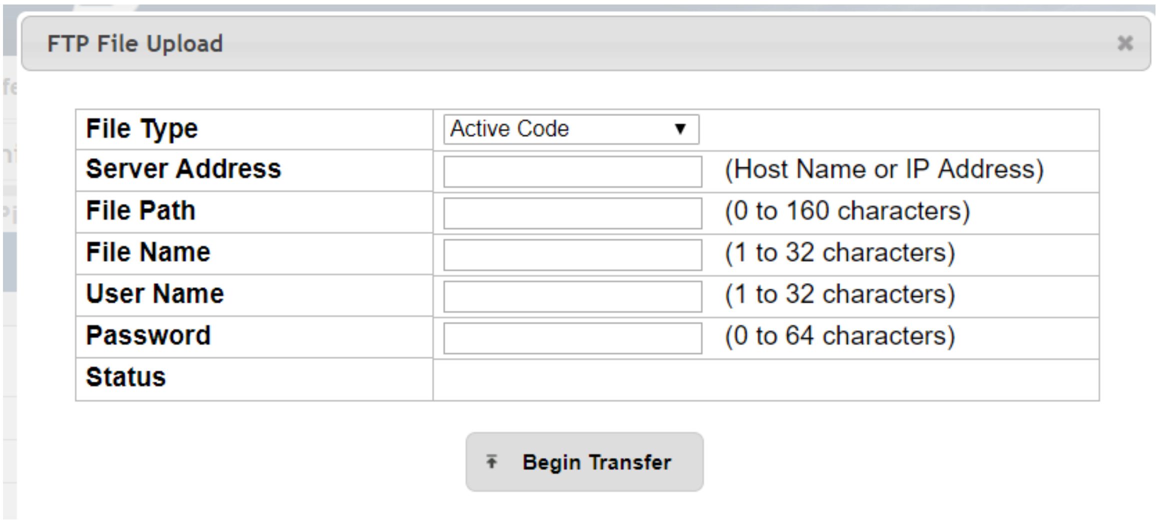
File Transfer

Transfer Protocol	Upload *Transfer a file from the device*	Download *Transfer a file to the device*
HTTP		↓
TFTP	↑	↓
FTP	↑	↓



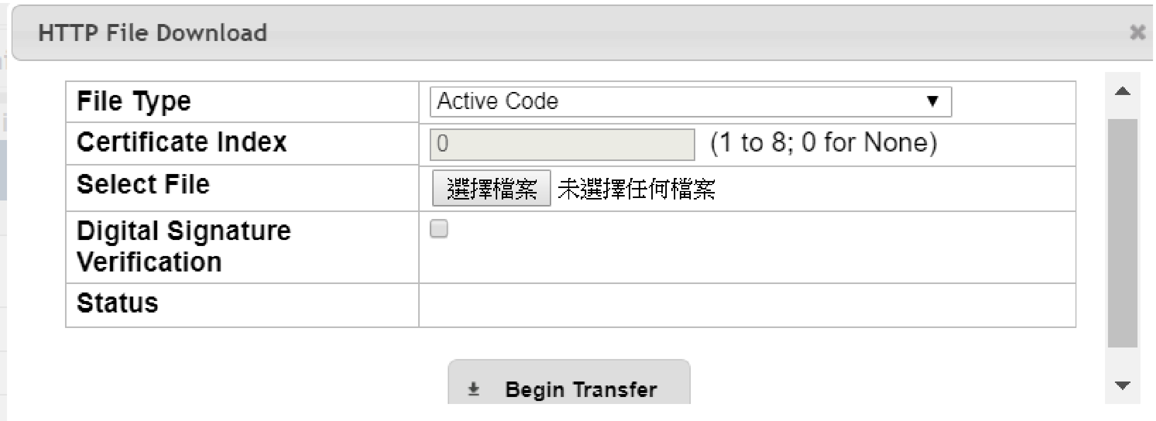
TFTP File Upload

File Type	Active Code ▼	
Server Address		(Host Name or IP Address)
File Path		(0 to 160 characters)
File Name		(1 to 32 characters)
Status		



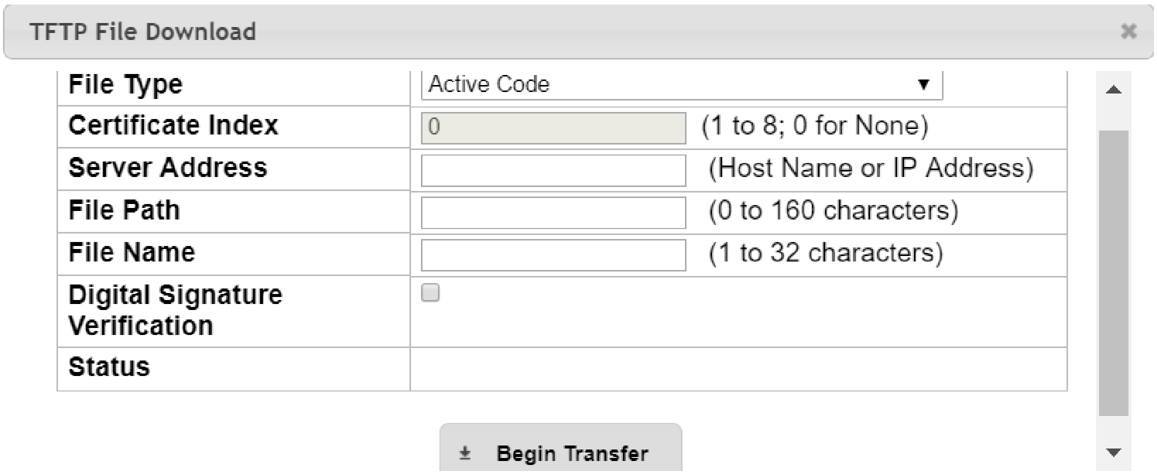
FTP File Upload

File Type	Active Code ▼	
Server Address		(Host Name or IP Address)
File Path		(0 to 160 characters)
File Name		(1 to 32 characters)
User Name		(1 to 32 characters)
Password		(0 to 64 characters)
Status		



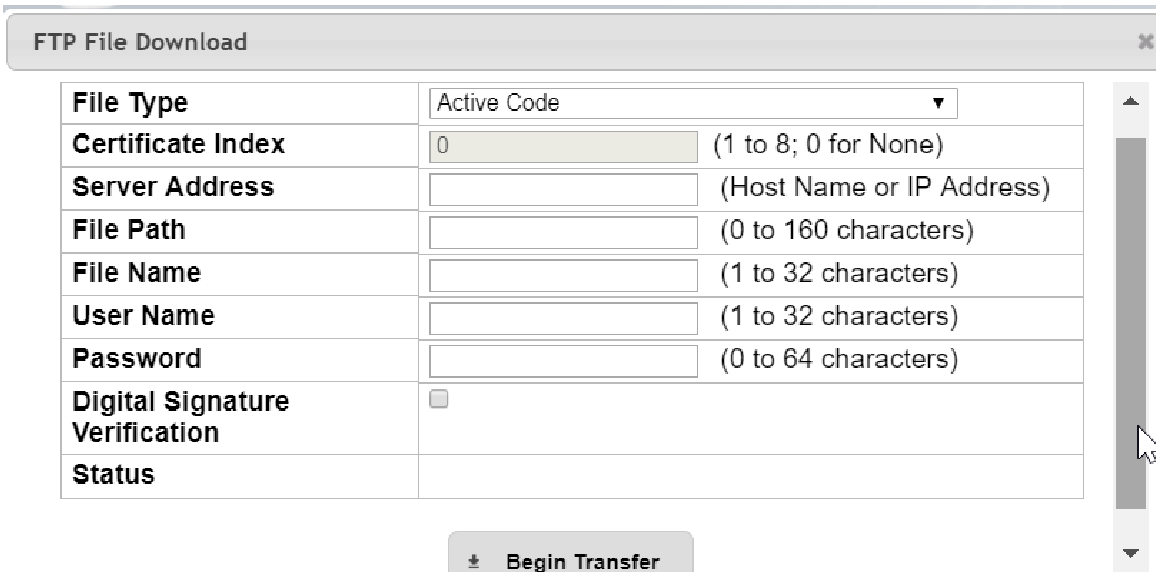
HTTP File Download

File Type	Active Code ▼
Certificate Index	0 (1 to 8; 0 for None)
Select File	選擇檔案 未選擇任何檔案
Digital Signature Verification	□
Status	



TFTP File Download

File Type	Active Code ▼
Certificate Index	0 (1 to 8; 0 for None)
Server Address	(Host Name or IP Address)
File Path	(0 to 160 characters)
File Name	(1 to 32 characters)
Digital Signature Verification	□
Status	



FTP File Download

File Type	Active Code ▼
Certificate Index	0 (1 to 8; 0 for None)
Server Address	(Host Name or IP Address)
File Path	(0 to 160 characters)
File Name	(1 to 32 characters)
User Name	(1 to 32 characters)
Password	(0 to 64 characters)
Digital Signature Verification	□
Status	

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, or FTP. Files can be transferred from a remote system to the device using HTTP, TFTP, or FTP.
Upload	To transfer a file from the device to a remote system using TFTP, or FTP, 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, or FTP, 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. The following information describes the fields in the File Upload window for all protocols.

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 an backup image. Startup Configuration – Select this option to transfer a copy of the stored startup configuration from the device to a remote system. Backup Configuration – Select this option to transfer a copy of the stored backup configuration from the device to a remote system. Script File – Select this option to transfer a custom text configuration script from the device to a remote system. CLI Banner – Select this option to transfer the file containing the text to be displayed on the CLI before the login prompt to a remote system. Crash Log – Select this option to transfer the system crash log to a remote system. Operational Log – Select this option to transfer the system operational log to a remote system. Startup Log – Select this option to transfer the system startup log to a remote system.

	Trap Log – Select this option to transfer the system trap records to a remote system. Factory Defaults – Select this option to transfer the factory default configuration file 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, IPv6 address, or DNS-resolvable hostname of the remote server that will receive the file.
File Path	Specify the path on the server where you want to put the file.
File Name	Specify the name that the file will have on the remote server.
User Name	For and FTP transfers, if the server requires authentication, specify the user name for remote login to the server that will receive the file.
Password	For and FTP 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. The following information describes the fields in the File Download window for all protocols.

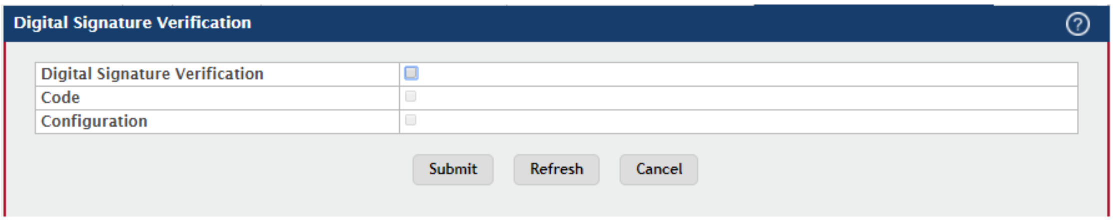
Field	Description
File Type	Specify the type of file to transfer to the device: Active Code – Select this option to transfer a new image to the device. The code file is stored as the active image. Backup Code – Select this option to transfer a new image to the device. The code file is stored as the backup image. Startup Configuration – Select this option to update the stored startup configuration file. If the file has errors, the update will be stopped. Backup Configuration – Select this option to update the stored backup configuration file. If the file has errors, the update will be stopped. Script File – Select this option to transfer a text-based configuration script to the device. You must use the command-line interface (CLI) to

	validate and activate the script. CLI Banner – Select this option to transfer the CLI banner file to the device. This file contains the text to be displayed on the CLI before the login prompt. IAS Users – Select this option to transfer an Internal Authentication Server (IAS) users database file to the device. The IAS user database stores a list of user name and (optional) password values for local port-based user authentication. SSH-1 RSA Key File – Select this option to transfer an SSH-1 Rivest-Shamir-Adleman (RSA) key file to the device. SSH key files contain information to authenticate SSH sessions for remote CLI-based access to the device. SSH-2 RSA Key PEM File – Select this option to transfer an SSH-2 Rivest-Shamir-Adleman (RSA) key file (PEM Encoded) to the device. SSH-2 DSA Key PEM File – Select this option to transfer an SSH-2 Digital Signature Algorithm (DSA) key file (PEM Encoded) to the device. 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. SSL Trusted Root Certificate PEM File – Select this option to transfer an SSL Trusted Root Certificate file (PEM Encoded) to the device. SSL files contain information to encrypt, authenticate, and validate HTTPS sessions. SSL Server Certificate PEM File – Select this option to transfer an SSL Server Certificate file (PEM Encoded) to the device. SSL DH Weak Encryption Parameter PEM File – Select this option to transfer an SSL Diffie-Hellman Weak Encryption Parameter file (PEM Encoded) to the device.

	SSL DH Strong Encryption Parameter PEM File – Select this option to transfer an SSL Diffie-Hellman Strong Encryption Parameter file (PEM Encoded) to the device. Public Key Image – Select this option to transfer the public key file used for code image validation to the device. Public Key Config – Select this option to transfer the public key file used for configuration script validation to the device. Note: To download SSH key files, SSH must be administratively disabled, and there can be no active SSH sessions. To download SSL related files, HTTPS must be administratively disabled
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.
Server Address	For TFTP, or FTP transfers, specify the IPv4 address, IPv6 address, or DNS-resolvable hostname of the remote server.
File Path	For TFTP, or FTP transfers, specify the path on the server where the file is located.
File Name	For TFTP, or FTP transfers, specify the name of the file you want to transfer to the device.
User Name	For FTP transfers, if the server requires authentication, specify the user name for remote login to the server where the file resides.
Password	For FTP 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.

3.1.17.8 Digital Signature Verfication

Use this page to configure digital signature verification on downloading files from a remote system to the device.



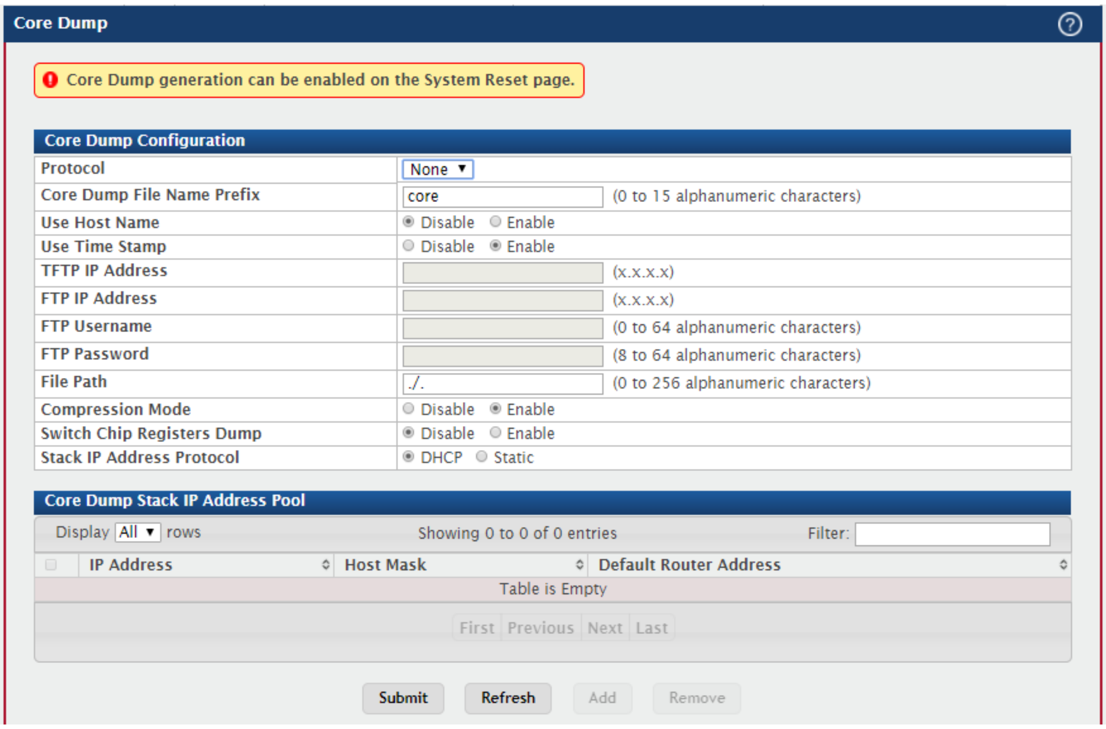
Digital Signature Verification

Digital Signature Verification	☐
Code	☐
Configuration	☐

Field	Description
Digital Signature Verification	Provides option to verify the digital signature of a downloaded file.
Code	Verify the digital signature of downloaded code image files.
Configuration	Verify the digital signature of downloaded configuration script files.

3.1.17.9 Core Dump

Use this page to configure Core Dump feature.



Core Dump

Core Dump generation can be enabled on the System Reset page.

Core Dump Configuration

Protocol	None ▾
Core Dump File Name Prefix	core (0 to 15 alphanumeric characters)
Use Host Name	● Disable ○ Enable
Use Time Stamp	○ Disable ● Enable
TFTP IP Address	(x.x.x.x)
FTP IP Address	(x.x.x.x)
FTP Username	(0 to 64 alphanumeric characters)
FTP Password	(8 to 64 alphanumeric characters)
File Path	./ (0 to 256 alphanumeric characters)
Compression Mode	○ Disable ● Enable
Switch Chip Registers Dump	● Disable ○ Enable
Stack IP Address Protocol	● DHCP ○ Static

Core Dump Stack IP Address Pool

Display All ▾ rows Showing 0 to 0 of 0 entries Filter:

☐	IP Address	Host Mask	Default Router Address
Table is Empty			

Field	Description
Core Dump Configuration	
Protocol	The protocol used to store the core dump file. User can select one of the options to configure:

	None - Disable Core Dump. TFTP - Configure protocol to upload Core Dump to the TFTP server. NFS - Configure protocol to upload Core Dump to the NFS share. Local - Configure protocol to generate Core Dump on switch local file system. 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 then 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.
Core Dump Stack IP Address Pool	
IP Address	Static IP address to be assigned to individual units 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.

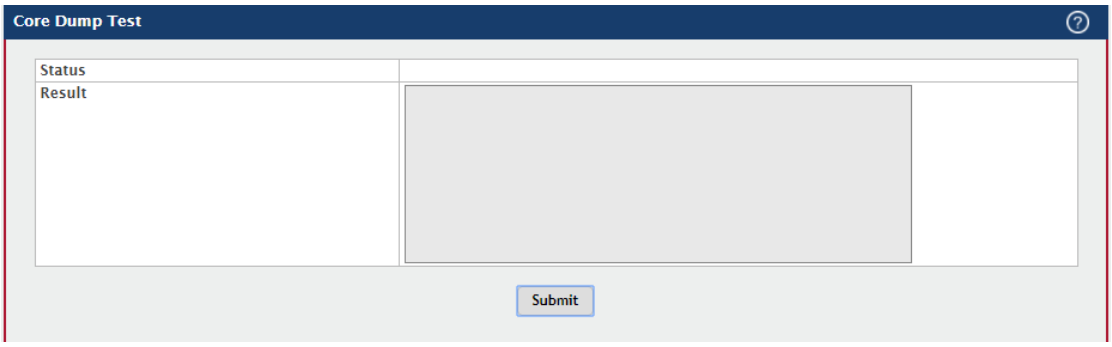
Use the buttons to perform the following tasks:

To add a stack IP address, click Add and configure an IP address, netmask and gateway address.

To delete a configured stack IP address, select each entry to delete, click Remove, and confirm the action.

3.1.17.10 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 TFTP server and informs user if the TFTP server can be contacted.



Core Dump Test

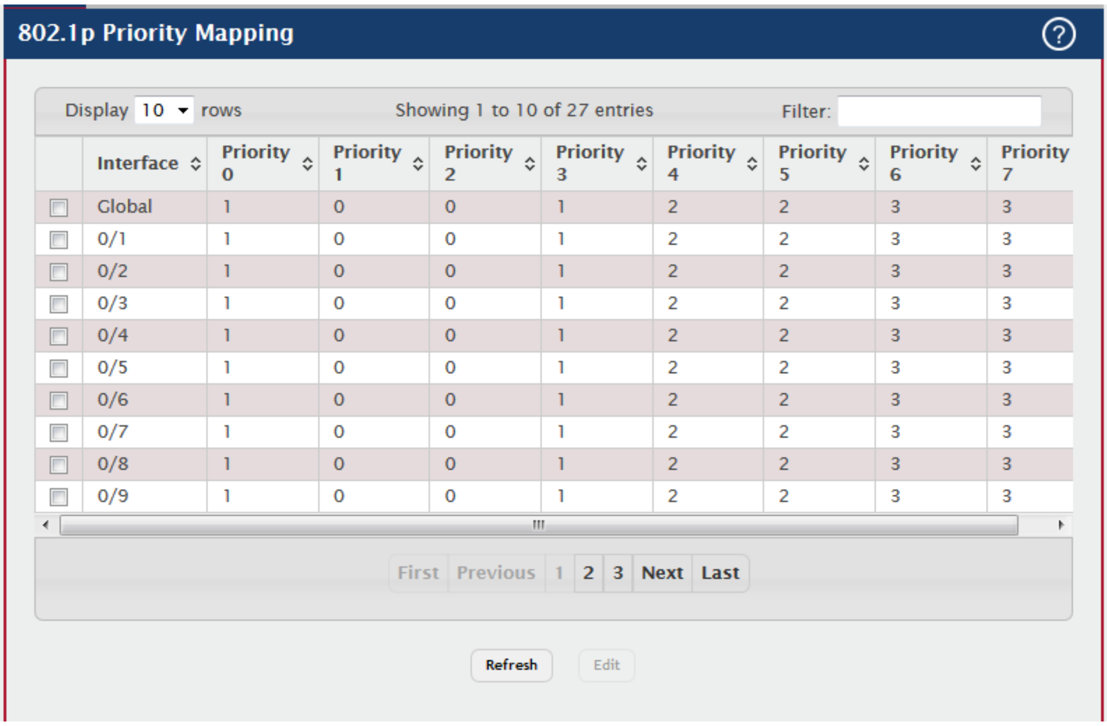
Field	Description
Status	Displays test status as Ok if test passes and Error if test fails.
Result	Displays detailed error information with logs.

4.1 Switching

4.1.1 Class of Service

4.1.1.1 802.1p

Use this page to view or change which internal traffic classes are mapped to the 802.1p priority class values in Ethernet frames the device receives. The priority-to-traffic class mappings can be applied globally or per-interface. The mapping allows the device to group various traffic types (e.g. data or voice) based on their latency requirements and give preference to time-sensitive traffic.



802.1p Priority Mapping

Display 10 rows Showing 1 to 10 of 27 entries Filter:

	Interface	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7
□	Global	1	0	0	1	2	2	3	3
□	0/1	1	0	0	1	2	2	3	3
□	0/2	1	0	0	1	2	2	3	3
□	0/3	1	0	0	1	2	2	3	3
□	0/4	1	0	0	1	2	2	3	3
□	0/5	1	0	0	1	2	2	3	3
□	0/6	1	0	0	1	2	2	3	3
□	0/7	1	0	0	1	2	2	3	3
□	0/8	1	0	0	1	2	2	3	3
□	0/9	1	0	0	1	2	2	3	3

Field	Description
Interface	The interface associated with the rest of the data in the row. The Global entry represents the common settings for all interfaces, unless specifically overridden individually.
Priority	The heading row lists each 802.1p priority value (0–7), and the data in the table shows which traffic class is mapped to the priority value. Incoming frames containing the designated 802.1p priority value are mapped to the corresponding traffic class in the device.

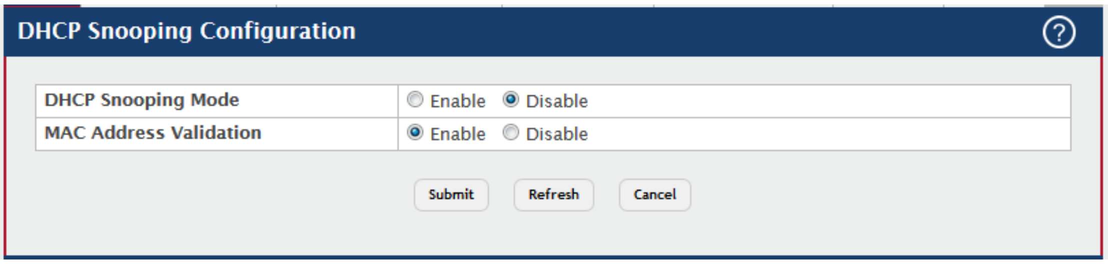
To change the traffic class mappings either globally or for an interface, select the entry to change and click Edit. Modifications to the Global entry apply the same traffic class mappings to all interfaces. The Edit 802.1p Priority Mapping window includes the following fields:

Field	Description
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.

4.1.2 DHCP Snooping

4.1.2.1 Base-Gload

Use this page to view and configure the global settings for DHCP Snooping. DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized. You can enable DHCP snooping globally and on specific VLANs, and configure ports within the VLAN to be trusted or untrusted. If a DHCP message arrives on an untrusted port, DHCP snooping filters messages that are not from authorized DHCP clients. DHCP server messages are forwarded only through trusted ports.



DHCP Snooping Configuration

DHCP Snooping Mode	○ Enable ● Disable
MAC Address Validation	● Enable ○ Disable

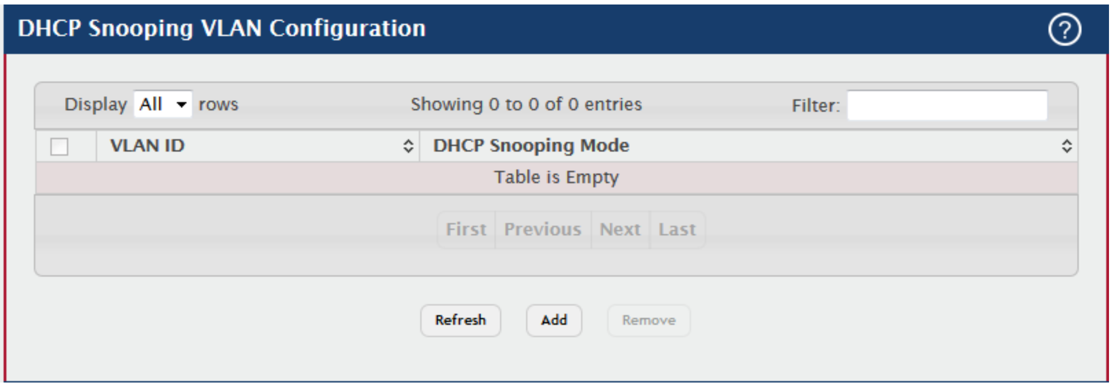
Field	Description
DHCP Snooping Mode	The administrative mode of DHCP snooping on the device.
MAC Address Validation	Enables or Disables the verification of the sender MAC address for DHCP snooping. When enabled, the device checks packets that are received on untrusted interfaces to verify that the MAC address and the DHCP client hardware address match. If the addresses do not match, the device drops the packet.

4.1.2.2 Base-VLAN Configuration

Use this page to view and configure the DHCP snooping settings on VLANs that exist on the device. DHCP snooping can be configured on switching VLANs and routing VLANs. For Layer 2 (non-routing) VLANs, DHCP snooping forwards valid DHCP client messages received on the VLANs. The message is forwarded on all trusted interfaces in the VLAN. When a DHCP packet is received on a routing VLAN, the DHCP snooping application applies its filtering rules and updates the bindings database. If a client message passes filtering rules, the message is placed into the software forwarding path, where it may be processed by the DHCP relay agent, the local DHCP server, or forwarded as an IP packet.

Use the buttons to perform the following tasks:

- To enable a VLAN for DHCP snooping, click **Add** and select the VLAN to administratively enable for DHCP snooping. To select multiple VLANs, CTRL + click each VLAN to select.
- To disable DHCP snooping on one or more VLANs, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.



DHCP Snooping VLAN Configuration

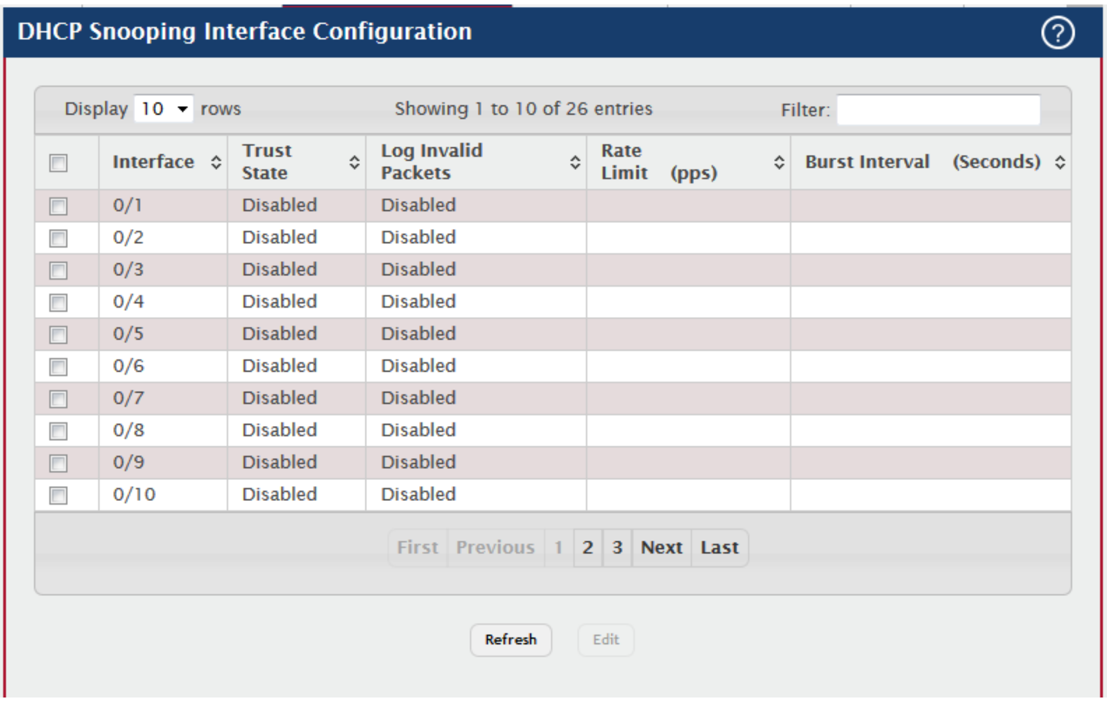
Display All rows Showing 0 to 0 of 0 entries Filter:

□	VLAN ID	DHCP Snooping Mode
Table is Empty		

Field	Description
VLAN ID	The VLAN ID that is enabled for DHCP snooping. In the Add DHCP Snooping VLAN Configuration window, this field lists the VLAN ID of all VLANs that exist on the device.
DHCP Snooping Mode	The current administrative mode of DHCP snooping for the VLAN. Only VLANs that are enabled for DHCP snooping appear in the list.

4.1.2.3 Base-Interface Configuration

Use this page to view and configure the DHCP snooping settings for each interface. The DHCP snooping feature processes incoming DHCP messages. For DHCPRELEASE and DHCPDECLINE messages, the feature compares the receive interface and VLAN with the client's interface and VLAN in the binding database. If the interfaces do not match, the application logs the event (when logging of invalid packets is enabled) and drops the message. If MAC address validation is globally enabled, messages that pass the initial validation are checked to verify that the source MAC address and the DHCP client hardware address match. Where there is a mismatch, DHCP snooping logs the event (when logging of invalid packets is enabled) and drops the packet. To change the DHCP Snooping settings for one or more interfaces, select each entry to modify and click Edit. The same settings are applied to all selected interfaces.



DHCP Snooping Interface Configuration

Display 10 rows Showing 1 to 10 of 26 entries Filter:

□	Interface	Trust State	Log Invalid Packets	Rate Limit (pps)	Burst Interval (Seconds)
□	0/1	Disabled	Disabled		
□	0/2	Disabled	Disabled		
□	0/3	Disabled	Disabled		
□	0/4	Disabled	Disabled		
□	0/5	Disabled	Disabled		
□	0/6	Disabled	Disabled		
□	0/7	Disabled	Disabled		
□	0/8	Disabled	Disabled		
□	0/9	Disabled	Disabled		
□	0/10	Disabled	Disabled		

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the settings for one or more interfaces, this field identifies each interface that is being configured.
Trust State	The trust state configured on the interface. The trust state is one of the following: Disabled – The interface is considered to be untrusted and could potentially be used to launch a network attack. DHCP server messages are checked against the bindings database. On untrusted

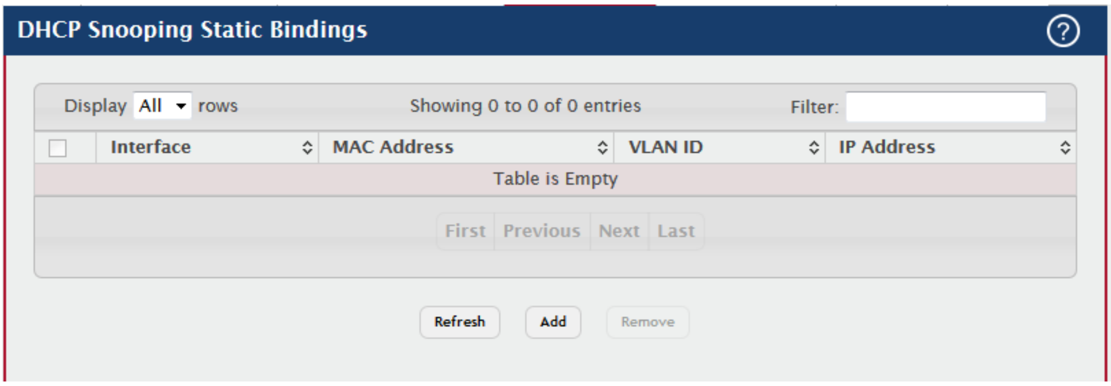
	ports, DHCP snooping enforces the following security rules: DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped. DHCPRELEASE and DHCPDECLINE messages are dropped if the MAC address is in the snooping database but the binding's interface is other than the interface where the message was received. DHCP packets are dropped when the source MAC address does not match the client hardware address if MAC Address Validation is globally enabled. Enabled – The interface is considered to be trusted and forwards DHCP server messages without validation.
Log Invalid Packets	The administrative mode of invalid packet logging on the interface. When enabled, the DHCP snooping feature generates a log message when an invalid packet is received and dropped by the interface.
Rate Limit (pps)	The rate limit value for DHCP packets received on the interface. To prevent DHCP packets from being used as a DoS attack when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. If the incoming rate of DHCP packets exceeds the value of this object during the amount of time specified for the burst interval, the port will be shutdown. You must administratively enable the port to allow it to resume traffic forwarding.
Burst Interval (Seconds)	The burst interval value for rate limiting on this interface. If the rate limit is unspecified, then burst interval has no meaning.

4.1.2.4 Base-Static Bindings

Use this page to view, add, and remove static bindings in the DHCP snooping bindings database.

Use the buttons to perform the following tasks:

- To add a static entry to the DHCP snooping bindings table, click **Add** and specify the desired settings.
- To remove one or more static entries, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

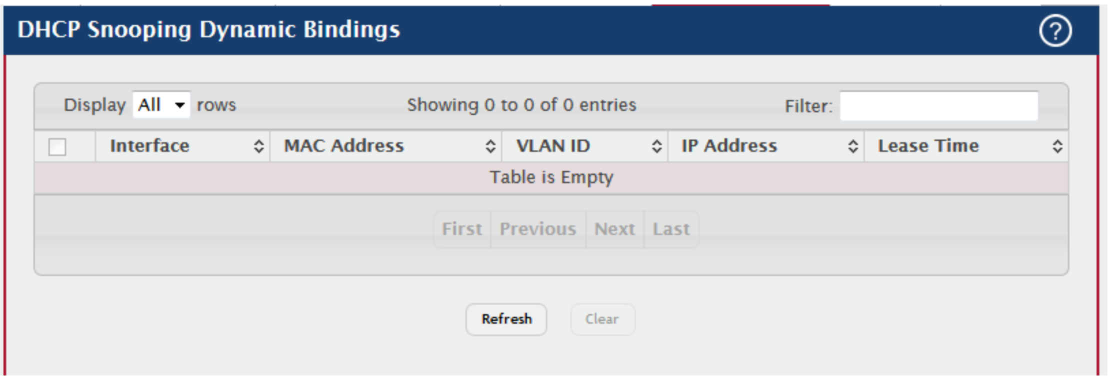


DHCP Snooping Static Bindings

Field	Description
Interface	The interface on which the DHCP client is authorized.
MAC Address	The MAC address associated with the DHCP client. This is the Key to the binding database.
VLAN ID	The ID of the VLAN the client is authorized to use.
IP Address	The IP address of the client.

4.1.2.5 Base-Dynamic Bindings

Use this page to view and clear dynamic bindings in the DHCP snooping bindings database. The DHCP snooping feature uses DHCP messages to build and maintain the bindings database. The bindings database includes data for clients only on untrusted ports. DHCP snooping creates a tentative binding from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to an interface (the interface where the DHCP client message was received). Tentative bindings are completed when DHCP snooping learns the client's IP address from a DHCP ACK message on a trusted port. DHCP snooping removes bindings in response to DECLINE, RELEASE, and NACK messages. The DHCP snooping feature ignores the ACK messages as a reply to the DHCP Inform messages received on trusted ports.



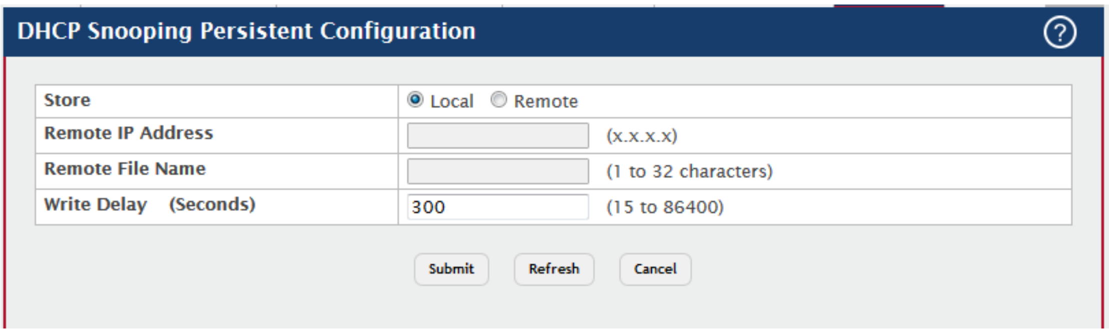
DHCP Snooping Dynamic Bindings

Field	Description
Interface	The interface on which the DHCP client message was received.

MAC Address	The MAC address associated with the DHCP client that sent the message. This is the Key to the binding database.
VLAN ID	The VLAN ID of the client interface.
IP Address	The IP address assigned to the client by the DHCP server.
Lease Time	The remaining IP address lease time for the client.
Clear (Button)	To remove one or more entries in the database, select each entry to delete and click Clear. You must confirm the action before the entry is deleted.

4.1.2.6 Base-Persistent

Use this page to configure the persistent location of the DHCP snooping bindings database. The bindings database can be stored locally on the device or on a remote system somewhere else in the network. The device must be able to reach the IP address of the remote system to send bindings to a remote database.



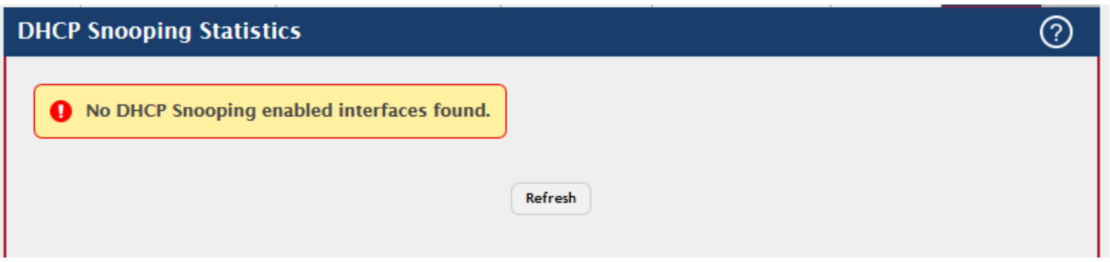
DHCP Snooping Persistent Configuration

Store	● Local ○ Remote	
Remote IP Address		(x.x.x.x)
Remote File Name		(1 to 32 characters)
Write Delay (Seconds)	300	(15 to 86400)

Field	Description
Store	The location of the DHCP snooping bindings database, which is either locally on the device (Local) or on a remote system (Remote).
Remote IP Address	The IP address of the system on which the DHCP snooping bindings database will be stored. This field is available only if Remote is selected in the Store field.
Remote File Name	The file name of the DHCP snooping bindings database in which the bindings are stored. This field is available only if Remote is selected in the Store field.
Write Delay (Seconds)	The amount of time to wait between writing bindings information to persistent storage. This allows the device to collect as many entries as possible (new and removed) before writing them to the persistent file.

4.1.2.7 Base-Statistics

Use this page to view and clear per-interface statistics about the DHCP messages filtered by the DHCP snooping feature. Only interfaces that are enabled for DHCP snooping and are untrusted appear in the table.



DHCP Snooping Statistics

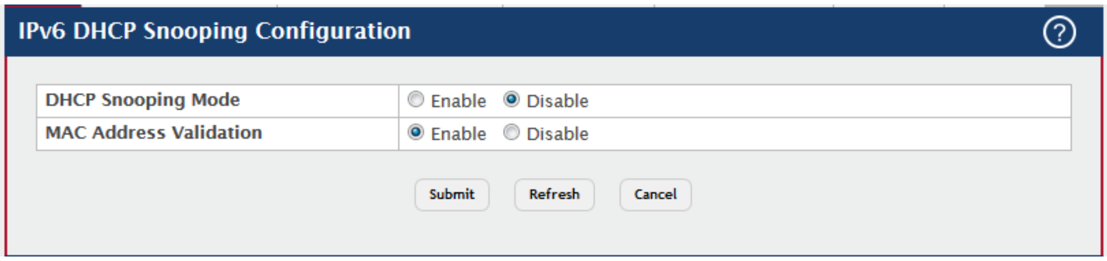
No DHCP Snooping enabled interfaces found.

Field	Description
Interface	The interface associated with the rest of the data in the row.
MAC Verify Failures	The number of DHCP messages that were dropped because the source MAC address and client hardware address did not match. MAC address verification is performed only if it is globally enabled.
Client Ifc Mismatch	The number of packets that were dropped by DHCP snooping because the interface and VLAN on which the packet was received does not match the client's interface and VLAN information stored in the binding database.
DHCP Server Msgs Received	The number of DHCP server messages ((DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) that have been dropped on an untrusted port.
Clear Counters (Button)	To reset the statistics to zero for all interfaces, click Clear Counters. You must confirm the action before the counters are reset.

4.1.3 IPv6 DHCP Snooping

4.1.3.1 Base-Global

Use this page to view and configure the global settings for IPv6 DHCP snooping. IPv6 DHCP snooping is a security feature that monitors DHCPv6 messages between a DHCPv6 client and DHCPv6 servers to filter harmful DHCPv6 messages and to build a bindings database of {MAC address, IPv6 address, VLAN ID, port} tuples that are considered authorized. You can enable IPv6 DHCP snooping globally and on specific VLANs, and configure ports within the VLAN to be trusted or untrusted. If a DHCPv6 message arrives on an untrusted port, IPv6 DHCP snooping filters messages that are not from authorized DHCPv6 clients. DHCPv6 server messages are forwarded only through trusted ports.



DHCP Snooping Mode	○ Enable ● Disable
MAC Address Validation	● Enable ○ Disable

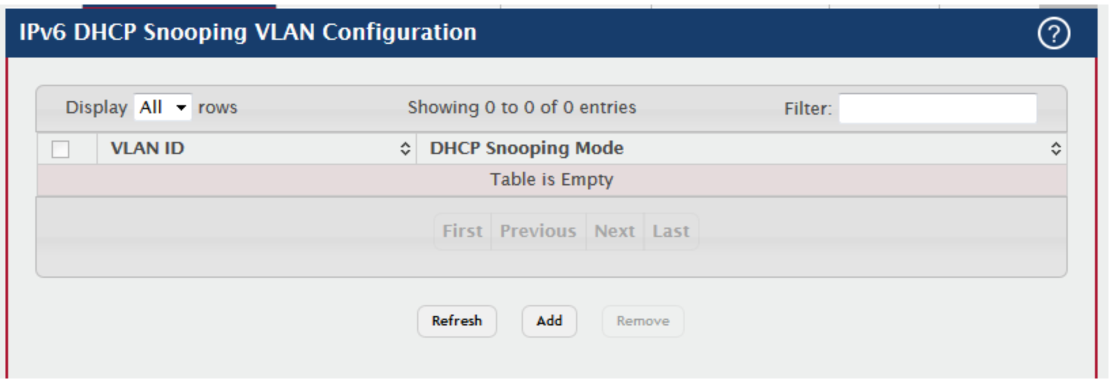
Field	Description
DHCP Snooping Mode	The administrative mode of IPv6 DHCP snooping on the device.
MAC Address Validation	Enables or Disables the verification of the sender MAC address for IPv6 DHCP snooping. When enabled, the device checks packets that are received on untrusted interfaces to verify that the MAC address and the DHCPv6 client hardware address match. If the addresses do not match, the device drops the packet.

4.1.3.2 Base-VLAN Configuration

Use this page to view and configure the IPv6 DHCP snooping settings on VLANs that exist on the device. IPv6 DHCP snooping can be configured on switching VLANs and routing VLANs. For Layer 2 (non-routing) VLANs, IPv6 DHCP snooping forwards valid DHCPv6 client messages received on the VLANs. The message is forwarded on all trusted interfaces in the VLAN. When a DHCPv6 packet is received on a routing VLAN, the IPv6 DHCP snooping application applies its filtering rules and updates the bindings database. If a client message passes filtering rules, the message is placed into the software forwarding path, where it may be processed by the DHCPv6 relay agent, the local DHCPv6 server, or forwarded as an IPv6 packet.

Use the buttons to perform the following tasks:

- To enable a VLAN for IPv6 DHCP snooping, click **Add** and select the VLAN to administratively enable for IPv6 DHCP snooping. To select multiple VLANs, CTRL + click each VLAN to select.
- To disable IPv6 DHCP snooping on one or more VLANs, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.



IPv6 DHCP Snooping VLAN Configuration

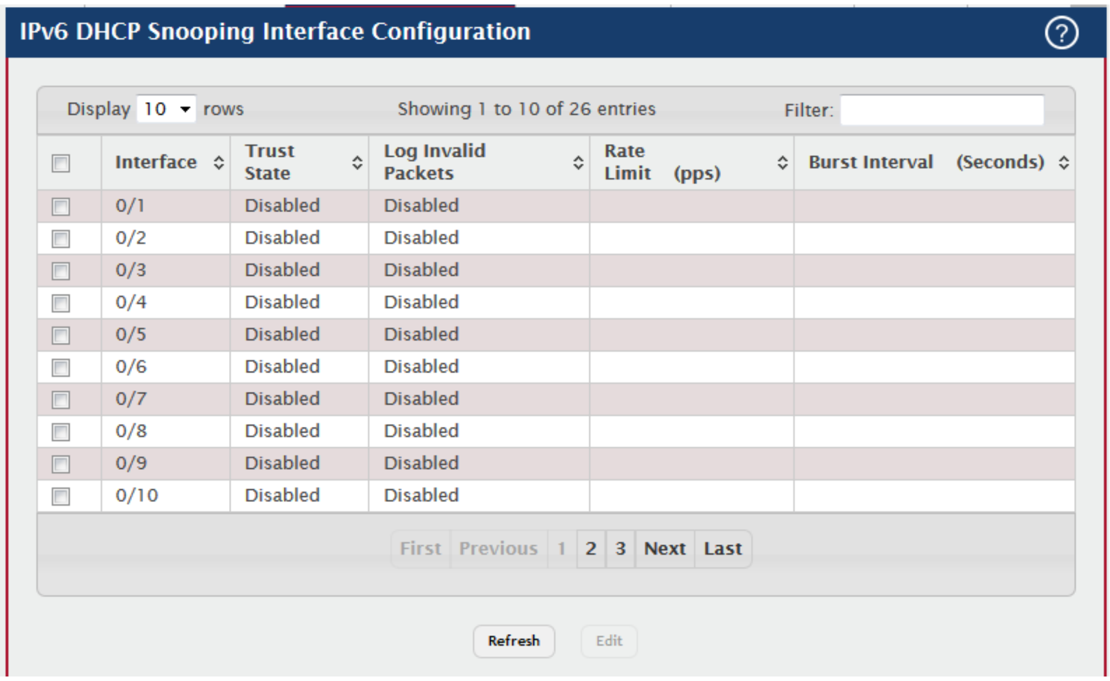
Display All rows Showing 0 to 0 of 0 entries Filter:

□	VLAN ID	DHCP Snooping Mode
Table is Empty		

Field	Description
VLAN ID	The VLAN ID that is enabled for IPv6 DHCP snooping. In the Add IPv6 DHCP Snooping VLAN Configuration window, this field lists the VLAN ID of all VLANs that exist on the device.
DHCP Snooping Mode	The current administrative mode of IPv6 DHCP snooping for the VLAN. Only VLANs that are enabled for IPv6 DHCP snooping appear in the list.

4.1.3.3 Base-Interface Configuration

Use this page to view and configure the IPv6 DHCP snooping settings for each interface. The IPv6 DHCP snooping feature processes incoming DHCPv6 messages. For RELEASE and DECLINE messages, the feature compares the receive interface and VLAN with the client's interface and VLAN in the binding database. If the interfaces do not match, the application logs the event (when logging of invalid packets is enabled) and drops the message. If MAC address validation is globally enabled, messages that pass the initial validation are checked to verify that the source MAC address and the DHCPv6 client hardware address match. Where there is a mismatch, IPv6 DHCP snooping logs the event (when logging of invalid packets is enabled) and drops the packet. To change the IPv6 DHCP snooping settings for one or more interfaces, select each entry to modify and click Edit. The same settings are applied to all selected interfaces.



IPv6 DHCP Snooping Interface Configuration

Display 10 rows Showing 1 to 10 of 26 entries Filter:

□	Interface	Trust State	Log Invalid Packets	Rate Limit (pps)	Burst Interval (Seconds)
□	0/1	Disabled	Disabled		
□	0/2	Disabled	Disabled		
□	0/3	Disabled	Disabled		
□	0/4	Disabled	Disabled		
□	0/5	Disabled	Disabled		
□	0/6	Disabled	Disabled		
□	0/7	Disabled	Disabled		
□	0/8	Disabled	Disabled		
□	0/9	Disabled	Disabled		
□	0/10	Disabled	Disabled		

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the settings for one or more interfaces, this field identifies each interface that is being configured.
Trust State	The trust state configured on the interface. The trust state is one of the following: Disabled – The interface is considered to be untrusted and could potentially be used to launch a network attack. DHCPv6 server messages are checked against the bindings database. On untrusted ports, IPv6 DHCP snooping enforces the following security rules: DHCPv6 packets from a DHCPv6 server (ADVERTISE, REPLY, and RECONFIGURE) are dropped. RELEASE and DECLINE messages are dropped if the MAC address is in the snooping database but the binding's interface is other than the interface where the message was received. DHCPv6 packets are dropped when the source MAC address does not match the client hardware address if MAC Address Validation is globally enabled. Enabled – The interface is considered to be trusted and forwards DHCPv6 server messages without validation.
Log Invalid	The administrative mode of invalid packet logging on the interface.

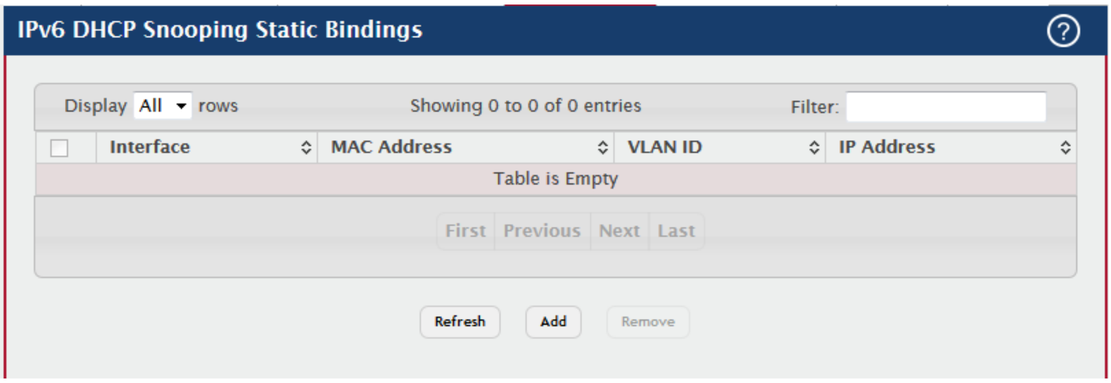
Packets	When enabled, the IPv6 DHCP snooping feature generates a log message when an invalid packet is received and dropped by the interface.
Rate Limit (pps)	The rate limit value for DHCPv6 packets received on the interface. To prevent DHCPv6 packets from being used as a DoS attack when IPv6 DHCP snooping is enabled, the snooping application enforces a rate limit for DHCPv6 packets received on untrusted interfaces. If the incoming rate of DHCPv6 packets exceeds the value of this object during the amount of time specified for the burst interval, the port will be shutdown. You must administratively enable the port to allow it to resume traffic forwarding.
Burst Interval (Seconds)	The burst interval value for rate limiting on this interface. If the rate limit is unspecified, then burst interval has no meaning.

4.1.3.4 Base-Static Bindings

Use this page to view, add, and remove static bindings in the IPv6 DHCP snooping bindings database.

Use the buttons to perform the following tasks:

- To add a static entry to the IPv6 DHCP snooping bindings table, click **Add** and specify the desired settings.
- To remove one or more static entries, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.



IPv6 DHCP Snooping Static Bindings

Display All rows   Showing 0 to 0 of 0 entries   Filter:

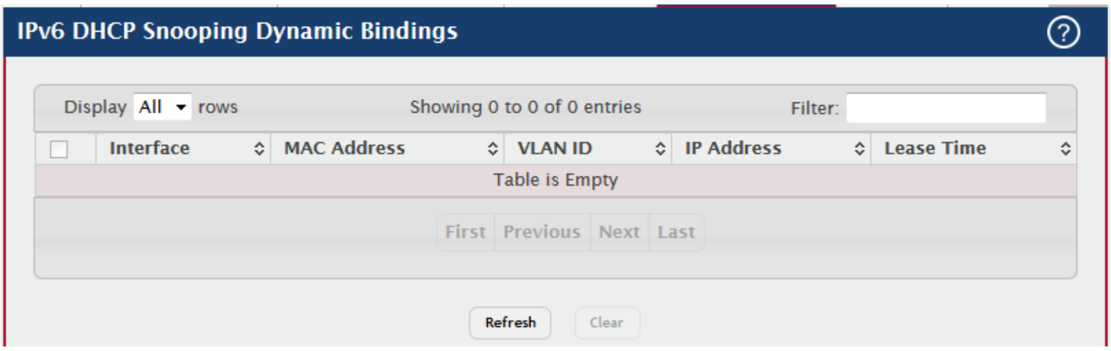
□	Interface	MAC Address	VLAN ID	IP Address
Table is Empty				

Field	Description
Interface	The interface on which the DHCPv6 client is authorized.
MAC Address	The MAC address associated with the DHCP client. This is the key to

	the binding database.
VLAN ID	The ID of the VLAN the client is authorized to use.
IP Address	The IPv6 address of the client.

4.1.3.5 Base-Dynamic Bindings

Use this page to view and clear dynamic bindings in the IPv6 DHCP snooping bindings database. The IPv6 DHCP snooping feature uses DHCPv6 messages to build and maintain the bindings database. The bindings database includes data for clients only on untrusted ports. IPv6 DHCP snooping creates a tentative binding from DHCPv6 SOLICIT and REQUEST messages. Tentative bindings tie a client to an interface (the interface where the DHCPv6 client message was received). Tentative bindings are completed when IPv6 DHCP snooping learns the client's IPv6 address from a REPLY message on a trusted port. DHCP snooping removes bindings in response to DECLINE and RELEASE messages.

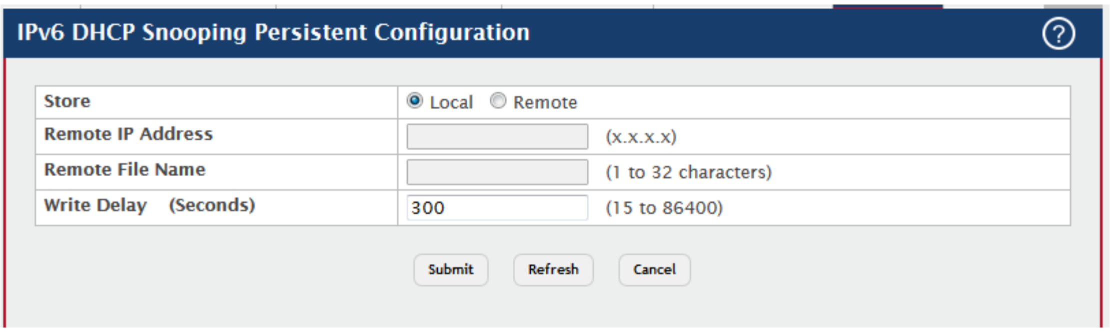

IPv6 DHCP Snooping Dynamic Bindings
?
Display All rows
Showing 0 to 0 of 0 entries
Filter:
First Previous Next Last
Refresh
Clear

□	Interface	MAC Address	VLAN ID	IP Address	Lease Time
Table is Empty					

Field	Description
Interface	The interface on which the DHCPv6 client message was received.
MAC Address	The MAC address associated with the DHCPv6 client that sent the message. This is the key to the binding database.
VLAN ID	The VLAN ID of the client interface.
IP Address	The IPv6 address assigned to the client by the DHCPv6 server.
Lease Time	The remaining IPv6 address lease time for the client.
Clear (Button)	To remove one or more entries in the database, select each entry to delete and click Clear. You must confirm the action before the entry is deleted.

4.1.3.6 Base-Presistent

Use this page to configure the persistent location of the IPv6 DHCP snooping bindings database. The bindings database can be stored locally on the device or on a remote system somewhere else in the network. The device must be able to reach the IP address of the remote system to send bindings to a remote database.



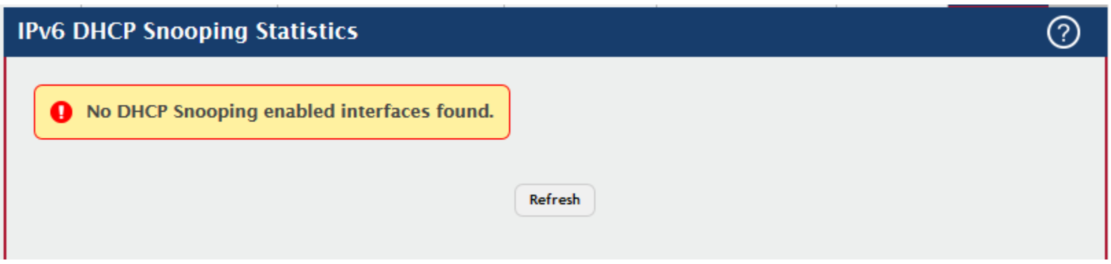
IPv6 DHCP Snooping Persistent Configuration

Store	● Local ○ Remote
Remote IP Address	(x.x.x.x)
Remote File Name	(1 to 32 characters)
Write Delay (Seconds)	300 (15 to 86400)

Field	Description
Store	The location of the IPv6 DHCP snooping bindings database, which is either locally on the device (Local) or on a remote system (Remote).
Remote IP Address	The IP address of the system on which the IPv6 DHCP snooping bindings database will be stored. This field is available only if Remote is selected in the Store field.
Remote File Name	The file name of the IPv6 DHCP snooping bindings database in which the bindings are stored. This field is available only if Remote is selected in the Store field.
Write Delay (Seconds)	The amount of time to wait between writing bindings information to persistent storage. This allows the device to collect as many entries as possible (new and removed) before writing them to the persistent file.

4.1.3.7 Base-Satistics

Use this page to view and clear per-interface statistics about the DHCPv6 messages filtered by the IPv6 DHCP snooping feature. Only interfaces that are enabled for IPv6 DHCP snooping and are untrusted appear in the table.



IPv6 DHCP Snooping Statistics

No DHCP Snooping enabled interfaces found.

Field	Description
Interface	The interface associated with the rest of the data in the row.
MAC Verify Failures	The number of DHCPv6 messages that were dropped because the source MAC address and client hardware address did not match. MAC address verification is performed only if it is globally enabled.
Client Ifc Mismatch	The number of packets that were dropped by IPv6 DHCP snooping because the interface and VLAN on which the packet was received does not match the client's interface and VLAN information stored in the binding database.
DHCP Server Msgs Received	The number of DHCPv6 server messages ((ADVERTISE, REPLY, RECONFIGURE, RELAY-REPL) that have been dropped on an untrusted port.
Clear Counters (Button)	To reset the statistics to zero for one or more interfaces, select each interface with the data to reset and click Clear Counters. You must confirm the action before the entry is deleted.

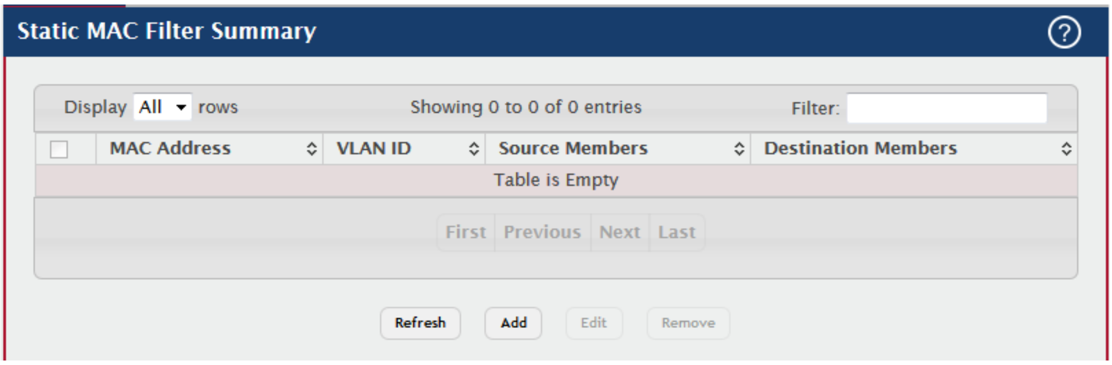
4.1.4 Filters

4.1.4.1 MAC Filters

Use this page to view, create, edit, and remove static MAC filters on the device. A MAC filter is a security mechanism that allows Ethernet frames that match the filter criteria (destination MAC address and VLAN ID) to be received and transmitted only on certain ports.

Use the buttons to perform the following tasks:

- To add a filter, click **Add** and configure the filter criteria.
- To edit a filter, select the filter to update and click **Edit**.
- To remove a filter, select each entry to delete and click **Remove**.



Static MAC Filter Summary

Display All rows   Showing 0 to 0 of 0 entries   Filter:

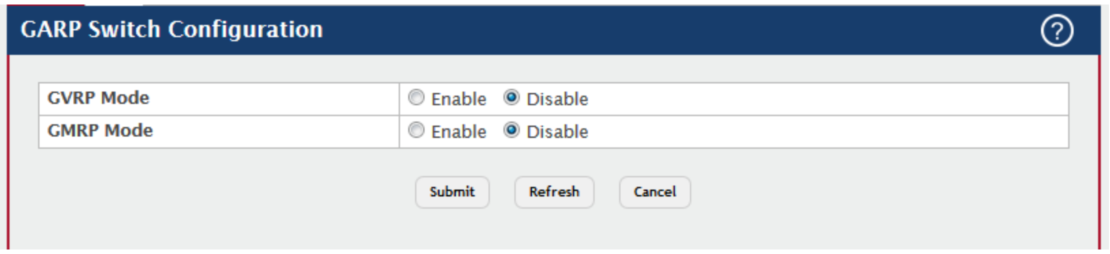
□	MAC Address	VLAN ID	Source Members	Destination Members
Table is Empty				

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:C2:00:00:10 01:80:C2:00:00:20 to 01:80:C2:00:00:2F 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 Members	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 Members	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.

4.1.5 GARP

4.1.5.1 Switch

Use this page to set the administrative mode for the features that use the Generic Attribute Registration Protocol (GARP), including GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). GARP is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of switches interested in a given network attribute, such as VLAN ID or multicast address.



GARP Switch Configuration

GVRP Mode ○ Enable ● Disable

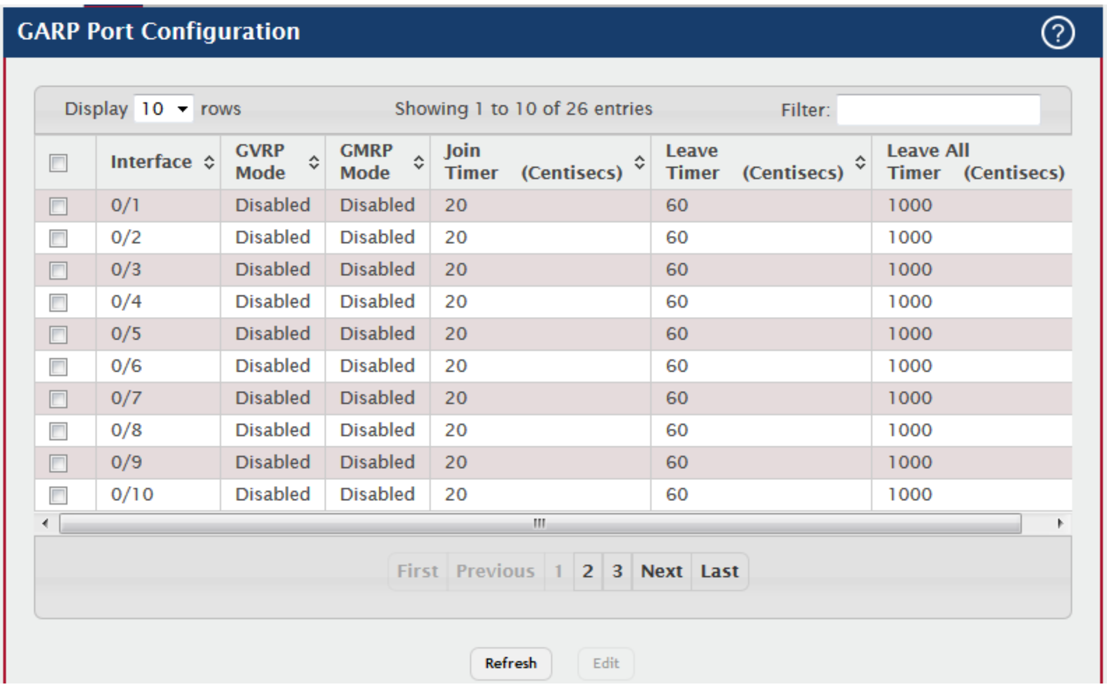
GMRP Mode ○ Enable ● Disable

Field	Description
GVRP Mode	The administrative mode of GVRP on the system. When enabled, GVRP can help dynamically manage VLAN memberships on trunk ports.
GMRP Mode	The administrative mode of GMRP on the system. When enabled, GMRP can help control the flooding of multicast traffic by keeping track of group membership information. GMRP is similar to IGMP snooping in its purpose, but IGMP snooping is more widely used. GMRP must be running on both the host and the switch to function properly.

4.1.5.2 Port

Use this page to set the per-interface administrative mode for GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). On this page, you can also set the GARP timers for each interface. GVRP and GMRP use the same set of GARP timers to specify the amount of time to wait before transmitting various GARP messages.

To change the GARP settings for one or more interfaces, select each interface to configure and click Edit. The same settings are applied to all selected interfaces.



□	Interface	GVRP Mode	GMRP Mode	Join Timer (Centisecs)	Leave Timer (Centisecs)	Leave All Timer (Centisecs)
□	0/1	Disabled	Disabled	20	60	1000
□	0/2	Disabled	Disabled	20	60	1000
□	0/3	Disabled	Disabled	20	60	1000
□	0/4	Disabled	Disabled	20	60	1000
□	0/5	Disabled	Disabled	20	60	1000
□	0/6	Disabled	Disabled	20	60	1000
□	0/7	Disabled	Disabled	20	60	1000
□	0/8	Disabled	Disabled	20	60	1000
□	0/9	Disabled	Disabled	20	60	1000
□	0/10	Disabled	Disabled	20	60	1000

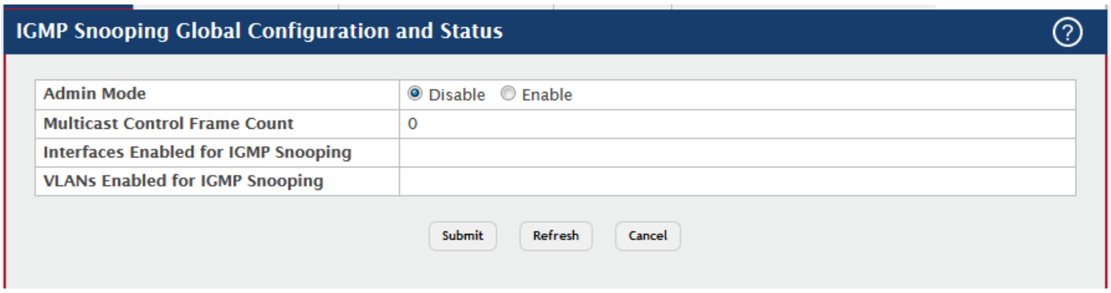
Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring one or more interfaces in the Edit GARP Port Configuration window, this field identifies the interfaces that are being configured.
GVRP Mode	The administrative mode of GVRP on the interface. When enabled, GVRP can help dynamically manage VLAN memberships on trunk ports. GVRP must also be enabled globally for the protocol to be active on the interface. When disabled, the protocol will not be active on the interface, and the GARP timers have no effect.
GMRP Mode	The administrative mode of GMRP on the interface. When enabled, GMRP can help control the flooding of multicast traffic by keeping track of group membership information. GMRP must also be enabled globally for the protocol to be active on the interface. When disabled, the protocol will not be active on the interface, and the GARP timers have no effect.
Join Timer (Centisecs)	The amount of time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group.
Leave Timer (Centisecs)	The amount of time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry. This

	timer allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service.
Leave All Timer (Centisecs)	The amount of time to wait before sending a LeaveAll PDU after the GARP application has been enabled on the interface or the last LeaveAll PDU was sent. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration.

4.1.6 IGMP Snooping

4.1.6.1 Configuration

Use this page to enable Internet Group Management Protocol (IGMP) snooping on the device and to view global status information. IGMP snooping allows a device to forward multicast traffic intelligently. 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 device forwards traffic only to the ports that request the multicast traffic. This prevents the device from broadcasting the traffic to all ports and possibly affecting network performance.



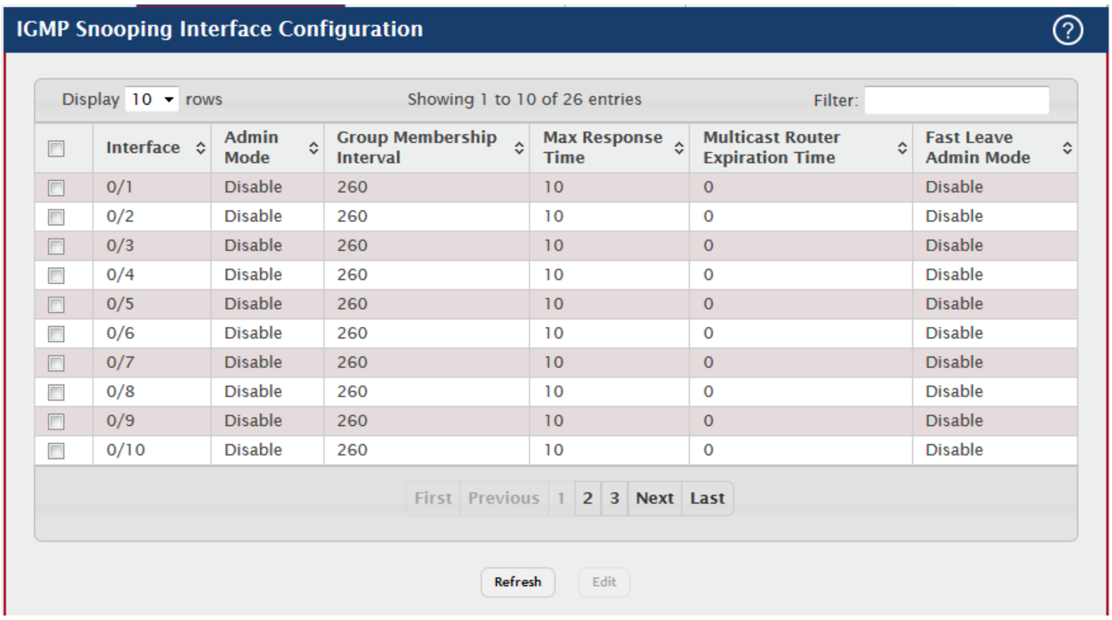
IGMP Snooping Global Configuration and Status

Admin Mode	● Disable ○ Enable
Multicast Control Frame Count	0
Interfaces Enabled for IGMP Snooping	
VLANs Enabled for IGMP Snooping	

Field	Description
Admin Mode	The administrative mode of IGMP snooping on the device.
Multicast Control Frame Count	The number of multicast control frames that have been processed by the CPU.
Interfaces Enabled for IGMP Snooping	One or more interfaces on which IGMP snooping is administratively enabled. IGMP snooping must be enabled globally and on an interface for the interface to be able to snoop IGMP packets to determine which segments should receive multicast packets directed to the group address.
VLANs Enabled for IGMP Snooping	One or more VLANs on which IGMP snooping is administratively enabled.

4.1.6.2 Interface Configuration

Use this page to configure IGMP snooping settings on specific interfaces. To configure the settings for one or more interfaces, select each entry to modify and click Edit. The same IGMP snooping settings are applied to all selected interfaces.



IGMP Snooping Interface Configuration

Display 10 rows | Showing 1 to 10 of 26 entries | Filter:

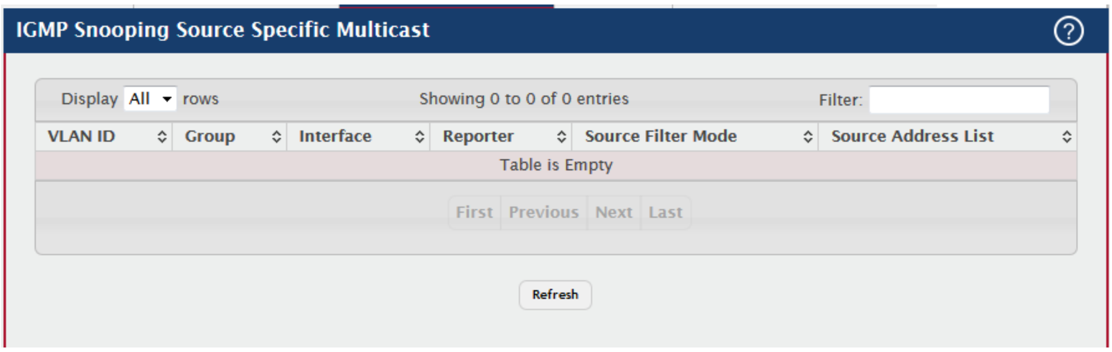
□	Interface	Admin Mode	Group Membership Interval	Max Response Time	Multicast Router Expiration Time	Fast Leave Admin Mode
□	0/1	Disable	260	10	0	Disable
□	0/2	Disable	260	10	0	Disable
□	0/3	Disable	260	10	0	Disable
□	0/4	Disable	260	10	0	Disable
□	0/5	Disable	260	10	0	Disable
□	0/6	Disable	260	10	0	Disable
□	0/7	Disable	260	10	0	Disable
□	0/8	Disable	260	10	0	Disable
□	0/9	Disable	260	10	0	Disable
□	0/10	Disable	260	10	0	Disable

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring IGMP snooping settings, this field identifies the interface(s) that are being configured.
Admin Mode	The administrative mode of IGMP snooping on the interface. IGMP snooping must be enabled globally and on an interface for the interface to be able to snoop IGMP packets to determine which segments should receive multicast packets directed to the group address.
Group Membership Interval	The number of seconds the interface should wait for a report for a particular group on the interface before the IGMP snooping feature deletes the interface from the group.
Max Response Time	The number of seconds the interface should wait after sending a query if it does not receive a report for a particular group. The specified value should be less than the Group Membership Interval.
Multicast Router Expiration Time	The number of seconds the interface should wait to receive a query before it is removed from the list of interfaces with multicast routers attached.

Fast Leave Admin Mode	The administrative mode of Fast Leave on the interface. If Fast Leave is enabled, the interface can be immediately removed from the layer 2 forwarding table entry upon receiving an IGMP leave message for a multicast group without first sending out MAC-based general queries.

4.1.6.3 Source Specific Multicast

This page displays information about IGMP snooping for source specific multicast.



IGMP Snooping Source Specific Multicast

Display All rows Showing 0 to 0 of 0 entries Filter:

VLAN ID	Group	Interface	Reporter	Source Filter Mode	Source Address List
Table is Empty					

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.

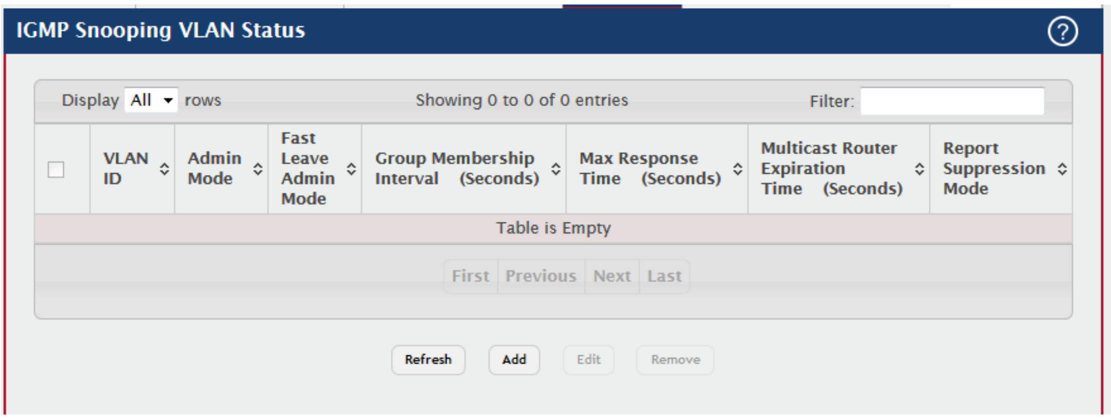
4.1.6.4 VLAN Status

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.

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.



IGMP Snooping VLAN Status

Display All rows Showing 0 to 0 of 0 entries Filter:

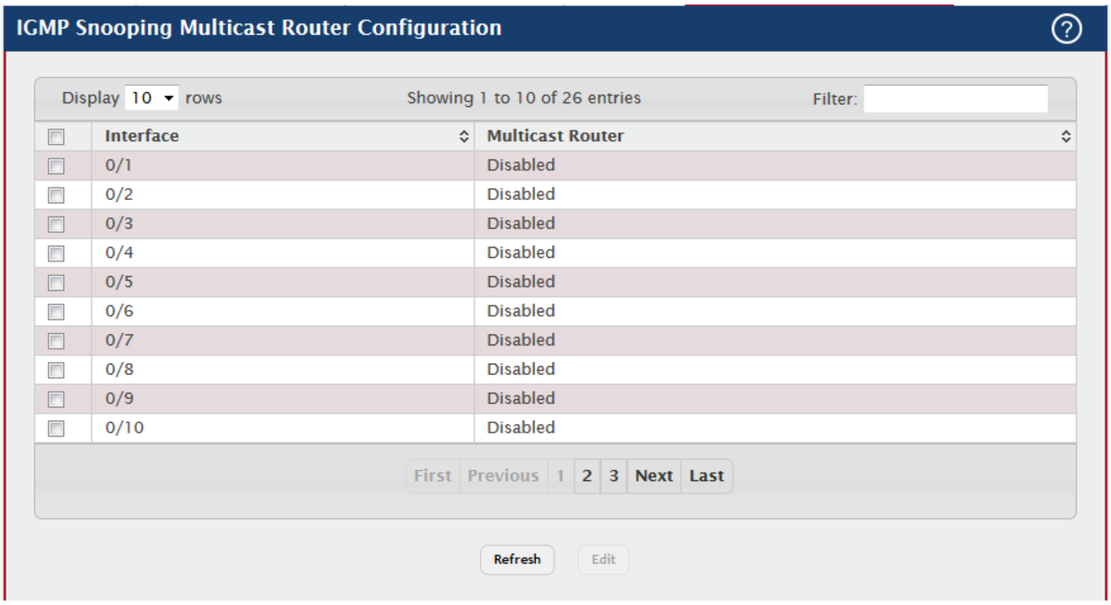
□	VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval (Seconds)	Max Response Time (Seconds)	Multicast Router Expiration Time (Seconds)	Report Suppression Mode
Table is Empty							

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 wait for a report for a particular group on the VLAN before the IGMP snooping feature deletes the VLAN from the group.
Max Response Time (Seconds)	The number of seconds the VLAN should wait after sending a query if it 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.

4.1.6.5 Multicast Router Configuration

If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure an interface as a multicast router interface, which is an interface that faces a multicast router or IGMP querier and receives multicast traffic. Use this page to manually configure an interface as a static multicast router interface. To change the multicast router mode for one or more interfaces, select each entry to modify and click Edit.



IGMP Snooping Multicast Router Configuration

Display 10 rows   Showing 1 to 10 of 26 entries   Filter:

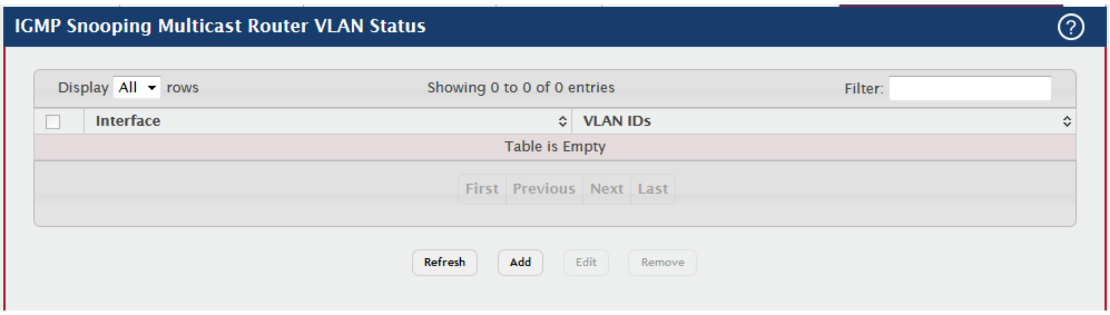
□	Interface	Multicast Router
□	0/1	Disabled
□	0/2	Disabled
□	0/3	Disabled
□	0/4	Disabled
□	0/5	Disabled
□	0/6	Disabled
□	0/7	Disabled
□	0/8	Disabled
□	0/9	Disabled
□	0/10	Disabled

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the IGMP snooping multicast router settings, this field identifies the interface(s) that are being configured.
Multicast Router	Indicates whether the interface is enabled or disabled as a multicast router interface.

4.1.6.6 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.

Use this page to view the multicast router VLAN status for each interface. From this page, you can also click the Add and Edit buttons to be redirected to the Multicast Router VLAN Configuration page for the selected interface to enable or disable VLANs as multicast router interfaces. To disable all VLANs as multicast router interfaces for one or more physical ports or LAGs, select each entry to modify and click Remove.


IGMP Snooping Multicast Router VLAN Status

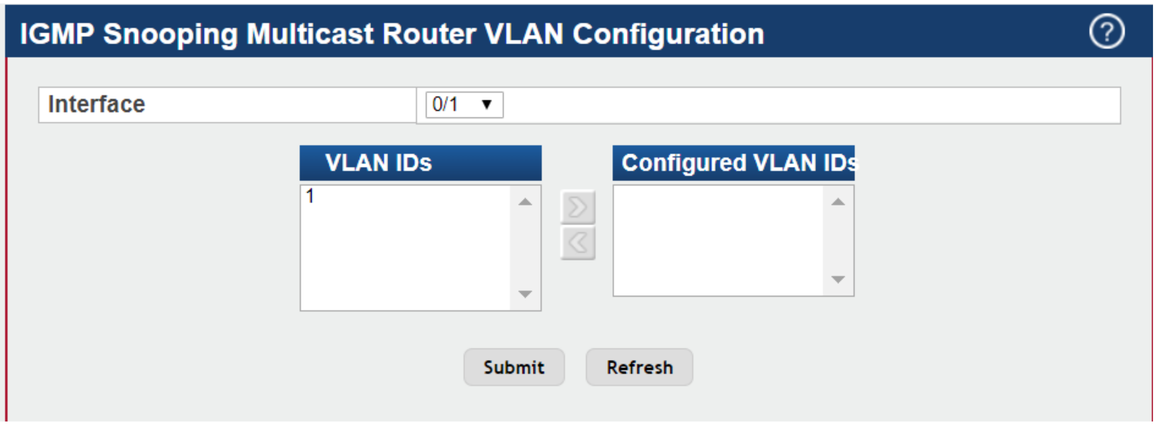
Display All rows Showing 0 to 0 of 0 entries Filter:

□	Interface	VLAN IDs
	Table is Empty	

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.

4.1.6.7 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.



IGMP Snooping Multicast Router VLAN Configuration

Interface: 0/1

VLAN IDs: 1

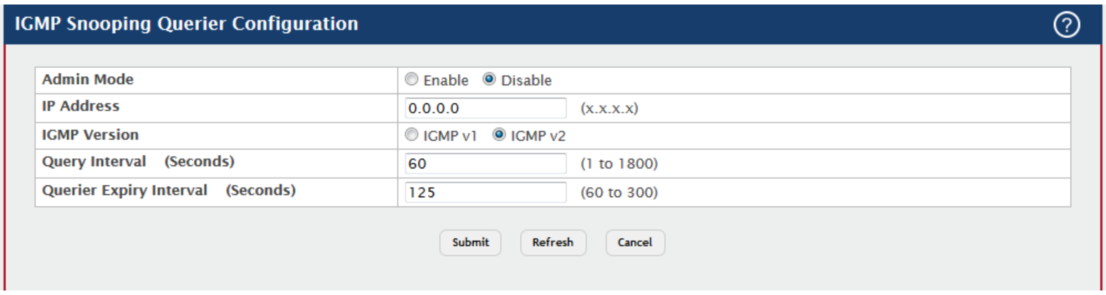
Configured VLAN IDs:

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.

4.1.7 IGMP Snooping Querier

4.1.7.1 Multicast Router VLAN Status

Use this page to configure the global IGMP snooping querier settings on the device. IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP querier. When layer 3 IP multicast routing protocols are enabled in a network with IP multicast routing, the IP multicast router acts as the IGMP querier. However, if the IP-multicast traffic in a VLAN needs to be layer 2 switched only, an IP-multicast router is not required. The IGMP snooping querier can perform the IGMP snooping functions on the VLAN.



IGMP Snooping Querier Configuration

Admin Mode	○ Enable ● Disable	
IP Address	0.0.0.0	(x.x.x.x)
IGMP Version	○ IGMP v1 ● IGMP v2	
Query Interval (Seconds)	60	(1 to 1800)
Querier Expiry Interval (Seconds)	125	(60 to 300)

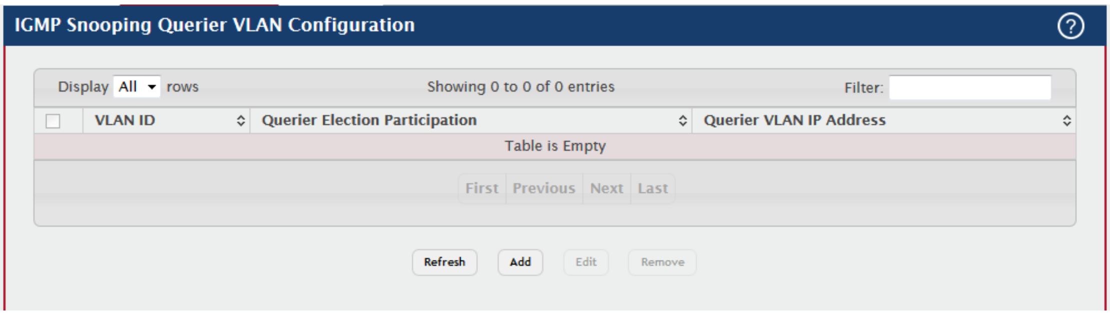
Field	Description
Admin Mode	The administrative mode for the IGMP snooping querier on the device. When enabled, the IGMP snooping querier sends out periodic IGMP queries that trigger IGMP report messages from the switches that want to receive IP multicast traffic. The IGMP snooping feature listens to these IGMP reports to establish appropriate forwarding.
IP Address	The snooping querier address to be used as source address in periodic IGMP queries. This address is used when no IP address is configured on the VLAN on which the query is being sent.
IGMP Version	The IGMP protocol version used in periodic IGMP queries.
Query Interval (Seconds)	The amount of time the IGMP snooping querier on the device should wait between sending periodic IGMP queries.
Querier Expiry Interval (Seconds)	The amount of time the device remains in non-querier mode after it has discovered that there is a multicast querier in the network.

4.1.7.2 VLAN Configuration

Use this page to enable the IGMP snooping querier feature on one or more VLANs and to configure per-VLAN IGMP snooping querier settings. Only VLANS that have the IGMP snooping querier feature enabled appear in the table.

Use the buttons to perform the following tasks:

- To enable the IGMP snooping querier feature on a VLAN, click **Add** and specify the desired settings.
- To change the IGMP snooping querier settings for a VLAN, select the entry to modify and click **Edit**.
- To disable the IGMP snooping querier feature on one or more VLANs, select each entry to change and click **Remove**. You must confirm the action before the entry is deleted. Clicking this button does not remove the VLAN from the system.



IGMP Snooping Querier VLAN Configuration

Display All rows Showing 0 to 0 of 0 entries Filter:

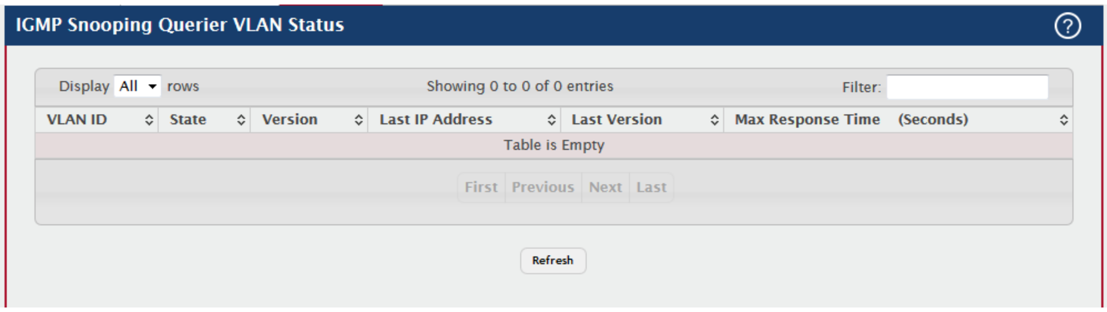
□	VLAN ID	Querier Election Participation	Querier VLAN IP Address
Table is Empty			

Field	Description
VLAN ID	The VLAN on which the IGMP snooping querier is enabled. When enabling the IGMP snooping querier on a VLAN, use this menu to select the desired VLAN. Only VLANs that have been configured on the system and are not already enabled for the IGMP snooping querier appear in the menu. When modifying IGMP snooping querier settings, this field identifies the VLAN that is being configured.
Querier Election Participation	The participation mode for the IGMP snooping querier election process: Enabled – The IGMP snooping querier on this VLAN participates in the querier election process when it discovers the presence of another querier in the VLAN. If the snooping querier finds that the other querier source IP address is lower than its own address, it stops sending periodic queries. If the snooping querier wins the election (because it has the lowest IP address), then it continues sending periodic queries. Disabled – When the IGMP snooping querier on this VLAN sees other queriers of the same version in the VLAN, the snooping querier moves to the non-querier state and stops sending periodic queries.

Querier VLAN IP Address	The IGMP snooping querier address the VLAN uses as the source IP address in periodic IGMP queries sent on the VLAN. If this value is not configured, the VLAN uses the global IGMP snooping querier IP address.

4.1.7.3 VLAN Status

Use this page to view information about the IGMP snooping querier status for all VLANs that have the snooping querier enabled.


IGMP Snooping Querier VLAN Status

Display All rows Showing 0 to 0 of 0 entries Filter:

VLAN ID	State	Version	Last IP Address	Last Version	Max Response Time (Seconds)
Table is Empty					

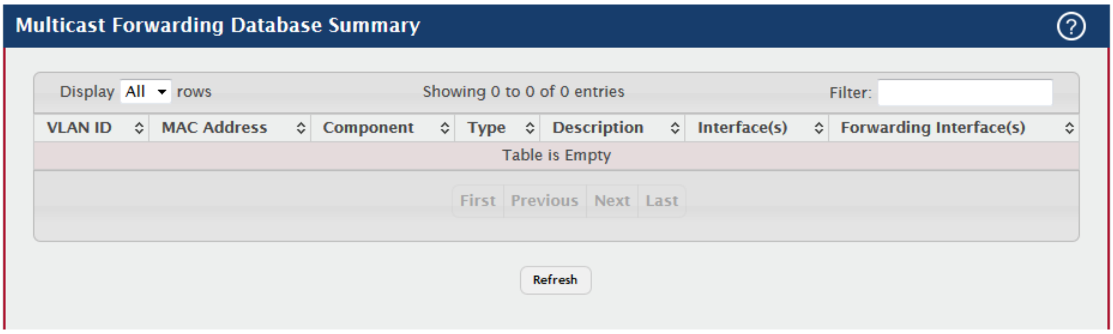
Field	Description
VLAN ID	The VLAN associated with the rest of the data in the row. The table includes only VLANs that have the snooping querier enabled.
State	The operational state of the IGMP snooping querier on the VLAN, which is one of the following: Querier – The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode. Non-Querier – The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. Disabled – The snooping querier is not operational on the VLAN. The snooping querier moves to the disabled mode when IGMP snooping is not operational on the VLAN, when the querier address is not configured, or the network management address is not configured.
Version	The operational IGMP protocol version of the querier.
Last IP Address	The IP address of the last querier from which a query was snooped on the VLAN.
Last Version	The IGMP protocol version of the last querier from which a query was snooped on the VLAN.

Max Response Time (Seconds)	The maximum response time to be used in the queries that are sent by the snooping querier.

4.1.8 Multicast Forwarding Database

4.1.8.1 Summary

This page displays the entries in the multicast forwarding database (MFDB) on the device. The MFDB holds the port membership information for all active multicast address entries and is used to make forwarding decisions for frames that arrive with a multicast destination MAC address. The key for an entry consists of a VLAN ID and MAC address pair. Entries may contain data for more than one protocol.



Multicast Forwarding Database Summary

Display All rows Showing 0 to 0 of 0 entries Filter:

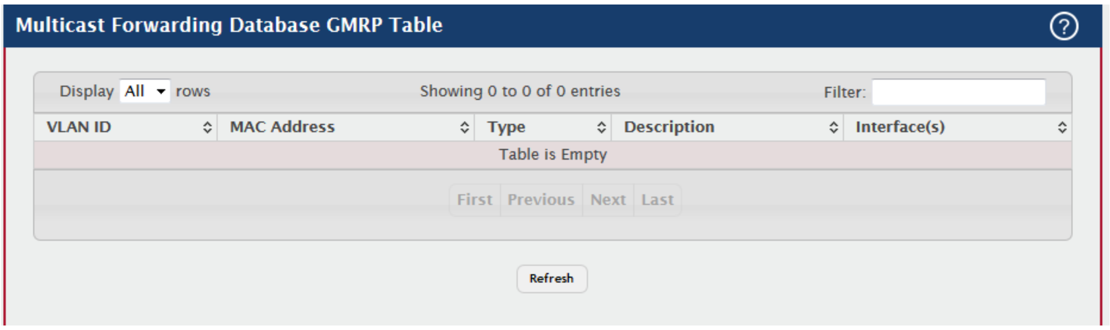
VLAN ID	MAC Address	Component	Type	Description	Interface(s)	Forwarding Interface(s)
Table is Empty						

Field	Description
VLAN ID	The VLAN ID associated with the entry in the MFDB.
MAC Address	The multicast MAC address 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. GMRP – Generic Address Resolution Protocol (GARP) Multicast Registration Protocol, which helps 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.

4.1.8.2 GMRP

This page displays the entries in the multicast forwarding database (MFDB) that were added by using the GARP Multicast Registration Protocol (GMRP).


Multicast Forwarding Database GMRP Table

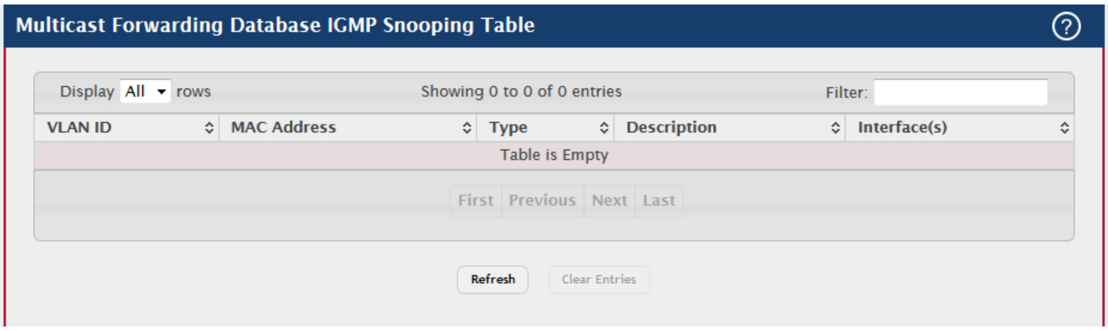
Display All rows Showing 0 to 0 of 0 entries Filter:

VLAN ID	MAC Address	Type	Description	Interface(s)
Table is Empty				

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.

4.1.8.3 IGMP Snooping

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.


Multicast Forwarding Database IGMP Snooping Table

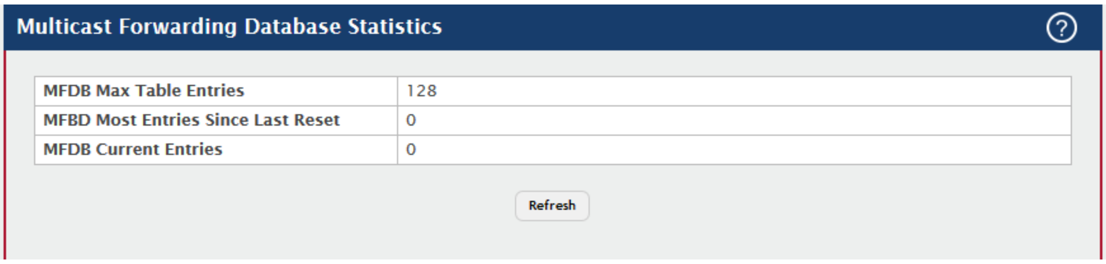
Display All rows — Showing 0 to 0 of 0 entries — Filter:

VLAN ID	MAC Address	Type	Description	Interface(s)
Table is Empty				

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.
Clear Entries (Button)	To remove all IGMP snooping entries from the MFDB table, click Clear Entries. The table is repopulated as new addresses are discovered by the IGMP snooping feature.

4.1.8.4 Statistics

This page displays statistical information about the multicast forwarding database (MFDB).


Multicast Forwarding Database Statistics

MFDB Max Table Entries	128
MFBD Most Entries Since Last Reset	0
MFDB Current Entries	0

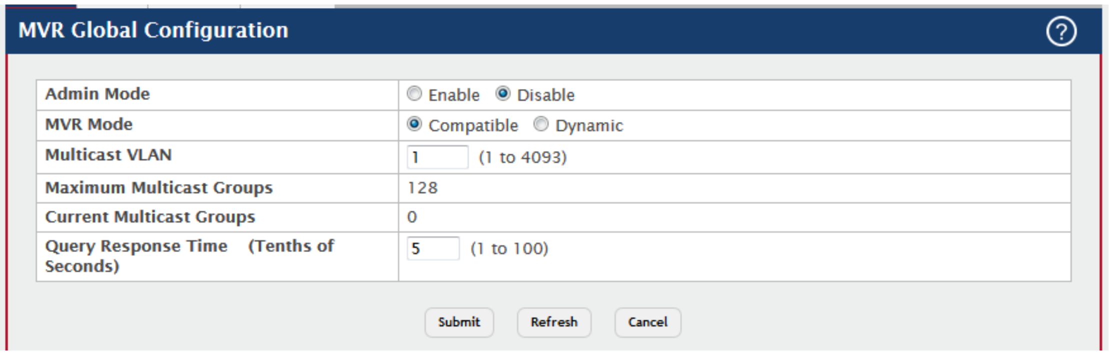
Field	Description
MFDB Max Table Entries	The maximum number of entries that the multicast forwarding database can hold.

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.

4.1.9 MVR

4.1.9.1 Global

Use this page to view and configure the global settings for Multicast VLAN Registration (MVR). MVR allows the switch to listen to the Internet Group Management Protocol (IGMP) frames. Both protocols operate independently from each other and can be enabled on the switch interfaces. In such case, MVR listens to the Join and Report messages only for the statically configured groups. All other groups are managed by IGMP snooping. MVR uses the multicast VLAN, a dedicated VLAN used to transfer multicast traffic over the network avoiding duplication of multicast streams for clients in different VLANs.



MVR Global Configuration

Admin Mode	○ Enable ● Disable
MVR Mode	● Compatible ○ Dynamic
Multicast VLAN	1 (1 to 4093)
Maximum Multicast Groups	128
Current Multicast Groups	0
Query Response Time (Tenths of Seconds)	5 (1 to 100)

Field	Description
Admin Mode	The administrative mode of MVR on the device.
MVR Mode	The MVR learning mode, which can be one of the following: Compatible – MVR does not learn source ports membership, instead all source ports are members of all groups by default. MVR does not forward IGMP Joins and Leaves from the hosts to the router. Dynamic – MVR learns source ports membership from IGMP queries. MVR forwards the IGMP Joins and Leaves from the hosts to the router. The multicast traffic is forwarded only to the receiver ports that joined the group, either by IGMP Joins or MVR static configuration.
Multicast VLAN	A dedicated VLAN used to transfer multicast traffic over the network

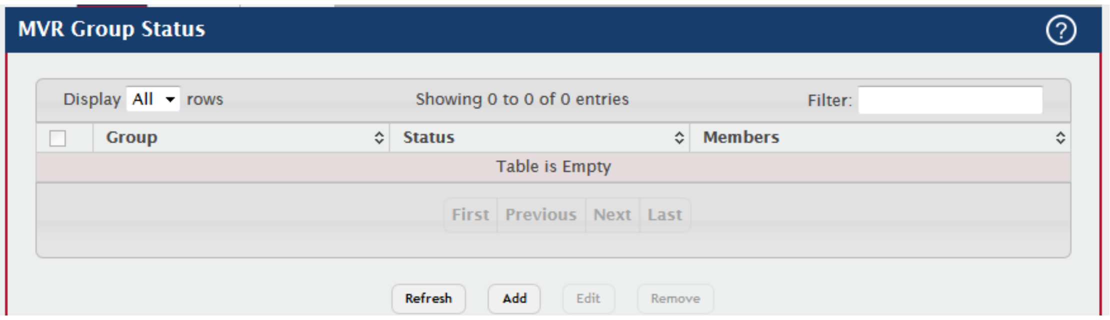
	avoiding duplication of multicast streams for clients in different VLANs.
Maximum Multicast Groups	The maximum number of membership groups that can be statically configured in the MVR database.
Current Multicast Groups	The current number of membership groups that are statically configured in the MVR database.
Query Response Time	The maximum time to wait for an IGMP membership report on a receiver port before removing the port from the multicast group. The query time is specified in tenths of a second.

4.1.9.2 Group

Use this page to view or configure MVR groups. MVR maintains two types of group entries in its database, Static and Dynamic. Static entries are configured by the administrator and Dynamic entries are learned by MVR on the source ports.

Use the buttons to perform the following tasks:

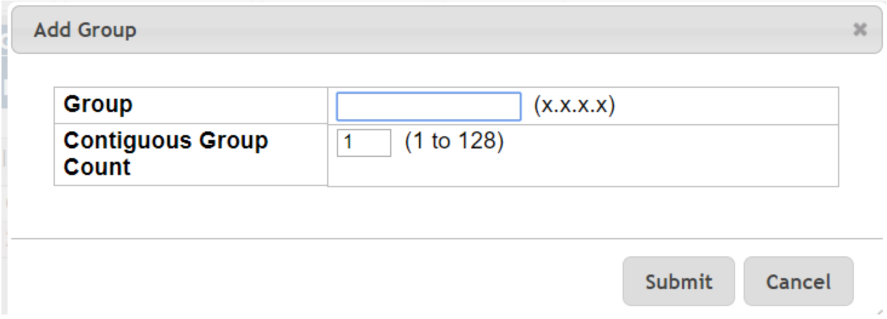
- To add a group, click **Add** and specify a group address in the available field.
- To edit a configured group, select the entry to modify and click **Edit.** Then, configure the desired VLAN settings.
- To remove one or more configured groups, select each entry to delete and click **Remove.** You must confirm the action before the entry is deleted.



MVR Group Status

Display All rows   Showing 0 to 0 of 0 entries   Filter:

□	Group	Status	Members
	Table is Empty		



Add Group

Group	(x.x.x.x)
Contiguous Group Count	1 (1 to 128)

Field	Description
Group	The multicast group address.
Status	The status of the group, which can be one of the following: Active – Group has one or more MVR ports participating. Inactive – Group has no MVR ports participating.
Members	The list of interfaces which participate in the MVR group. In the compatible mode, all source ports are members of all groups by default.

After you click Add, the Add Group window opens and allows you to create groups. The following information describes the additional field in this window.

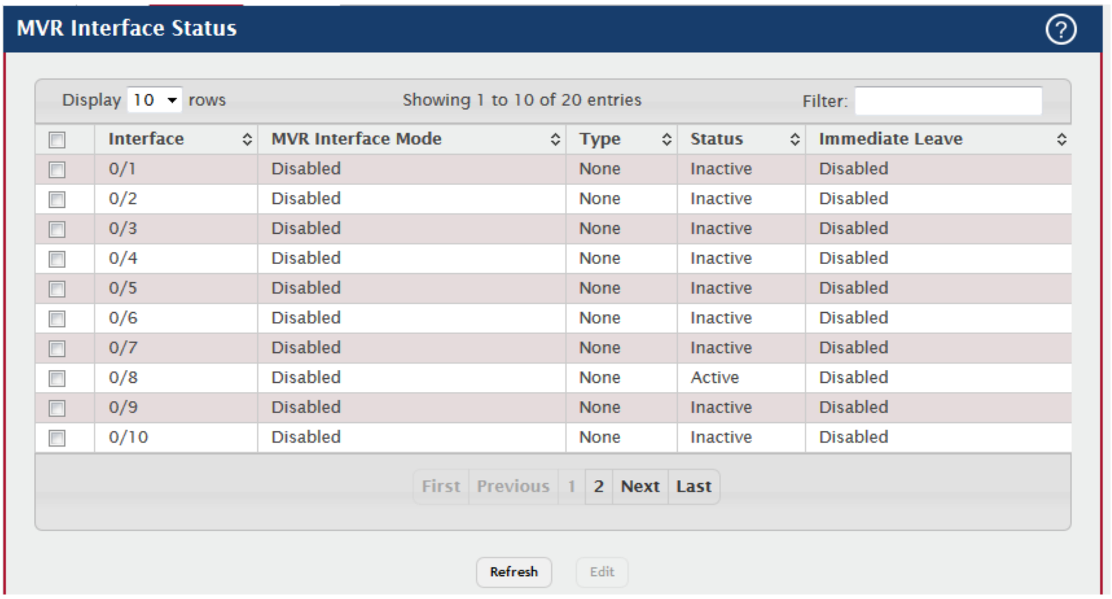
Field	Description
Contiguous Group Count	Specify the desired number of groups to be created starting with the entered group address. The default contiguous group count is 1.

When you click Edit, the Edit Group Configuration window opens. The following information describes the fields in this window.

Field	Description
Available Interfaces	The interfaces that can be added to the group. To move an interface between the Available Interfaces and Group Interfaces fields, click the interface (or CTRL + click to select multiple interfaces), and then click the appropriate arrow to move the selected interfaces to the desired field.
Group Interfaces	The interfaces that are members of the MVR group.

4.1.9.3 Interface

Use this page to configure MVR settings on specific interfaces. To configure the settings for one or more interfaces, select each entry to modify and click Edit. The same MVR settings are applied to all selected interfaces.



MVR Interface Status

Display 10 rows   Showing 1 to 10 of 20 entries   Filter:

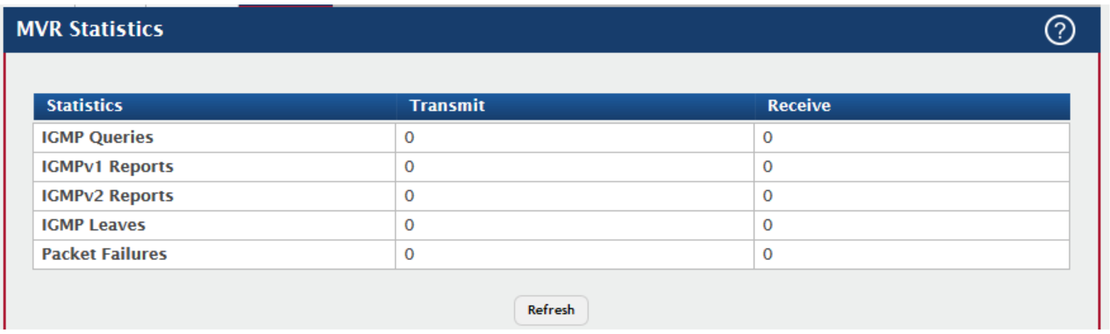
□	Interface	MVR Interface Mode	Type	Status	Immediate Leave
□	0/1	Disabled	None	Inactive	Disabled
□	0/2	Disabled	None	Inactive	Disabled
□	0/3	Disabled	None	Inactive	Disabled
□	0/4	Disabled	None	Inactive	Disabled
□	0/5	Disabled	None	Inactive	Disabled
□	0/6	Disabled	None	Inactive	Disabled
□	0/7	Disabled	None	Inactive	Disabled
□	0/8	Disabled	None	Active	Disabled
□	0/9	Disabled	None	Inactive	Disabled
□	0/10	Disabled	None	Inactive	Disabled

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring MVR settings, this field identifies the interface(s) that are being configured.
MVR Interface Mode	The administrative mode of MVR on the interface. MVR must be enabled globally and on an interface in order to listen to the Join and Report messages for the configured groups.
Type	The type of interface, which can be one of the following: Source – The port where multicast traffic is flowing to. It must be a member of the multicast VLAN. Receiver – The port where listening host is connected to the switch. It must not be a member of the multicast VLAN. None – The port is not an MVR port.
Status	The active state of the interface, which can be one of the following: Active – The port has link up and is in the forwarding state. Inactive – The port may not have link up, not be in the forwarding state, or both. The interface VLAN information is also displayed as part of the status and can be one of the following: In VLAN – Interface is a member of one or more VLANs. Not In VLAN – Interface is not a member of any VLAN.
Immediate Leave	The MVR immediate leave mode on the interface. It can only be configured on the receiver ports. MVR handles IGMP Leaves in

	Normal or Immediate leave mode. When a Leave message is received, in the normal mode a general IGMP query is sent from the switch to the receiver port, whereas in the immediate leave mode the switch is immediately reconfigured not to forward specific multicast stream to the receiver port. The immediate leave mode is used for ports where only one client may be connected.

4.1.9.4 Statistics

This page shows statistical information about IGMP packets intercepted by MVR.



MVR Statistics

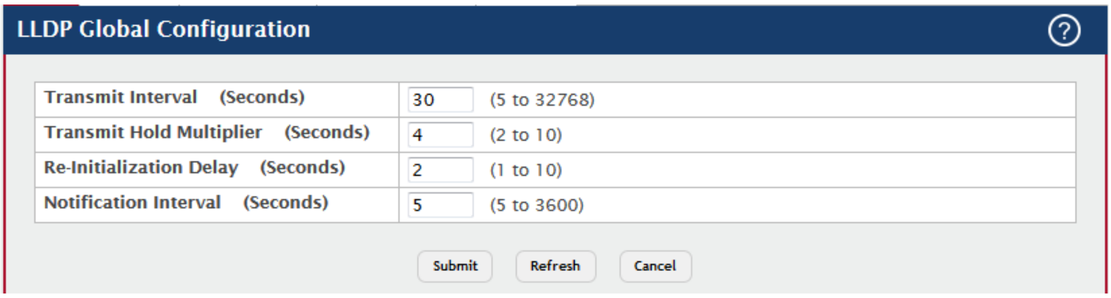
Statistics	Transmit	Receive
IGMP Queries	0	0
IGMPv1 Reports	0	0
IGMPv2 Reports	0	0
IGMP Leaves	0	0
Packet Failures	0	0

Field	Description
IGMP Queries	The total number of IGMP Queries successfully transmitted or received by the processor.
IGMPv1 Reports	The total number of IGMPv1 Reports successfully transmitted or received by the processor.
IGMPv2 Reports	The total number of IGMPv2 Reports successfully transmitted or received by the processor.
IGMP Leaves	The total number of IGMP Leaves successfully transmitted or received by the processor.
Packet Failures	The total number of packets which failed to get transmitted or received by the processor.

4.1.10 LLDP

4.1.10.1 Global

Use this page to set the global Link Layer Discovery Protocol (LLDP) timers. LLDP is defined by the IEEE 802.1AB standard and allows the device to advertise major capabilities and physical descriptions. This information can help you identify system topology and detect bad configurations on the LAN. All time intervals are expressed in seconds.



LLDP Global Configuration

Transmit Interval (Seconds)	30	(5 to 32768)
Transmit Hold Multiplier (Seconds)	4	(2 to 10)
Re-Initialization Delay (Seconds)	2	(1 to 10)
Notification Interval (Seconds)	5	(5 to 3600)

Field	Description
Transmit Interval	The number of seconds between transmissions of LLDP advertisements.
Transmit Hold Multiplier	The Transmit Interval multiplier value, where Transmit Hold Multiplier × Transmit Interval = the time to live (TTL) value the device advertises to neighbors.
Re-Initialization Delay	The number of seconds to wait before attempting to reinitialize LLDP on a port after the LLDP operating mode on the port changes.
Notification Interval	The minimum number of seconds to wait between transmissions of remote data change notifications to the SNMP trap receiver(s) configured on the device.

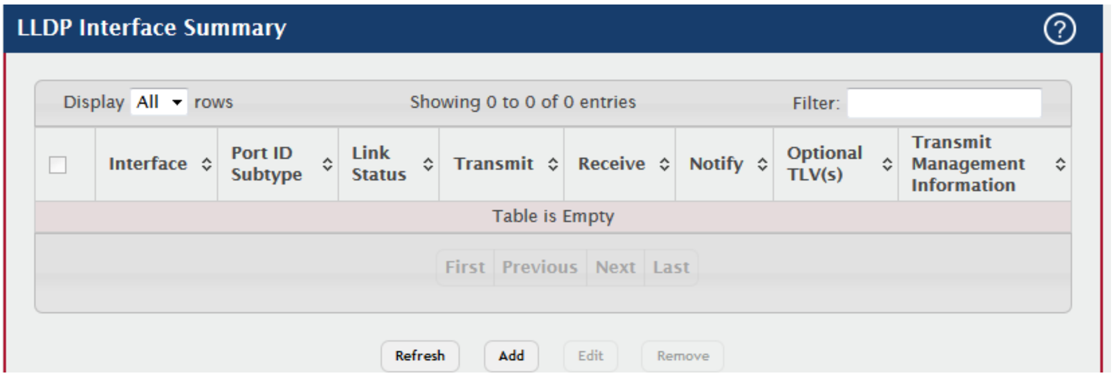
4.1.10.2 Interface

Use this page to view and configure the Link Layer Discovery Protocol (LLDP) - 802.1AB settings for each interface. The table shows entries only for interfaces that have at least one LLDP setting enabled. LLDP uses LLDP Data Units (LLDPDUs) to advertise information about the device and its interfaces. The information is advertised as type-length-value (TLV) elements. Each LLDPDU includes four mandatory TLVs and can also include optional TLVs. The mandatory TLVs are Chassis ID, Port ID, Time-to-Live, and end of LLDPDU.

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**.

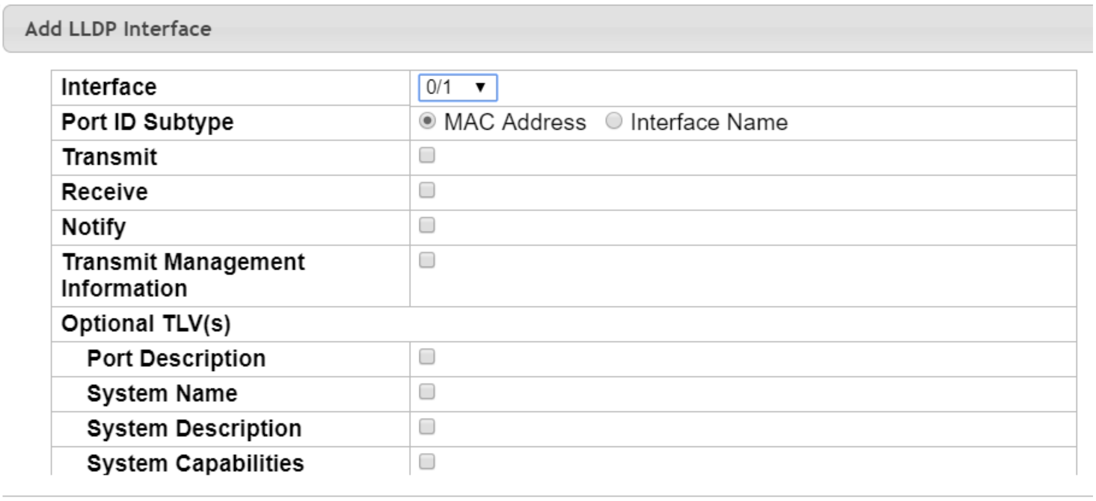
Note: When adding or editing LLDP settings on an interface, select the appropriate check box to enable a feature, or clear the check box to disable a feature.



LLDP Interface Summary

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Interface	Port ID Subtype	Link Status	Transmit	Receive	Notify	Optional TLV(s)	Transmit Management Information
Table is Empty								



Add LLDP Interface

Interface	0/1 ▾
Port ID Subtype	● MAC Address ○ Interface Name
Transmit	□
Receive	□
Notify	□
Transmit Management Information	□
Optional TLV(s)	
Port Description	□
System Name	□
System Description	□
System Capabilities	□

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)

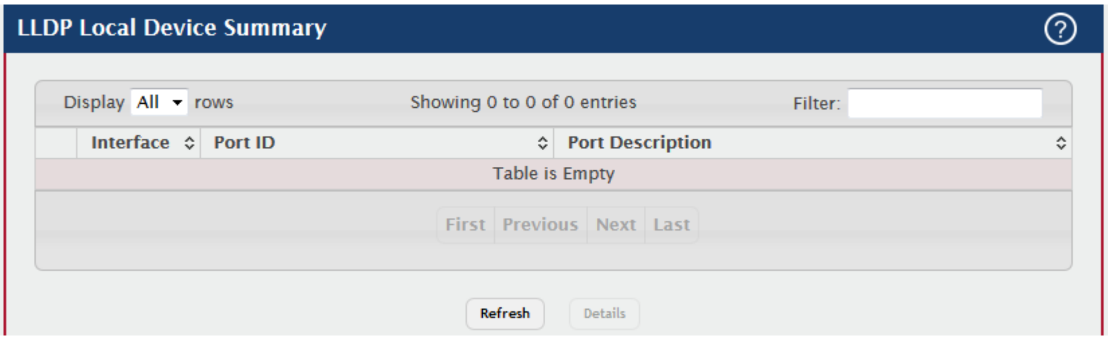
	that advertise the mandatory TLVs and any optional TLVs that are enabled.
Receive	The LLDP receive mode on the interface. If the receive mode is enabled, the device can receive LLDPDUs from other devices.
Notify	The LLDP remote data change notification status on the interface. If the notify mode is enabled, the interface sends SNMP notifications when a link partner device is added or removed.
Optional TLV(s)	Indicates which optional LLDP TLV(s) are included in the LLDPDUs that the interface transmits: 0 – Port Description 1 – System Name 2 – System Description 3 – System Capabilities
Transmit Management Information	Indicates whether management address information for the local device is transmitted in LLDPDUs. Other remote managers can obtain information about the device by using its advertised management address.

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.

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.

4.1.10.3 Local Devices

This page displays summary information about the Link Layer Discovery Protocol (LLDP) data each interface advertises in the LLDP data units (LLDPDUs) it transmits. An interface appears in the table only if its LLDP transmit setting is enabled. To view additional LLDP information that the interface advertises, select the interface with the information to view and click Details.



Interface	Port ID	Port Description
Table is Empty		

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.

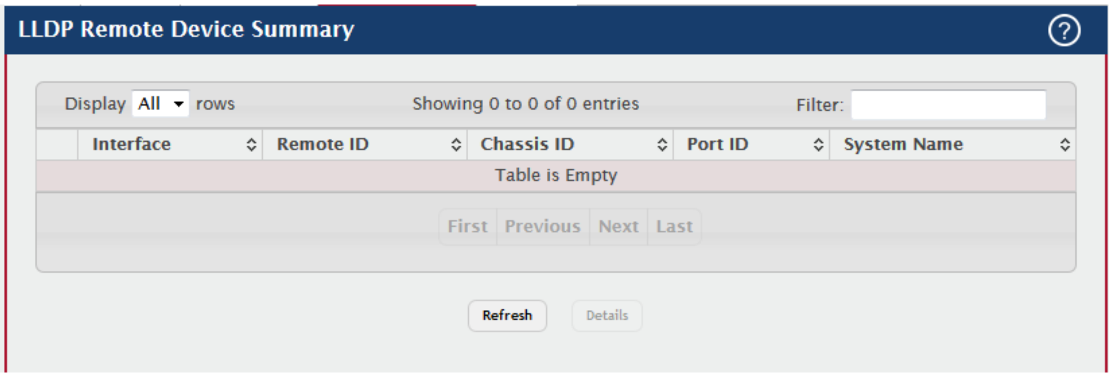
After you click Details, a window opens and displays additional information about the data the interface transmits in its LLDPDUs. The following information describes the additional fields that appear in the LLDP Local Device Information window.

Field	Description
Chassis ID Subtype	The type of information used to identify the device in the Chassis ID field.
Chassis ID	The hardware platform identifier for the device.
Port ID Subtype	The type of information used to identify the interface in the Port ID field.
System Name	The user-configured system name for the device. The system name is configured on the System Description page and is the SNMP server name for the device.
System Description	The device description, which includes information about the product model and platform.
System	The primary function(s) the device supports.

Capabilities Supported	
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.

4.1.10.4 Remote Devcies

This page displays information about the remote devices the local system has learned about through the Link Layer Discovery Protocol (LLDP) data units received on its interfaces. The table lists all interfaces that are enabled to receive LLDP data from remote devices. However, information is available about remote devices only if the interface receives an LLDP data unit (LLDPDU) from a device. To view additional information about a remote device, select the interface that received the LLDP data and click Details.



LLDP Remote Device Summary

Display All rows   Showing 0 to 0 of 0 entries   Filter:

Interface	Remote ID	Chassis ID	Port ID	System Name
Table is Empty				

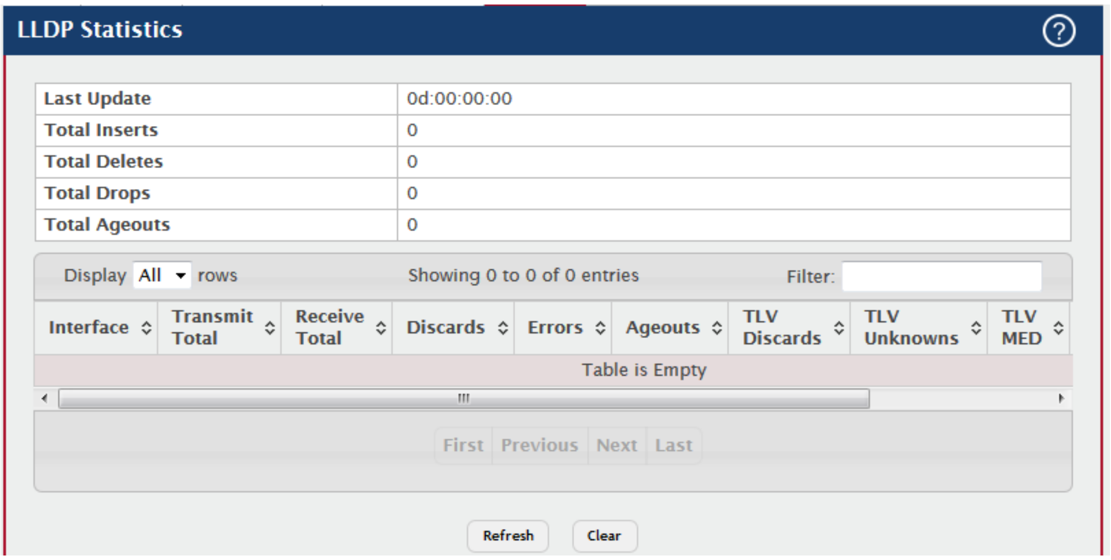
Field	Description
Interface	The local interface that is enabled to receive LLDPDUs from remote devices.
Remote ID	The client identifier assigned to the remote system that sent the LLDPDU.
Chassis ID	The information the remote device sent as the Chassis ID TVL. This identifies the hardware platform for 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.

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.

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.

4.1.10.5 Statistics

This page displays statistical information about the Link Layer Discovery Protocol (LLDP) Data Units (LLDPDUs) the interfaces on the local device have sent and received. The table that shows per-interface statistics contains entries only for interfaces that have at least one LLDP setting enabled.



LLDP Statistics

Last Update	0d:00:00:00
Total Inserts	0
Total Deletes	0
Total Drops	0
Total Ageouts	0

Display All rows Showing 0 to 0 of 0 entries Filter:

Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV Unknowns	TLV MED
Table is Empty								

Field	Description
Last Update	The amount of time that has passed since an entry was created, modified, or deleted in the local database that maintains LLDP information received from remote systems.
Total Inserts	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Total Deletes	The number of times the complete set of information advertised by a particular MSAP has been deleted from tables associated with the remote systems.
Total Drops	The number of times the complete set of information advertised by a particular MSAP could not be entered into tables associated with the remote systems because of insufficient resources.
Total Ageouts	The number of times the complete set of information advertised by a particular MSAP has been deleted from tables associated with the remote systems because the information timeliness interval has expired.
Interface	The interface associated with the rest of the data in the row.
Transmit Total	The number of LLDPDUs transmitted by the LLDP agent on the interface.
Receive Total	The number of valid LLDPDUs received by this interface while the LLDP agent is enabled.
Discards	The number of LLDP TLVs discarded for any reason by the LLDP agent on the interface.

Errors	The number of invalid LLDPDUs received by the LLDP agent on the interface while the LLDP agent is enabled.
Ageouts	The number of age-outs that have occurred on the interface. An age-out occurs the complete set of information advertised by a particular MSAP has been deleted from tables associated with the remote entries because the information timeliness interval had expired.
TLV Discards	The number of LLDP TLVs discarded for any reason by the LLDP agent on the interface.
TLV Unknowns	The number of LLDP TLVs received on the interface that were not recognized by the LLDP agent.
TLV MED	The total number of LLDP-MED TLVs received on the interface.
TLV 802.1	The total number of LLDP TLVs received on the interface which are of type 802.1.
TLV 802.3	The total number of LLDP TLVs received on the interface which are of type 802.3.
Clear (Button)	Resets all LLDP statistics counters to 0.

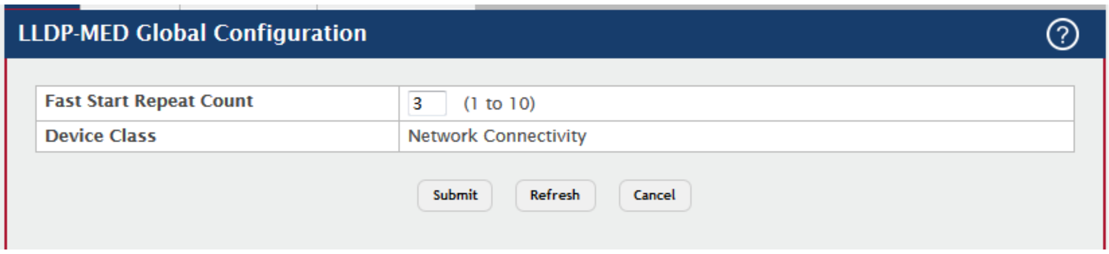
4.1.11 LLDP-MED

4.1.11.1 Global

Use this page to configure the global Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) settings on the device. LLDP-MED is an enhancement to LLDP that enables:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and DiffServ settings), enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet (PoE) 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 uses LLDP's organizationally-specific Type- Length-Value (TLV) extensions and defines new TLVs that make it easier for a VoIP deployment in a wired or wireless LAN/MAN environment. It also makes mandatory a few optional TLVs from LLDP and recommends not transmitting some TLVs.



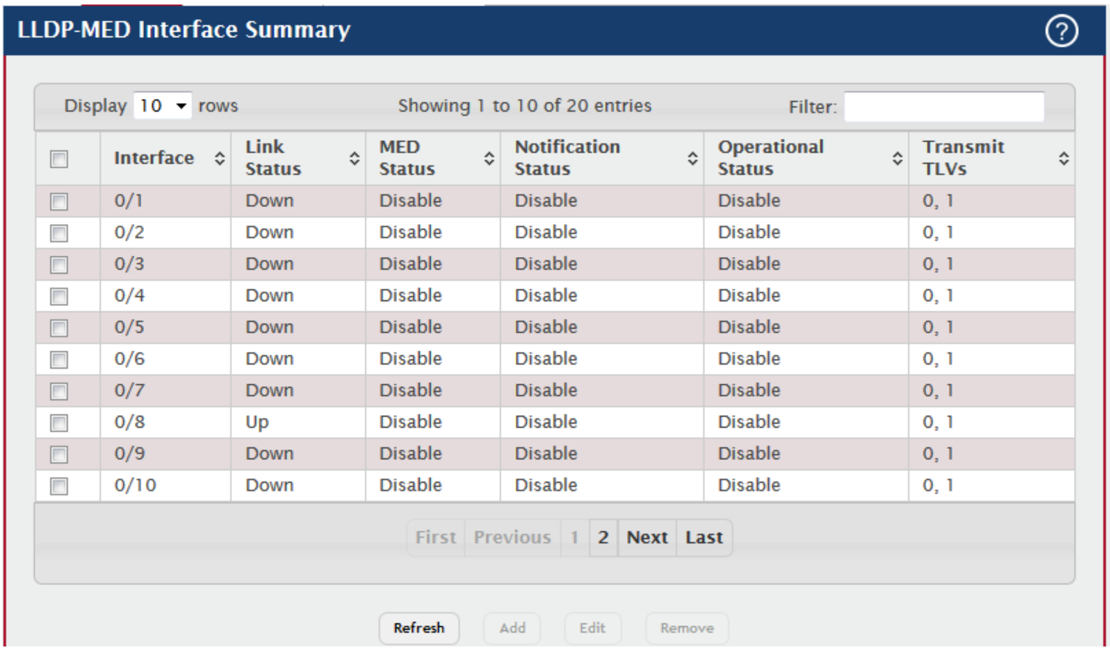
LLDP-MED Global Configuration

Fast Start Repeat Count	3 (1 to 10)
Device Class	Network Connectivity

Field	Description
Fast Start Repeat Count	The number of LLDP-MED Protocol Data Units (PDUs) that will be transmitted when the protocol is enabled.
Device Class	The device's MED Classification. 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.

4.1.11.2 Interface

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.

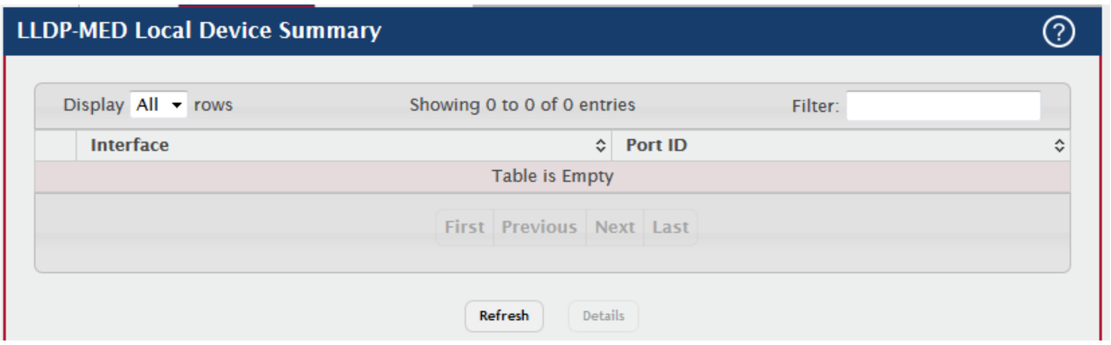

LLDP-MED Interface Summary
?
Display 10 rows
Showing 1 to 10 of 20 entries
Filter:
First Previous 1 2 Next Last
Refresh
Add
Edit
Remove

□	Interface	Link Status	MED Status	Notification Status	Operational Status	Transmit TLVs
□	0/1	Down	Disable	Disable	Disable	0, 1
□	0/2	Down	Disable	Disable	Disable	0, 1
□	0/3	Down	Disable	Disable	Disable	0, 1
□	0/4	Down	Disable	Disable	Disable	0, 1
□	0/5	Down	Disable	Disable	Disable	0, 1
□	0/6	Down	Disable	Disable	Disable	0, 1
□	0/7	Down	Disable	Disable	Disable	0, 1
□	0/8	Up	Disable	Disable	Disable	0, 1
□	0/9	Down	Disable	Disable	Disable	0, 1
□	0/10	Down	Disable	Disable	Disable	0, 1

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring LLDP-MED settings, this field identifies the interfaces that are being configured.
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: Capabilities : 0 Network Policy : 1

4.1.11.3 Local Devices

This page displays information about the LLPD-MED information advertised on the local interfaces that are enabled for LLDP-MED. To view additional LLDP-MED information for a local interface, select the interface with the information to view and click Details.



LLDP-MED Local Device Summary

Display All rows   Showing 0 to 0 of 0 entries   Filter:

Interface	Port ID
Table is Empty	

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.

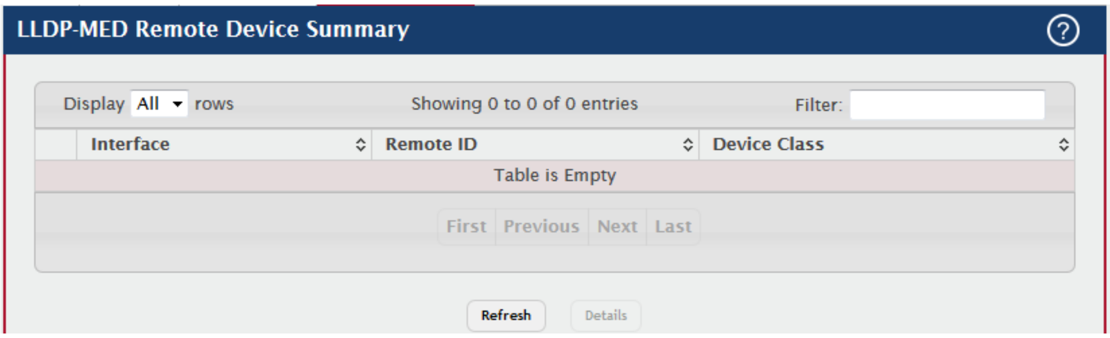
After you click Details, a window opens and shows detailed information about the LLDP-MED information the selected interface transmits. The following information describes the additional fields that appear in the LLDP-MED Local Device Information window.

Field	Description
Network Policy Information	
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	The unknown bit associated with a particular policy type.

Status	
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.

4.1.11.4 Remote Devices

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.



LLDP-MED Remote Device Summary

Display All rows Showing 0 to 0 of 0 entries Filter:

Interface	Remote ID	Device Class
Table is Empty		

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	The supported capabilities on the remote device that are also

Capabilities	enabled.
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	
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	
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	
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.

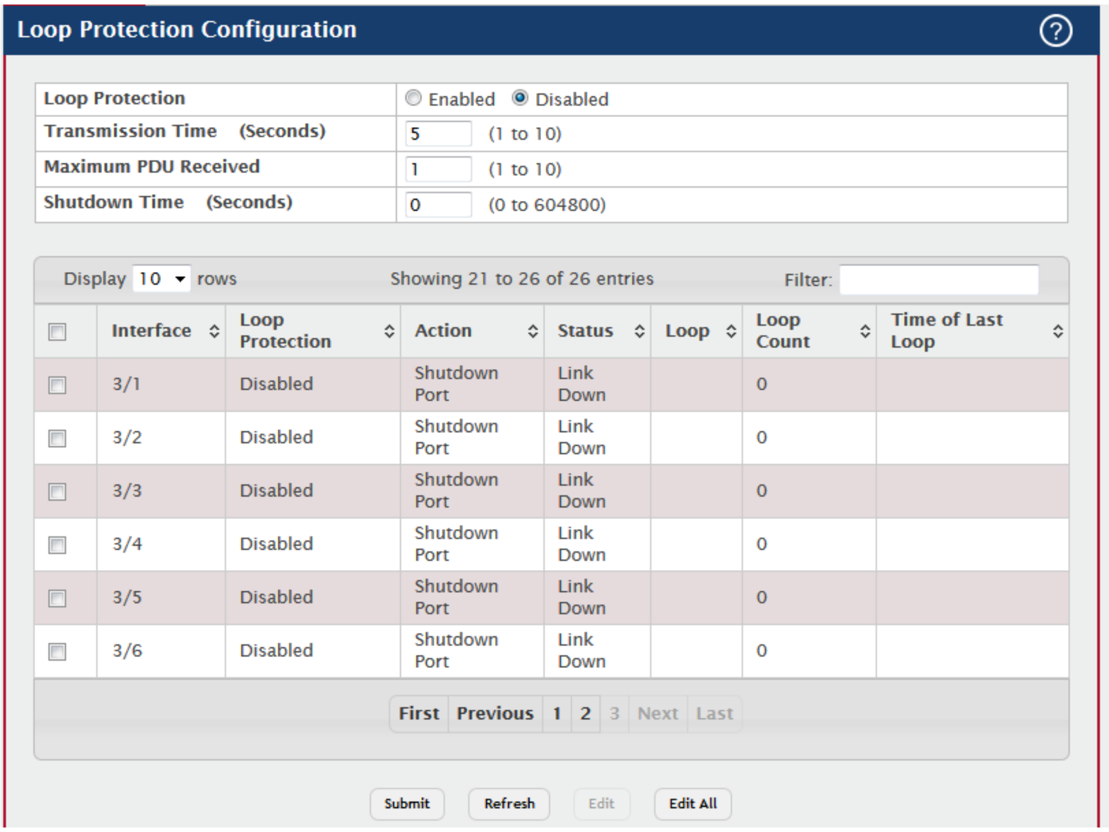
4.1.12 Loop Protection

4.1.12.1 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 configure Loop Protection settings on interfaces, 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.



Loop Protection Configuration

Loop Protection	○ Enabled ● Disabled
Transmission Time (Seconds)	5 (1 to 10)
Maximum PDU Received	1 (1 to 10)
Shutdown Time (Seconds)	0 (0 to 604800)

Display 10 rows Showing 21 to 26 of 26 entries Filter:

□	Interface	Loop Protection	Action	Status	Loop	Loop Count	Time of Last Loop
□	3/1	Disabled	Shutdown Port	Link Down		0	
□	3/2	Disabled	Shutdown Port	Link Down		0	
□	3/3	Disabled	Shutdown Port	Link Down		0	
□	3/4	Disabled	Shutdown Port	Link Down		0	
□	3/5	Disabled	Shutdown Port	Link Down		0	
□	3/6	Disabled	Shutdown Port	Link Down		0	

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.
Shutdown Time (Seconds)	The period that a port is shut down when a loop is detected.
Interface	The port or trunk ID.
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.

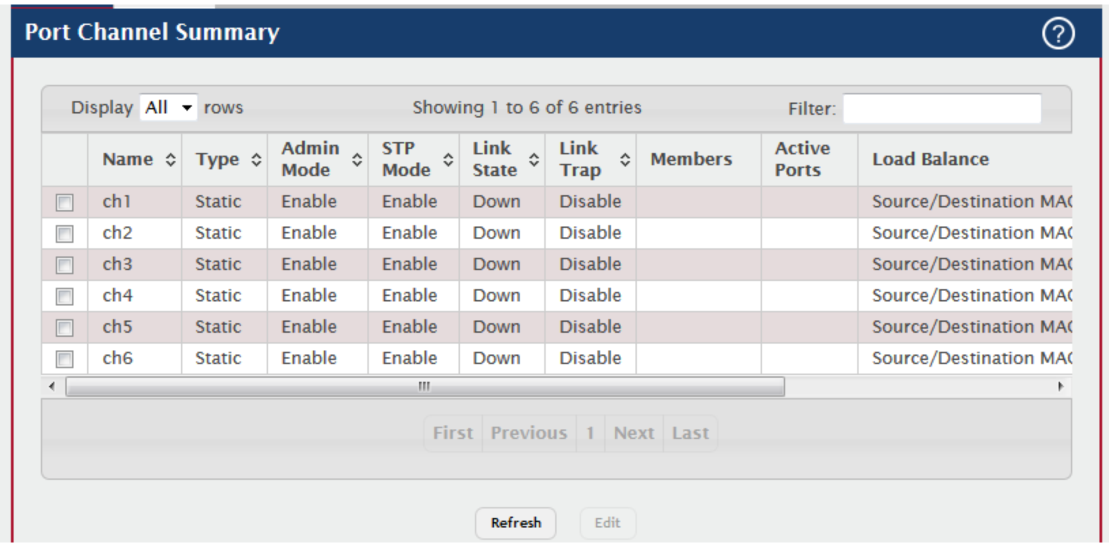
	Log Only: Send a message to the system log but do not shut down the port.
Status	The current status of the interface. Link Up indicates the interface is operating normally. Link Down indicates that the port has been shut down due to the detection of a loop.
Loop	Indicates whether a loop is currently 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.

4.1.13 Port Channel

4.1.13.1 Summary

Use this page to view and manage port channels on the device. 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. This allows the device to treat the port channel as a single, logical link. The primary purpose of a port channel is to increase the bandwidth between two devices. Port channels can also provide redundancy.

To add or remove member ports or to change other port channel settings, select the port channel to configure and click Edit.



Port Channel Summary

Display All rows Showing 1 to 6 of 6 entries Filter:

	Name	Type	Admin Mode	STP Mode	Link State	Link Trap	Members	Active Ports	Load Balance
□	ch1	Static	Enable	Enable	Down	Disable			Source/Destination MA(
□	ch2	Static	Enable	Enable	Down	Disable			Source/Destination MA(
□	ch3	Static	Enable	Enable	Down	Disable			Source/Destination MA(
□	ch4	Static	Enable	Enable	Down	Disable			Source/Destination MA(
□	ch5	Static	Enable	Enable	Down	Disable			Source/Destination MA(
□	ch6	Static	Enable	Enable	Down	Disable			Source/Destination MA(

Field	Description
Name	A unique name to identify the port channel. Depending on the type of

	port channel, this name is automatically assigned by the system or can be configured by a system administrator.
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.

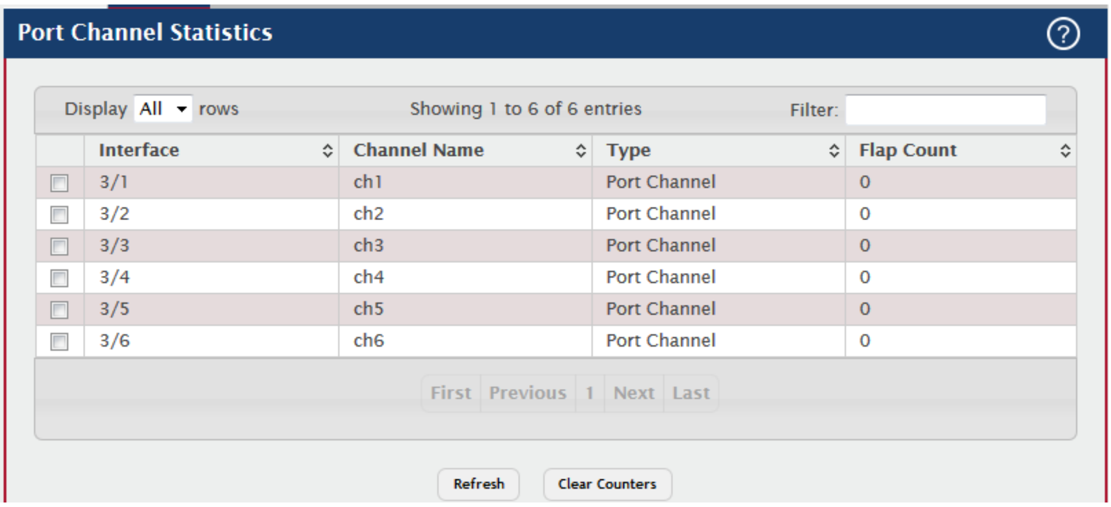
When configuring a port channel, use the Static Mode field to set the port channel type. If the Static Mode is disabled, the port channel type is Dynamic.

Field	Description
Admin Mode	The administrative mode of the port channel. When disabled, the port channel does not send and receive traffic.
STP Mode	The spanning tree protocol (STP) mode of the port channel. When enabled, the port channel participates in the STP operation to help prevent network loops.
Link State	The current link status of the port channel, which can be Up, Up (SFP), or Down.
Link Trap	The link trap mode of the port channel. When enabled, a trap is sent to any configured SNMP receiver(s) when the link state of the port channel changes.
Members	The ports that are members of a port channel. Each port channel can have a maximum of 8 member ports. To add ports to the port channel, select one or more ports from the Port List field (CTRL + click to select multiple ports). Then, use the appropriate arrow icon to move the selected ports to the Members field.
Active Ports	The ports that are actively participating members of a port channel. A member port that is operationally or administratively disabled or does not have a link is not an active port.
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

4.1.13.2 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.



Port Channel Statistics

Display All rows Showing 1 to 6 of 6 entries Filter:

	Interface	Channel Name	Type	Flap Count
□	3/1	ch1	Port Channel	0
□	3/2	ch2	Port Channel	0
□	3/3	ch3	Port Channel	0
□	3/4	ch4	Port Channel	0
□	3/5	ch5	Port Channel	0
□	3/6	ch6	Port Channel	0

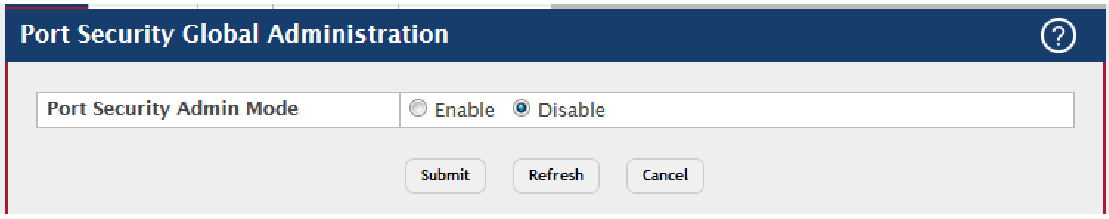
Field	Description
Interface	The port channel or member port (physical port) associated with the rest of the data in the row.
Channel Name	The port channel name associated with the port channel. For a physical port, this field identifies the name of the port channel of which the port is a member.
Type	The interface type, which is either Port Channel (logical link-aggregation group) or Member Port (physical port).
Flap Count	The number of times the interface has gone down. The counter for a member port is incremented when the physical port is either manually shut down by the administrator or when its link state is down. When a port channel is administratively shut down, the flap counter for the port channel is incremented, but the flap counters for its member ports are not affected. When all active member ports for a port channel are inactive (either administratively down or link down), then the port

	channel flap counter is incremented.
Clear Counters (Button)	Click this button to reset the flap counters for all port channels and member ports to 0.

4.1.14 Port Security

4.1.14.1 Global

Use this page to configure the global administrative mode for the port security feature. Port security, which is also known as port MAC locking, allows you to limit the number of source MAC address that can be learned on a port. If a port 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. Port security can help secure the network by preventing unknown devices from forwarding packets into the network.


Port Security Global Administration

Port Security Admin Mode ○ Enable ● Disable

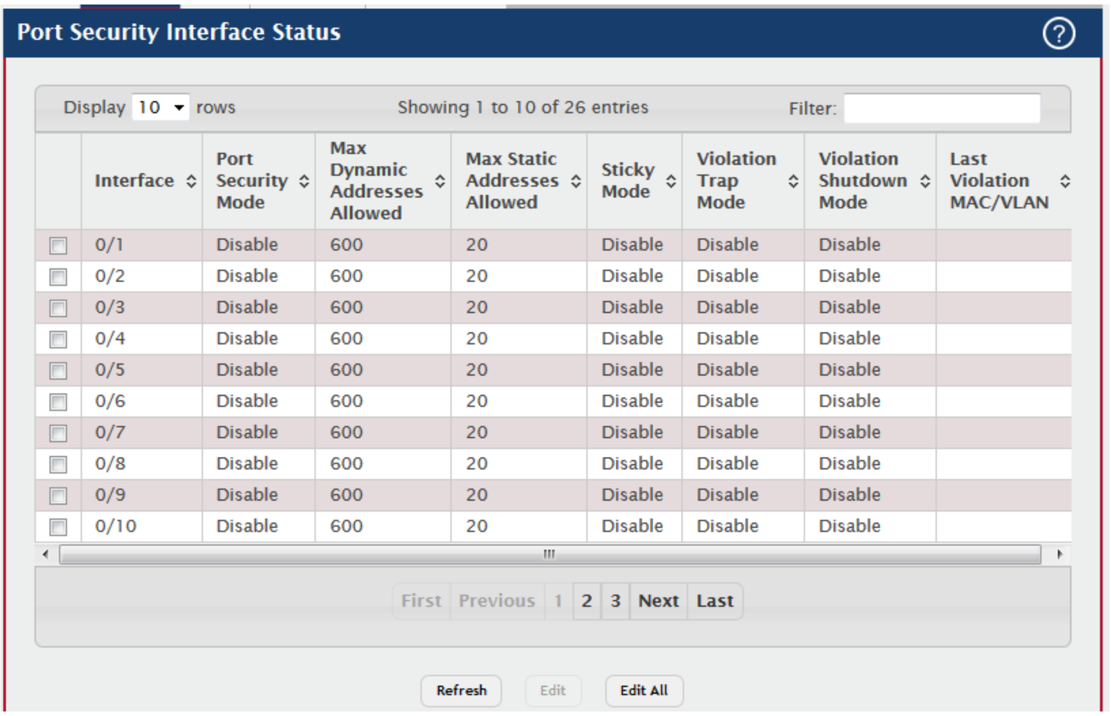
Field	Description
Port Security Admin Mode	Enable or disable the global administrative mode for port security. The port security mode must be enabled both globally and on an interface to enforce the configured limits for the number of static and dynamic MAC addresses allowed on that interface.

4.1.14.2 Interface

Use this page to view and configure the port security settings for each interface.

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.**



Port Security Interface Status

Display 10 rows Showing 1 to 10 of 26 entries Filter:

	Interface	Port Security Mode	Max Dynamic Addresses Allowed	Max Static Addresses Allowed	Sticky Mode	Violation Trap Mode	Violation Shutdown Mode	Last Violation MAC/VLAN
□	0/1	Disable	600	20	Disable	Disable	Disable	
□	0/2	Disable	600	20	Disable	Disable	Disable	
□	0/3	Disable	600	20	Disable	Disable	Disable	
□	0/4	Disable	600	20	Disable	Disable	Disable	
□	0/5	Disable	600	20	Disable	Disable	Disable	
□	0/6	Disable	600	20	Disable	Disable	Disable	
□	0/7	Disable	600	20	Disable	Disable	Disable	
□	0/8	Disable	600	20	Disable	Disable	Disable	
□	0/9	Disable	600	20	Disable	Disable	Disable	
□	0/10	Disable	600	20	Disable	Disable	Disable	

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the port security settings for one or more interfaces, this field lists the interfaces that are being configured.
Port Security Mode	The administrative mode of the port security feature on the interface. The port security mode must be enabled both globally and on an interface to enforce the configured limits for the number of static and dynamic MAC addresses allowed on that interface.
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.
Max Static Addresses Allowed	The number of source MAC addresses that can be manually added to the port security MAC address table for an interface. If the port link goes down, the statically configured MAC addresses remain in the

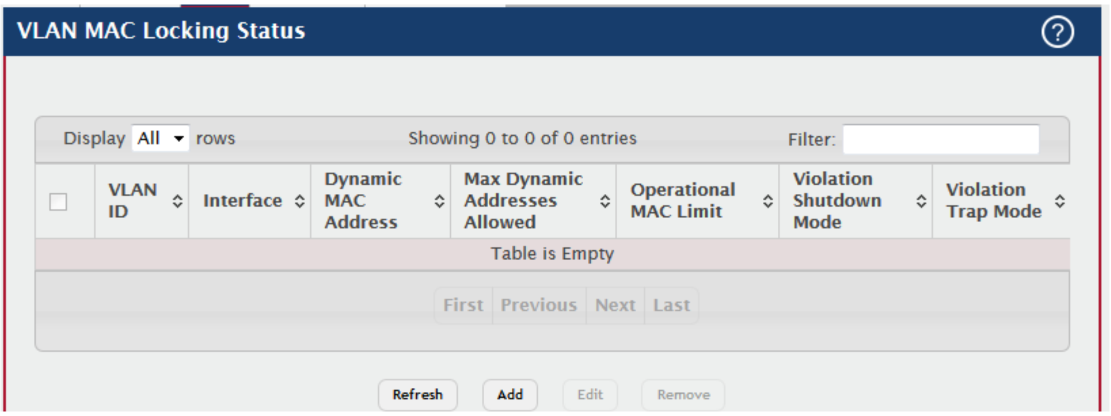
	MAC address table. The maximum number includes all dynamically-learned MAC addresses that have been converted to static MAC addresses.
Sticky Mode	The sticky MAC address learning mode, which is one of the following: **Enabled** – MAC addresses learned or manually configured on this interface are learned in sticky mode. A sticky-mode MAC address is a MAC address that does not age out and is added to the running configuration. If the running configuration is saved to the startup configuration, the sticky addresses are saved to persistent storage and do not need to be relearned when the device restarts. Upon enabling sticky mode on an interface, all dynamically learned MAC addresses in the MAC address table for that interface are converted to sticky mode. Additionally, new addresses dynamically learned on the interface will also become sticky. **Disabled** – When a link goes down on a port, all of the dynamically learned addresses are cleared from the source MAC address table the feature maintains. When the link is restored, the interface can once again learn addresses up to the specified limit. If sticky mode is disabled after being enabled on an interface, the sticky-mode addresses learned or manually configured on the interface are converted to dynamic entries and are automatically removed from persistent storage.
Violation Trap Mode	Indicates whether the port security feature sends a trap to the SNMP agent when a port is locked and a frame with a MAC address not currently in the table arrives on the port. A port is considered to be locked once it has reached the maximum number of allowed dynamic or static MAC address entries in the port security MAC address table.
Violation Shutdown Mode	Indicates whether the port security feature shuts down the port after MAC limit is reached.
Last Violation MAC/VLAN	The source MAC address and, if applicable, associated VLAN ID of the last frame that was discarded at a locked port.

4.1.14.3 VLAN

VLAN MAC Locking allows a network administrator 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.

To configure The VLAN MAC Locking, use the following buttons to perform the tasks:

- Use **Submit** button to enable or disable VLAN MAC Locking Admin Mode.
- Use **Add** button to configure VLANs.
- Use **Edit** button to modify configuration parameters of VLAN MAC Locking.
- Use **Remove** button to remove configured VLANs.



VLAN MAC Locking Status

Display All rows   Showing 0 to 0 of 0 entries   Filter:

□	VLAN ID	Interface	Dynamic MAC Address	Max Dynamic Addresses Allowed	Operational MAC Limit	Violation Shutdown Mode	Violation Trap Mode
Table is Empty							

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.
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	After MAC limit has reached, a log message will be generated with

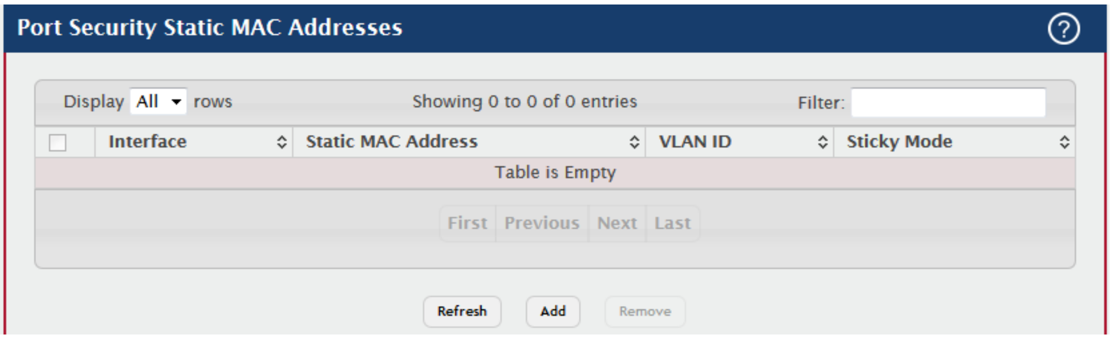
Mode	violation MAC address details.

4.1.14.4 Static MAC

Use this page to add and remove the MAC addresses of hosts that are allowed to send traffic to specific interfaces on the device. The number of MAC addresses you can associate with each interface is determined by the maximum static MAC addresses allowed on a given interface.

Use the buttons to perform the following tasks:

- To associate a static MAC address with an interface, click **Add** and configure the settings in the available fields.
- To remove one or more configured static MAC address entries, select each entry to delete and click **Remove.** You must confirm the action before the entry is deleted.



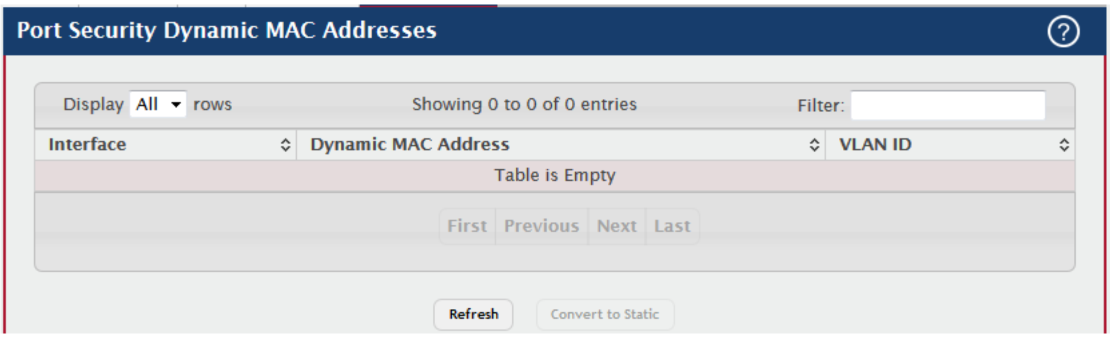
□	Interface	Static MAC Address	VLAN ID	Sticky Mode
		Table is Empty		

Field	Description
Interface	The interface associated with the rest of the data in the row. When adding a static MAC address entry, use the Interface menu to select the interface to associate with the permitted MAC address.
Static MAC Address	The MAC address of the host that is allowed to forward packets on the associated interface.
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.
Sticky Mode	Indicates whether the static MAC address entry is added in sticky mode. When adding a static MAC address entry, the Sticky Mode field can be selected only if it is enabled on the interface. If a static MAC address is added in sticky mode, and sticky mode is disabled on the interface, the MAC address entry is converted to a dynamic entry and will age out and be removed from the running (and saved)

	configuration if it is not relearned.

4.1.14.5 Dynamic MAC

Use this page to view the dynamic MAC address entries that have been learned on each interface. From this page, you can also convert dynamic MAC address entries to static MAC address entries for a given interface. If the limit of statically-locked MAC addresses is less than the number of dynamically-locked MAC addresses to convert, then the addresses are converted in the order in which they were learned until the number of allowed static MAC address entries is reached.



Port Security Dynamic MAC Addresses

Display All rows   Showing 0 to 0 of 0 entries   Filter:

Interface	Dynamic MAC Address	VLAN ID
Table is Empty		

Field	Description
Interface	The interface associated with the rest of the data in the row. When converting dynamic addresses to static addresses, use the Interface menu to select the interface to associate with the MAC addresses.
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.
VLAN ID	The VLAN ID specified in the Ethernet frame received by the interface.
Convert to Static (Button)	Converts all MAC addresses learned on an interface to static MAC address entries. After you click the button, a window opens and allows you to select the interface associated with the MAC address entries to convert. A static MAC address entry is written to the running configuration file and does not age out.

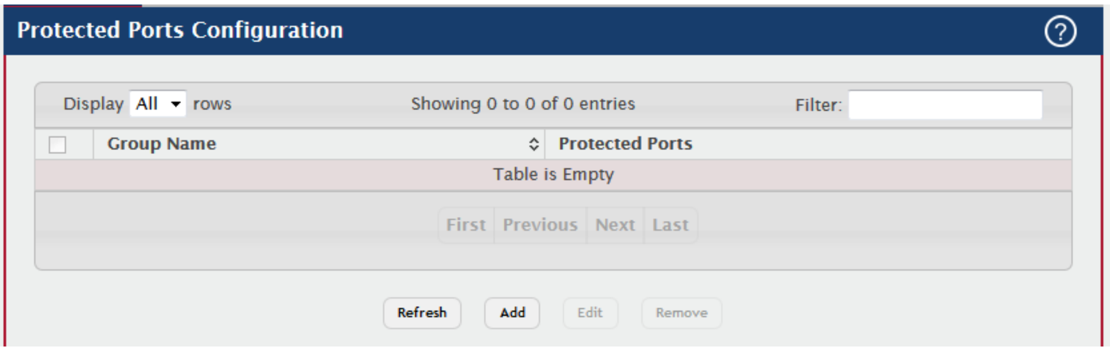
4.1.15 Protected Ports

4.1.15.1 Configuration

Use this page to configure and view protected ports groups. A port that is a member of a protected ports group is a *protected* port. A port that is not a member of any protected ports group is an *unprotected* port. Each port can be a member of only one protected ports group. Ports in the same protected ports group cannot forward traffic to other protected ports within the group, even if they are members of the same VLAN. However, a port in a protected ports group can forward traffic to ports that are in a different protected ports group. A protected port can also forward traffic to unprotected ports. Unprotected ports can forward traffic to both protected and unprotected ports.

Use the buttons to perform the following tasks:

- To create a protected ports group and add ports to the group, click **Add** and configure the settings in the available fields.
- To change the name or the port members for an existing group, select the group to update and click **Edit**.
- To remove one or more protected ports groups, select each entry to delete and click **Remove.**You must confirm the action before the entry is deleted.



Protected Ports Configuration

Display All rows   Showing 0 to 0 of 0 entries   Filter:

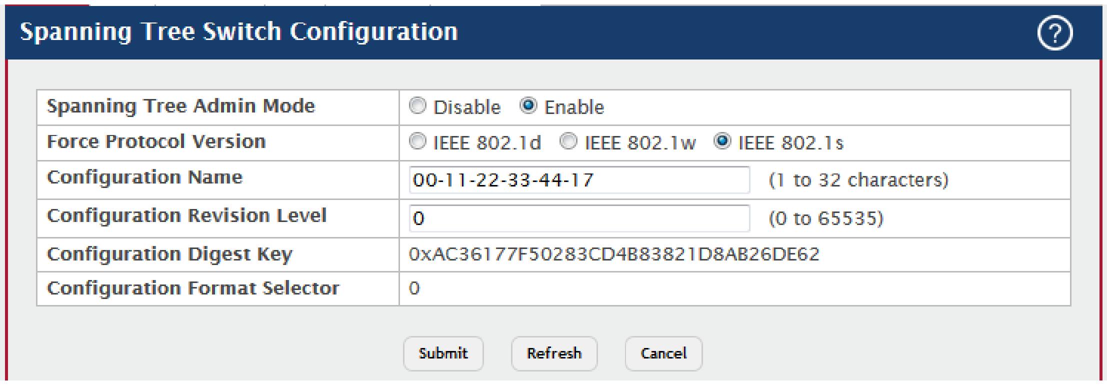
□	Group Name	Protected Ports
	Table is Empty	

Field	Description
Group Name	The user-configured name of the protected ports group.
Protected Ports	The ports that are members of the protected ports group. When adding a port to a protected ports group, the Available Interfaces field lists the ports that are not already members of a protected ports group. To move an interface between the Available Interfaces and Selected Interfaces fields, click the port (or CTRL + click to select multiple ports), and then click the appropriate arrow to move the port(s) to the desired field.

4.1.16 Spanning Tree

4.1.16.1 Switch

Use this page to view and configure global Spanning Tree Protocol (STP) settings for the device. 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. STP uses the spanning-tree algorithm to provide a single path between end stations on a network.



Spanning Tree Switch Configuration

Spanning Tree Admin Mode	○ Disable ● Enable
Force Protocol Version	○ IEEE 802.1d ○ IEEE 802.1w ● IEEE 802.1s
Configuration Name	00-11-22-33-44-17 (1 to 32 characters)
Configuration Revision Level	0 (0 to 65535)
Configuration Digest Key	0xAC36177F50283CD4B83821D8AB26DE62
Configuration Format Selector	0

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	The revision number of the MSTP region. This number must be the

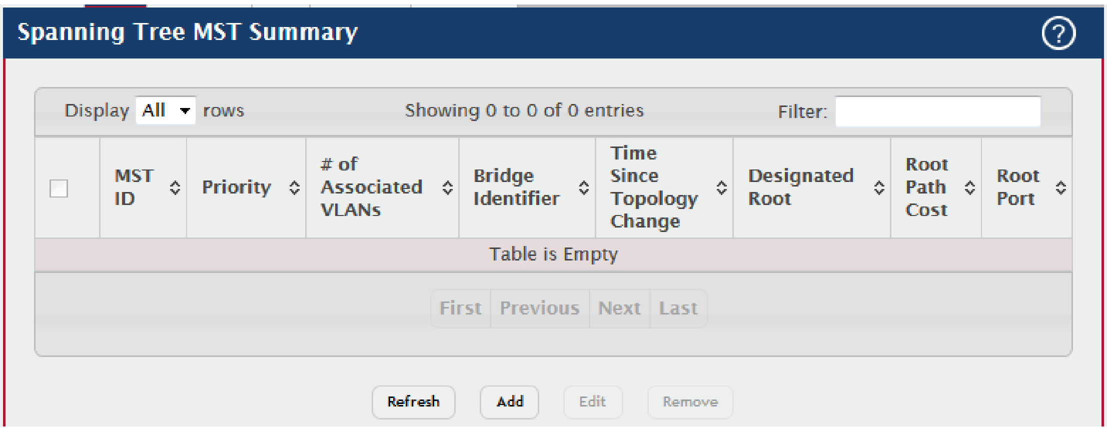
Revision Level	same on all switches that participate in the MSTP region.
Configuration Digest Key	The 16 byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID-to-MST ID mapping).
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.

4.1.16.2 MST

Use this 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.



Spanning Tree MST Summary

Display All rows   Showing 0 to 0 of 0 entries   Filter:

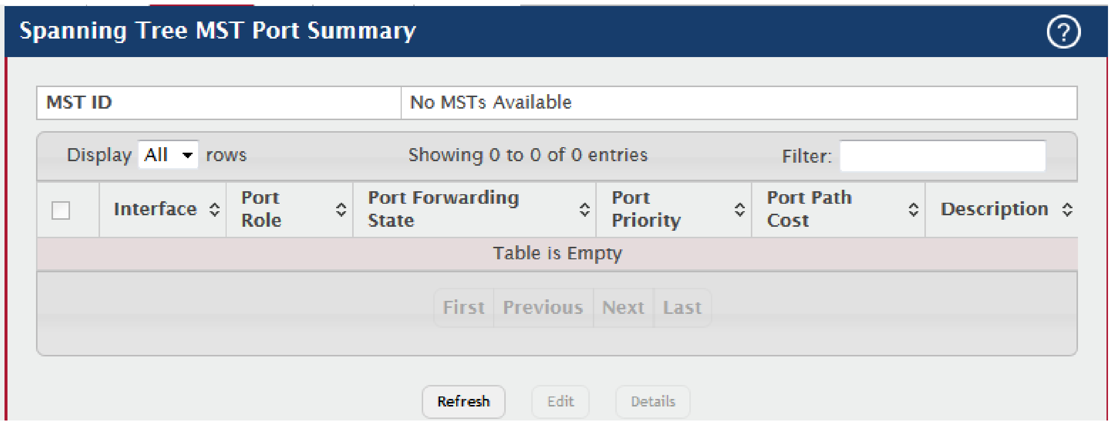
□	MST ID	Priority	# of Associated VLANs	Bridge Identifier	Time Since Topology Change	Designated Root	Root Path Cost	Root Port
Table is Empty								

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	The number of VLANs that are mapped to the MSTI. This number

VLANs	does not contain any information about the VLAN IDs that are mapped to the instance.
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value of the MSTI and the base MAC address of the bridge. When electing the root bridge for an MST instance, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Time Since Topology Change	The amount of time that has passed since the topology of the MSTI has changed.
Designated Root	The bridge identifier of the root bridge for the MST instance. The identifier is made up of the bridge priority and the base MAC address.
Root Path Cost	The path cost to the designated root for this MST instance. Traffic from a connected device to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Root Port	The port on the bridge with the least-cost path to the designated root for the MST instance.

4.1.16.3 MST Port

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.


Spanning Tree MST Port Summary

MST ID: No MSTs Available

Display All rows   Showing 0 to 0 of 0 entries   Filter:

□	Interface	Port Role	Port Forwarding State	Port Priority	Port Path Cost	Description
Table is Empty						

Field	Description
MST ID	The menu contains the ID of each MST instance that has been created on the device.

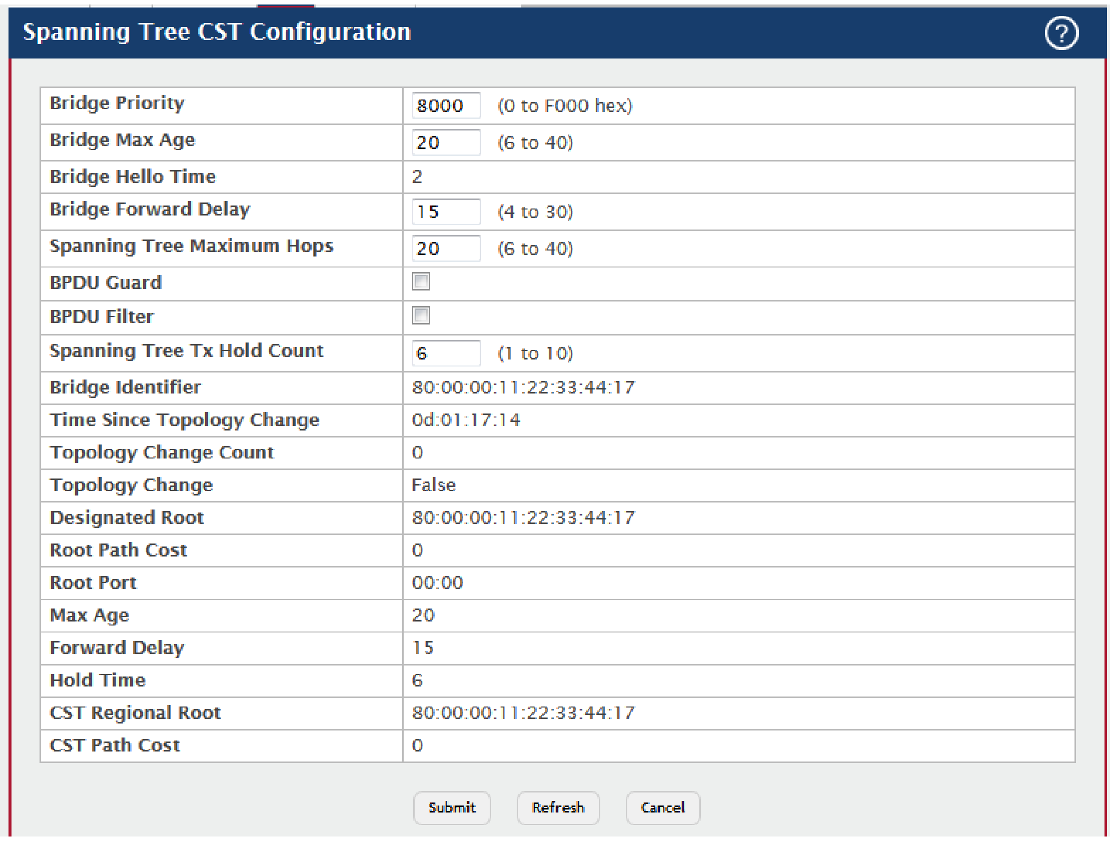
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring MST settings for an interface, this field identifies the interface being configured.
Port Role	Root – A port on the non-root bridge that has the least-cost path to the root bridge. Designated – 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.

Field	Description
Auto-calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Up Time Since Counters Last Cleared	The amount of time that the port has been up since the counters were cleared.
Port Mode	The administrative mode of spanning tree on the port.
Designated Root	The bridge ID of the root bridge for the MST instance.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.
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.

4.1.16.4 CST

Use this 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.



Spanning Tree CST Configuration

Bridge Priority	8000 (0 to F000 hex)
Bridge Max Age	20 (6 to 40)
Bridge Hello Time	2
Bridge Forward Delay	15 (4 to 30)
Spanning Tree Maximum Hops	20 (6 to 40)
BPDU Guard	□
BPDU Filter	□
Spanning Tree Tx Hold Count	6 (1 to 10)
Bridge Identifier	80:00:00:11:22:33:44:17
Time Since Topology Change	0d:01:17:14
Topology Change Count	0
Topology Change	False
Designated Root	80:00:00:11:22:33:44:17
Root Path Cost	0
Root Port	00:00
Max Age	20
Forward Delay	15
Hold Time	6
CST Regional Root	80:00:00:11:22:33:44:17
CST Path Cost	0

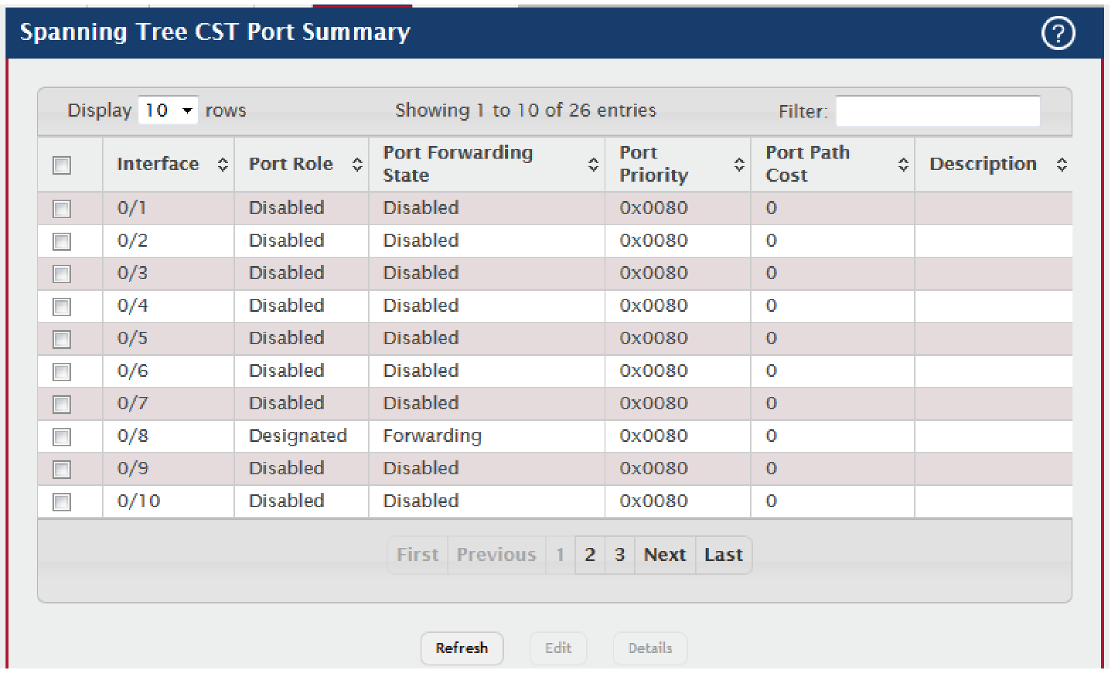
Field	Description
Bridge Priority	The value that helps determine which bridge in the spanning tree is elected as the root bridge during STP convergence. A lower value increases the probability that the bridge becomes the root bridge.
Bridge Max Age	The amount of time a bridge waits before implementing a topological change.
Bridge Hello Time	The amount of time the root bridge waits between sending hello BPDUs.
Bridge Forward Delay	The amount of time a bridge remains in a listening and learning state before forwarding packets.
Spanning Tree Maximum Hops	The maximum number of hops a Bridge Protocol Data Unit (BPDU) is allowed to traverse within the spanning tree region before it is discarded.
BPDU Guard	When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
BPDU Filter	When enabled, this feature filters the BPDU traffic on the edge ports.

	When spanning tree is disabled on a port, BPDU filtering allows BPDU packets received on that port to be dropped.
Spanning Tree Tx Hold Count	The maximum number of BPDUs that a bridge is allowed to send within a hello time window.
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.

4.1.16.5 CST Port

Use this 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.



Spanning Tree CST Port Summary

Display 10 rows   Showing 1 to 10 of 26 entries   Filter:

□	Interface	Port Role	Port Forwarding State	Port Priority	Port Path Cost	Description
□	0/1	Disabled	Disabled	0x0080	0	
□	0/2	Disabled	Disabled	0x0080	0	
□	0/3	Disabled	Disabled	0x0080	0	
□	0/4	Disabled	Disabled	0x0080	0	
□	0/5	Disabled	Disabled	0x0080	0	
□	0/6	Disabled	Disabled	0x0080	0	
□	0/7	Disabled	Disabled	0x0080	0	
□	0/8	Designated	Forwarding	0x0080	0	
□	0/9	Disabled	Disabled	0x0080	0	
□	0/10	Disabled	Disabled	0x0080	0	

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 admini

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.

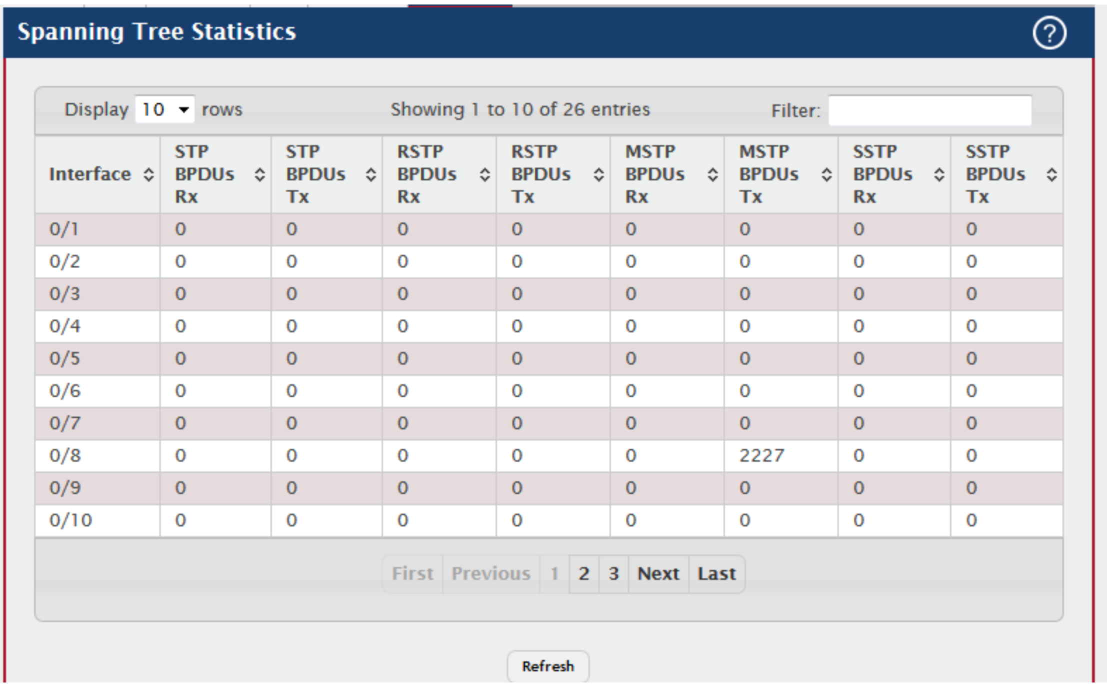
Field	Description
Admin Edge Port	Select this option administratively configure the interface as an edge port. An edge port is an interface that is directly connected to a host and is not at risk of causing a loop.
Auto-calculate Port Path Cost	Shows whether the path cost from the port to the root bridge 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	Shows whether the path cost from the port to the CIST root is automatically determined by the speed of the interface (Enabled) or

Path Cost	configured manually (Disabled).
BPDU Filter	When enabled, this feature filters the BPDU traffic on the edge ports. Edge ports do not need to participate in the spanning tree, so BPDU filtering allows BPDU packets received on edge ports to be dropped.
BPDU Flood	This option determines the behavior of the interface if STP is disabled on the port and the port receives a BPDU. If BPDU flooding is enabled, the port will flood the received BPDU to all the ports on the switch that are similarly disabled for spanning tree.
BPDU Guard Effect	Shows the status of BPDU Guard Effect on the interface. When enabled, BPDU Guard Effect can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Up Time Since Counters Last Cleared	The amount of time that the port has been up since the counters were cleared.
Port Mode	The administrative mode of spanning tree on the port.
Designated Root	The bridge ID of the root bridge for the CST.
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 acknowledgement 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.

4.1.16.6 Statistics

This page displays information about the number of bridge protocol data units (BPDUs) sent and received by each interface for each STP version.



Spanning Tree Statistics

Display 10 rows Showing 1 to 10 of 26 entries Filter:

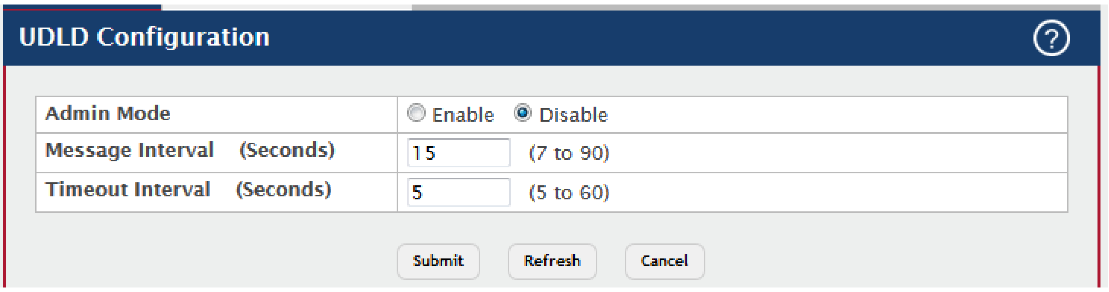
Interface	STP BPDUs Rx	STP BPDUs Tx	RSTP BPDUs Rx	RSTP BPDUs Tx	MSTP BPDUs Rx	MSTP BPDUs Tx	SSTP BPDUs Rx	SSTP BPDUs Tx
0/1	0	0	0	0	0	0	0	0
0/2	0	0	0	0	0	0	0	0
0/3	0	0	0	0	0	0	0	0
0/4	0	0	0	0	0	0	0	0
0/5	0	0	0	0	0	0	0	0
0/6	0	0	0	0	0	0	0	0
0/7	0	0	0	0	0	0	0	0
0/8	0	0	0	0	0	2227	0	0
0/9	0	0	0	0	0	0	0	0
0/10	0	0	0	0	0	0	0	0

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.
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.
SSTP BPDUs Rx	The number of classic SSTP BPDUs received by the interface.
SSTP BPDUs Tx	The number of classic SSTP BPDUs sent by the interface.

4.1.17 UDLD

4.1.17.1 Configuration

Use this page to configure the global Unidirectional Link Detection (UDLD) settings on the device. The UDLD feature detects unidirectional links on physical ports by exchanging packets containing information about neighboring devices. The purpose of the UDLD feature is to detect and avoid unidirectional links. A unidirectional link is a forwarding anomaly in a Layer 2 communication channel in which a bidirectional link stops passing traffic in one direction.



UDLD Configuration

Admin Mode	○ Enable ● Disable
Message Interval (Seconds)	15 (7 to 90)
Timeout Interval (Seconds)	5 (5 to 60)

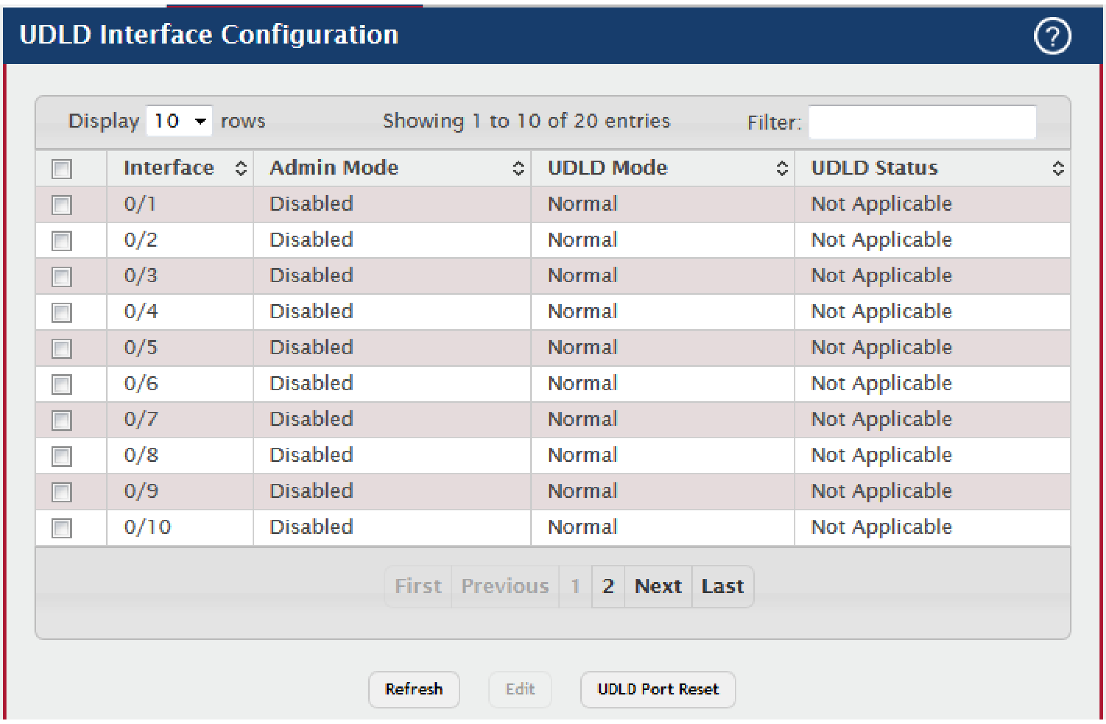
Field	Description
Admin Mode	The administrative mode of UDLD on the device. UDLD must be administratively enabled on the device and on an interface for that interface to send UDLD messages. Additionally, UDLD must be enabled on the both sides of the link for the device to detect a unidirectional link.
Message Interval (Seconds)	The amount of time to wait between sending UDLD probe messages on ports that are in the advertisement phase.
Timeout Interval (Seconds)	The amount of time to wait to receive a UDLD message before considering the UDLD link to be unidirectional.

4.1.17.2 Interface Configuration

Use this page to configure the per-port UDLD settings.

Use the buttons to perform the following tasks:

- To configure UDLD settings for one or more interfaces, select each interface to configure and click **Edit**. The same settings are applied to all selected interfaces.
- To reset all UDLD ports that have a UDLD Status of Shutdown, click **UDLD Port Reset**. If the global and interface UDLD administrative mode is enabled and the port link is up, the port restarts the exchange of UDLD messages with its link partner. The UDLD port status is Shutdown if UDLD has detected an unidirectional link and has put the port in a disabled state.



UDLD Interface Configuration

Display 10 rows   Showing 1 to 10 of 20 entries   Filter:

□	Interface	Admin Mode	UDLD Mode	UDLD Status
□	0/1	Disabled	Normal	Not Applicable
□	0/2	Disabled	Normal	Not Applicable
□	0/3	Disabled	Normal	Not Applicable
□	0/4	Disabled	Normal	Not Applicable
□	0/5	Disabled	Normal	Not Applicable
□	0/6	Disabled	Normal	Not Applicable
□	0/7	Disabled	Normal	Not Applicable
□	0/8	Disabled	Normal	Not Applicable
□	0/9	Disabled	Normal	Not Applicable
□	0/10	Disabled	Normal	Not Applicable

Field	Description
Interface	The interface associated with the rest of the data in the row. In the Edit UDLD Interface Configuration window, this field identifies each interface that is being configured.
Admin Mode	The administrative mode of UDLD on the port.
UDLD Mode	The UDLD mode for the port, which is one of the following: Normal – The state of the port is classified as Undetermined if an anomaly exists. An anomaly might be the absence of its own information in received UDLD messages or the failure to receive UDLD messages. An Undetermined state has no effect on the operation of the port. The port is not disabled and continues operating. When operating in UDLD normal mode, a port will be put into a disabled (Shutdown) state only in the following situations: The UDLD PDU received from a partner does not have its own details (echo). When there is a loopback, and information sent out on a port is received back exactly as it was sent. Aggressive – The port is put into a disabled state for the same reasons that it occurs in normal mode. Additionally, a port in UDLD aggressive mode can be disabled if the port does not receive any UDLD echo packets even after bidirectional connection was

	established. If a bidirectional link is established, and packets suddenly stop coming from partner device, the UDLD aggressive-mode port assumes that link has become unidirectional.
UDLD Status	The UDLD status on the port, which is one of the following: Not Applicable – The administrative status of UDLD is globally disabled or disabled on the interface. Bidirectional – UDLD has detected a bidirectional link. Shutdown – UDLD has detected a unidirectional link, and the port is in a disabled state. To clear the disabled state, click UDLD Port Reset. Undetermined – UDLD has not collected enough information to determine the state of the port. Unknown – The port link has physically gone down, but it is not because it was put in a disabled state by the UDLD feature.

4.1.18 VLAN

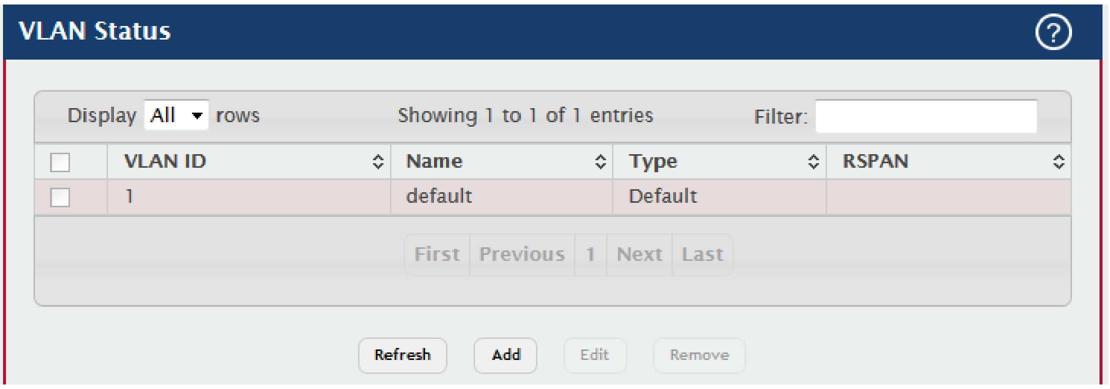
4.1.18.1 Status

Use this page to add and remove virtual local area networks (VLANs). VLANs allow you to divide a broadcast domain into smaller, logical networks. From this page, you can also configure a name for an existing VLAN and convert dynamic VLANs to static VLANs.

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.

Note: You cannot remove or rename VLAN 1



VLAN Status

Display All rows Showing 1 to 1 of 1 entries Filter:

□	VLAN ID	Name	Type	RSPAN
□	1	default	Default	

Field	Description
VLAN ID	The unique VLAN identifier (VID).
Name	A user-configurable name that identifies the VLAN.
Type	The type of VLAN, which can be one of the following: Default – The default VLAN. This VLAN is always present, and the VLAN ID is 1. Static – A user-configured VLAN. Dynamic – A VLAN created by GARP VLAN Registration Protocol (GVRP).
RSPAN	Identifies whether the VLAN is configured (Enabled) as the Remote Switched Port Analyzer (RSPAN) VLAN. The RSPAN VLAN is used to carry mirrored traffic from source ports to a destination probe port on a remote device.

After you click Add, the Add VLAN window opens and allows you to create VLANs. The following information describes the field in this window

Field	Description
VLAN ID or Range	Specify VLAN ID(s). Use '-' to specify a range and ',' to separate VLAN IDs or VLAN ranges in the list.

When you click Edit, the Edit VLAN Configuration window opens. The following information describes the fields in this window.

Field	Description
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	For dynamic VLANs, select this option to convert the dynamic VLAN

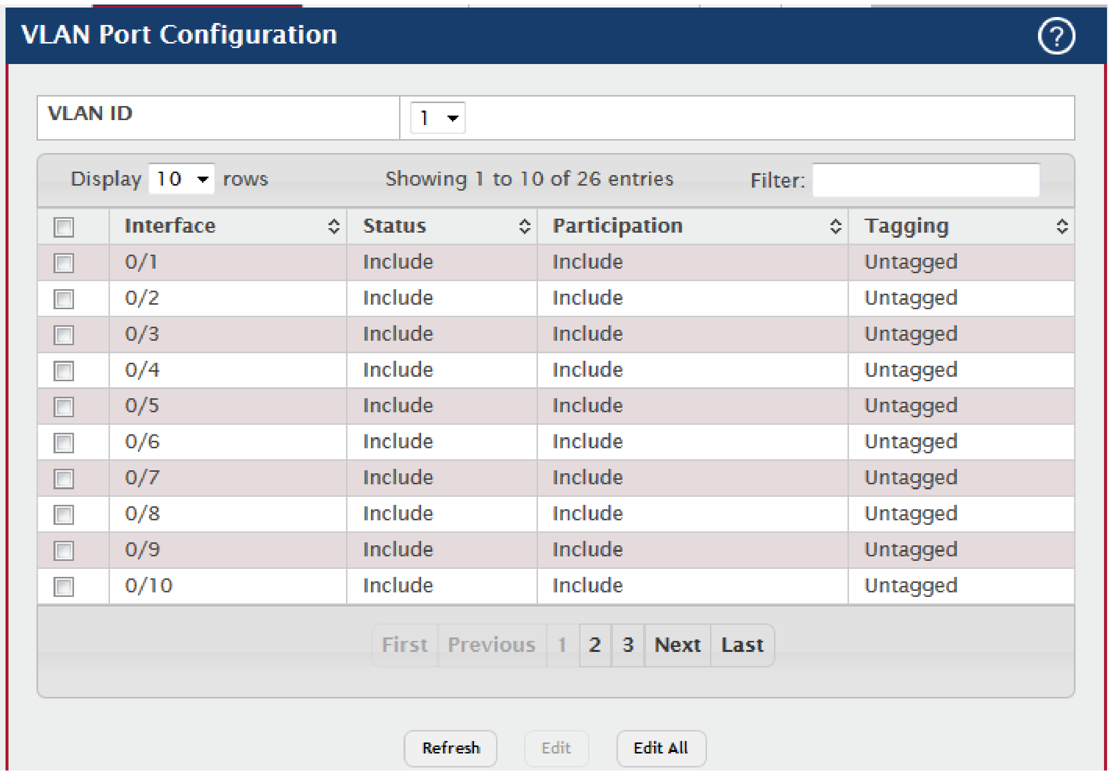
Type to Static	to a static VLAN. This option is not available for other VLAN types. A dynamic VLAN is learned by using GVRP, which is an industry-standard protocol that propagates VLAN information from one network device to another. GVRP can also remove dynamic VLANs. If you convert a dynamic VLAN to a static VLAN, it cannot be removed by GVRP.

4.1.18.2 Port Configuration

Use this page to configure VLAN membership for the interfaces on the device and to specify whether traffic transmitted by the member ports should be tagged. The device supports IEEE 802.1Q tagging. Ethernet frames on a tagged VLAN have a 4-byte VLAN tag in the header.

To configure VLAN membership and tagging settings for one or more interfaces, select the appropriate VLAN from the VLAN ID menu and use the buttons to perform the following tasks:

- To configure the VLAN settings for one or more interfaces in the selected VLAN, select each entry to modify and click Edit.
- To apply the same VLAN settings to all interfaces, click Edit All.



VLAN Port Configuration

VLAN ID: 1

Display 10 rows Showing 1 to 10 of 26 entries Filter:

□	Interface	Status	Participation	Tagging
□	0/1	Include	Include	Untagged
□	0/2	Include	Include	Untagged
□	0/3	Include	Include	Untagged
□	0/4	Include	Include	Untagged
□	0/5	Include	Include	Untagged
□	0/6	Include	Include	Untagged
□	0/7	Include	Include	Untagged
□	0/8	Include	Include	Untagged
□	0/9	Include	Include	Untagged
□	0/10	Include	Include	Untagged

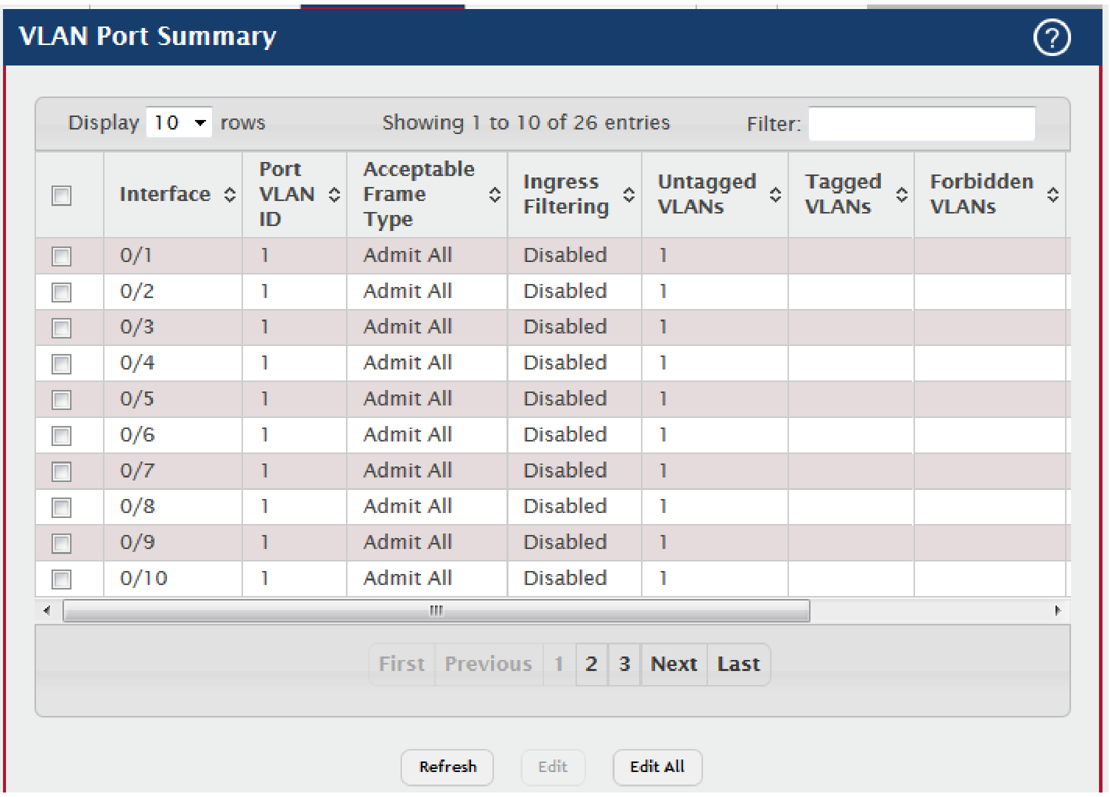
Field	Description
VLAN ID	The menu includes the VLAN ID for all VLANs configured on the device. To view or configure settings for a VLAN, be sure to select the correct VLAN from the menu.
Interface	The interface associated with the rest of the data in the row. When editing VLAN information for one or more interfaces, this field identifies the interfaces that are being configured.
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 or MVRP. The port will not participate in this VLAN unless it receives a GVRP or MVRP request and the device software supports the corresponding protocol. This mode is equivalent to registration normal in the IEEE 802.1Q standard.
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.

4.1.18.3 Port Summary

Use this page to configure the way interfaces handle VLAN-tagged, priority-tagged, and untagged traffic.

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.**



VLAN Port Summary

Display 10 rows Showing 1 to 10 of 26 entries Filter:

□	Interface	Port VLAN ID	Acceptable Frame Type	Ingress Filtering	Untagged VLANs	Tagged VLANs	Forbidden VLANs
□	0/1	1	Admit All	Disabled	1		
□	0/2	1	Admit All	Disabled	1		
□	0/3	1	Admit All	Disabled	1		
□	0/4	1	Admit All	Disabled	1		
□	0/5	1	Admit All	Disabled	1		
□	0/6	1	Admit All	Disabled	1		
□	0/7	1	Admit All	Disabled	1		
□	0/8	1	Admit All	Disabled	1		
□	0/9	1	Admit All	Disabled	1		
□	0/10	1	Admit All	Disabled	1		

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.
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 Type	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

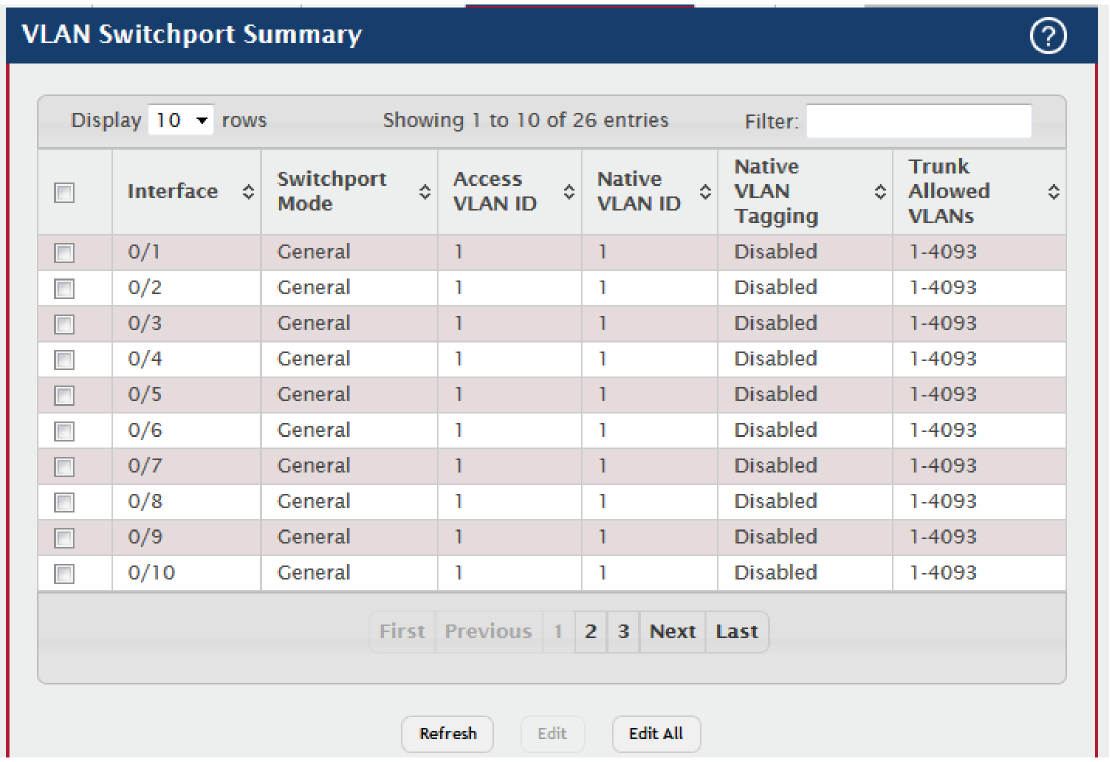
	receives. For all options, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard.
Ingress Filtering	Indicates how the interface handles tagged frames. The options include the following: Enabled – A tagged frame is discarded if this interface is not a member of the VLAN identified by the VLAN ID in the tag. Disabled – All tagged frames are accepted.
Untagged VLANs	VLANs which are configured on the port to transmit egress packets as untagged.
Tagged VLANs	VLANs which are configured on the port to transmit egress packets as tagged.
Forbidden VLANs	When configuring port memberships in VLANs, you can specify one or more VLANs to be excluded from the available VLANs for the port. The forbidden VLANs list shows the VLANs to which the port cannot be assigned membership.
Dynamic VLANs	The list of VLANs of which the port became a member as result of the operations of dynamic VLAN protocols. When a VLAN is created as a dynamic VLAN, any port that is configured as switchport type Trunk or General automatically becomes a member of the VLAN, unless the VLAN port is excluded from the VLAN.
Priority	The default 802.1p priority assigned to untagged packets arriving at the interface.

4.1.18.4 Switchport Summary

Use this 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 contraints the VLAN configuration of the port accordingly. Assigning the appropriate switchport mode helps simplify VLAN configuration and minimize errors.

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.**



VLAN Switchport Summary

Display 10 rows   Showing 1 to 10 of 26 entries   Filter:

□	Interface	Switchport Mode	Access VLAN ID	Native VLAN ID	Native VLAN Tagging	Trunk Allowed VLANs
□	0/1	General	1	1	Disabled	1-4093
□	0/2	General	1	1	Disabled	1-4093
□	0/3	General	1	1	Disabled	1-4093
□	0/4	General	1	1	Disabled	1-4093
□	0/5	General	1	1	Disabled	1-4093
□	0/6	General	1	1	Disabled	1-4093
□	0/7	General	1	1	Disabled	1-4093
□	0/8	General	1	1	Disabled	1-4093
□	0/9	General	1	1	Disabled	1-4093
□	0/10	General	1	1	Disabled	1-4093

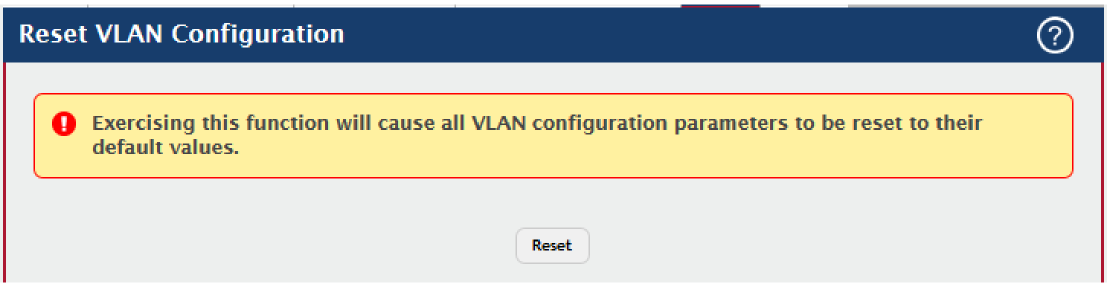
Field	Description
Interface	The interface associated with the rest of the data in the row. When editing information for one or more interfaces, this field identifies the interfaces that are being configured.
Switchport Mode	The switchport mode of the interface, which is one of the following: Access – 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.

4.1.18.5 Reset

Use this page to reset all VLAN settings to their default values. Any VLANs that have been created on the system will be deleted.

Initiates the action to reset all VLAN configuration parameters to their factory default settings. After you click Reset and confirm the action, all VLAN configuration changes are reset in the running configuration.

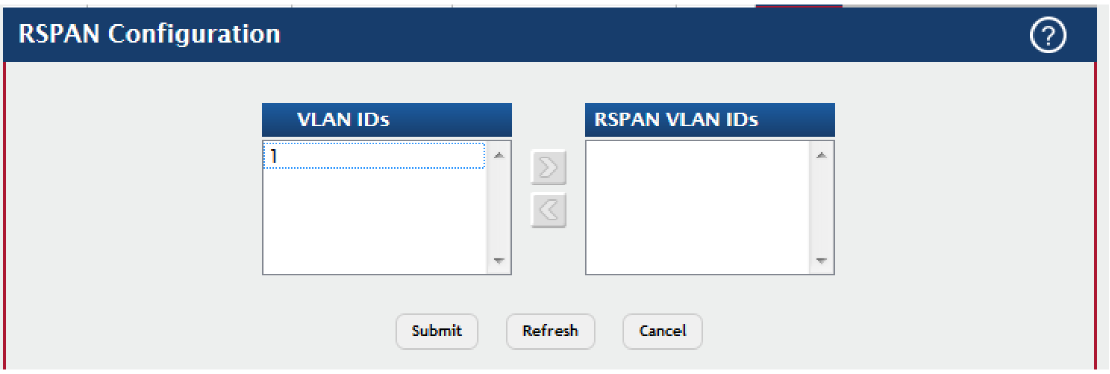


Reset VLAN Configuration

Exercising this function will cause all VLAN configuration parameters to be reset to their default values.

4.1.18.6 RSPAN

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.



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.
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.

4.1.19 Private VLAN

4.1.19.1 Configuration

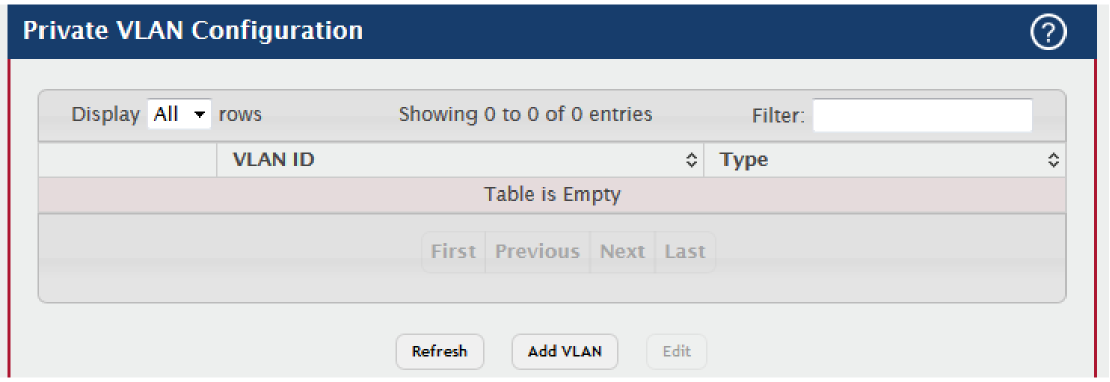
Use this page to add Virtual Local Area Networks (VLANs) to the device and to configure existing VLANs as private VLANs. Private VLANs provide Layer 2 isolation between ports that share the same broadcast domain. In other words, a private VLAN allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer 2 network. Each subdomain is defined (represented) by a primary VLAN and a secondary VLAN. The primary VLAN ID is the same for all subdomains that belong to a private VLAN. The secondary VLAN ID differentiates subdomains from each another and provides Layer 2 isolation between ports that are members of the same private VLAN.

Use the buttons to perform the following tasks:

- To add a VLAN, click **Add VLAN** and specify one or more VLAN IDs in the available field.

- To configure an existing VLAN as a private VLAN, select the entry to modify and click **Edit**.

Note: The default VLAN and management VLAN are not displayed on the page because they cannot be configured as private VLANs.


Private VLAN Configuration

Display All rows Showing 0 to 0 of 0 entries Filter:

VLAN ID	Type
Table is Empty	

Field	Description
VLAN ID	The ID of the VLAN that exists on the device.
Type	The private VLAN type, which is one of the following: Unconfigured – The VLAN is not configured as a private VLAN. Primary – A private VLAN that forwards the traffic from the promiscuous ports to isolated ports, community ports, and other promiscuous ports in the same private VLAN. Only one primary VLAN can be configured per private VLAN. All ports within a private VLAN share the same primary VLAN. Isolated – A secondary VLAN that carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN. Community – A secondary VLAN that forwards traffic between ports that belong to the same community and to the promiscuous ports. Multiple community VLANs can be configured per private VLAN.

After you click Add VLAN, the Add VLAN window opens and allows you to create VLANs. The following information describes the field in this window.

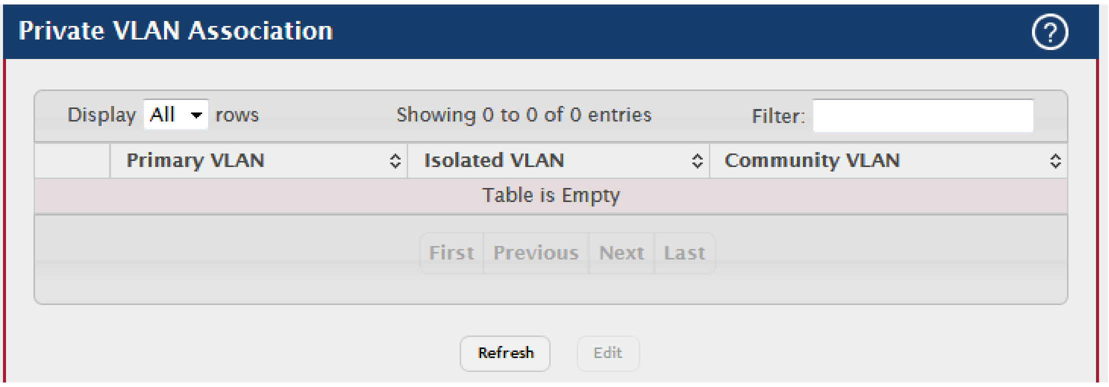
Field	Description
VLAN ID or Range	The ID of one or more VLANs to create. To create a single VLAN, enter its ID in the field. To create a continuous range of VLANs, use a hyphen (-) to separate the lowest and highest VLAN IDs in the range. To create multiple VLANs that are not in a continuous range, separate

	each VLAN ID or range of VLAN IDs with a comma (,). Do not use a space after the comma or anywhere in the field.

4.1.19.2 Association

Use this page to configure the association between the primary VLAN and secondary VLANs. Associating a secondary VLAN with a primary VLAN allows host ports in the secondary VLAN to communicate outside the private VLAN. To configure a primary VLAN association, select the entry to modify and click **Edit.**

Note: Isolated VLANs and Community VLANs are collectively called Secondary VLANs.



Private VLAN Association

Display All rows   Showing 0 to 0 of 0 entries   Filter:

	Primary VLAN	Isolated VLAN	Community VLAN
Table is Empty			

Field	Description
Primary VLAN	The VLAN ID of each VLAN configured as a primary VLAN.
Isolated VLAN	The VLAN ID of the isolated VLAN associated with the primary VLAN. If the field is blank, no isolated VLAN has been associated with the primary VLAN. An isolated VLAN is a secondary VLAN that carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN.
Community VLAN	The VLAN ID of each community VLAN associated with the primary VLAN. If the field is blank, no community VLANs have been associated with the primary VLAN. A community VLAN is a secondary VLAN that forwards traffic between ports that belong to the same community and to the promiscuous ports. Multiple community VLANs can be configured per private VLAN.

After you click Edit, the Edit Private VLAN Association window opens and allows you to create associations with the selected primary VLAN. The following information describes the field in this window.

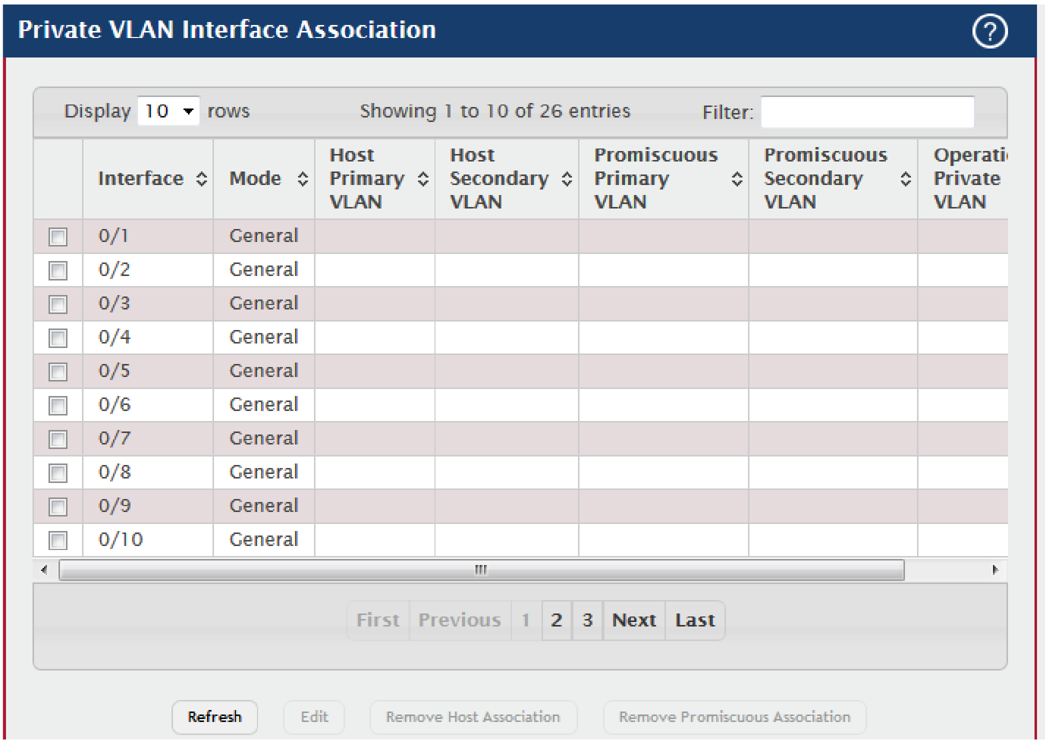
Field	Description
Secondary VLAN	The isolated or community VLANs that can be associated with the primary VLAN. Secondary VLANs that are already associated with a primary VLAN do not appear in the list and cannot be associated with another primary VLAN. To select multiple secondary VLANs, Ctrl + click each VLAN to associate with the primary VLAN.

4.1.19.3 Interface

Use this page to configure the port mode for the ports and LAGs that belong to a private VLAN and to configure associations between interfaces and primary/secondary private VLANs.

Use the buttons to perform the following tasks:

- To configure the port mode and private VLAN-to-interface associations, select the entry to modify and click **Edit.**
- To remove the association between an interface and the primary/secondary private VLANs that the interface belongs to when it operates in host mode, select each interface with the association to clear and click **Remove Host Association.** You must confirm the action before the host association for the entry is cleared.
- To remove the association between an interface and the primary/secondary private VLANs that the interface belongs to when it operates in promiscuous mode, select each interface with the association to clear and click **Remove Promiscuous Association.** You must confirm the action before the promiscuous association for the entry is cleared.



Private VLAN Interface Association

Display 10 rows Showing 1 to 10 of 26 entries Filter:

	Interface	Mode	Host Primary VLAN	Host Secondary VLAN	Promiscuous Primary VLAN	Promiscuous Secondary VLAN	Operati Private VLAN
□	0/1	General					
□	0/2	General					
□	0/3	General					
□	0/4	General					
□	0/5	General					
□	0/6	General					
□	0/7	General					
□	0/8	General					
□	0/9	General					
□	0/10	General					

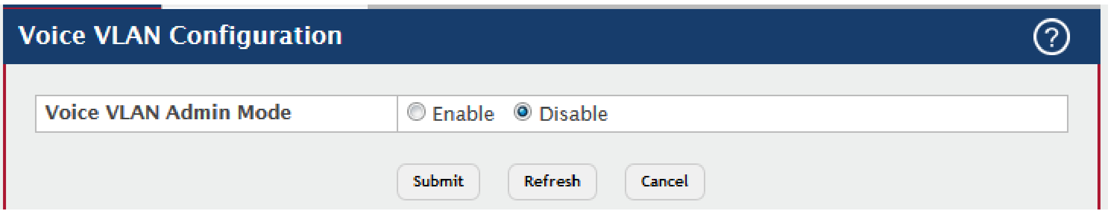
Field	Description
Interface	The interface associated with the rest of the data in the row. When editing interface settings, this field identifies the interface being configured.
Mode	The private VLAN mode of the interface, which is one of the following: General – The interface is in general mode and is not a member of a private VLAN. Promiscuous – The interface belongs to a primary VLAN and can communicate with all interfaces in the private VLAN, including other promiscuous ports, community ports, and isolated ports. Host – The interface belongs to a secondary VLAN and, depending upon the type of secondary VLAN, can either communicate with other ports in the same community (if the secondary VLAN is a community VLAN) and with the promiscuous ports or is able to communicate only with the promiscuous ports (if the secondary VLAN is an isolated VLAN).
Host Primary VLAN	The primary private VLAN the port is a member of when it is configured to operate in Host mode.
Host Secondary VLAN	The secondary private VLAN the port is a member of when it is configured to operate in Host mode. The secondary private VLAN is

	either an isolated or community VLAN.
Promiscuous Primary VLAN	The primary private VLAN in which the port is a member when it is configured to operate in Promiscuous mode.
Promiscuous Secondary VLAN	The secondary private VLAN the port is a member of when it is configured to operate in Promiscuous mode. The secondary private VLAN is either an isolated or community VLAN.
Operational Private VLAN	The primary and secondary operational private VLANs for the interface. The VLANs that are operational depend on the configured mode for the interface and the private VLAN type.

4.1.20 Voice VLAN

4.1.20.1 Configuration

Use this page to control the administrative mode of the Voice VLAN feature, which enables ports to carry voice traffic that has a defined priority. Voice over IP (VoIP) traffic is inherently time-sensitive: for a network to provide acceptable service, the transmission rate is vital. The priority level enables the separation of voice and data traffic entering the port.



Voice VLAN Configuration

Voice VLAN Admin Mode ○ Enable ● Disable

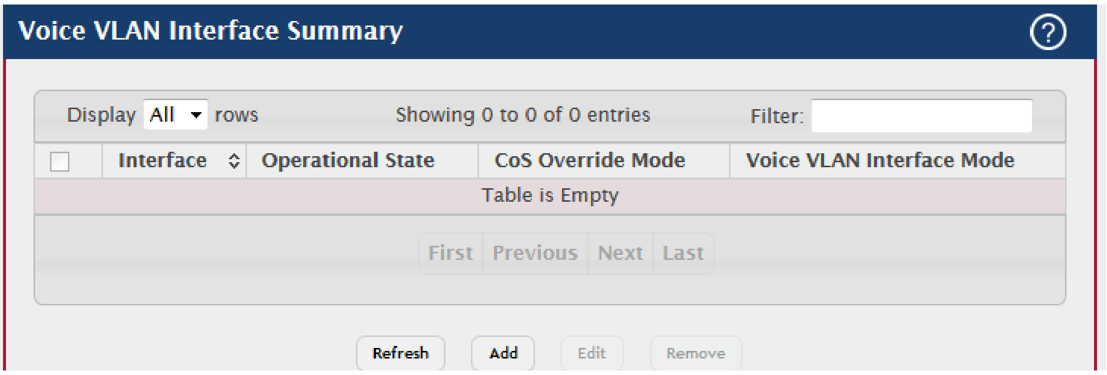
Field	Description
Voice VLAN Admin Mode	The administrative mode of the Voice VLAN feature. When Voice VLAN is enabled globally and configured on interfaces that carry voice traffic, this feature can help ensure that the sound quality of an IP phone does not deteriorate when data traffic on the port is high.

4.1.20.2 Interface Summary

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**.


Voice VLAN Interface Summary

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Interface	Operational State	CoS Override Mode	Voice VLAN Interface Mode
Table is Empty				

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	Indicates how an IP phone connected to the port should send voice traffic: VLAN 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.

5.1 Routing

5.1.1 ARP Table

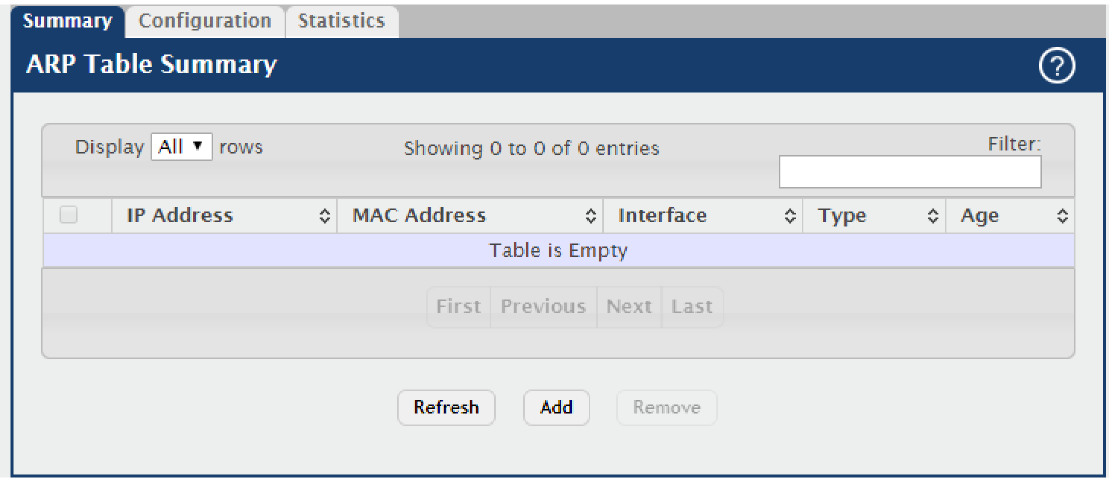
Use this page to view and manage the contents of the ARP table. The ARP table shows all of the IP addresses that have been resolved to MAC addresses, either dynamically or through static entry configuration. This table also shows which dynamic entries are associated with a routing interface (Gateway entries), as well as entries that have been statically configured by the user. In addition, the address resolution of all local routing interfaces is shown.

5.1.1.1 Summary

Use the buttons to perform the following tasks:

· To add a static ARP entry, click Add. The Add Static ARP Entry dialog box opens. Specify the new entry information in the available fields.

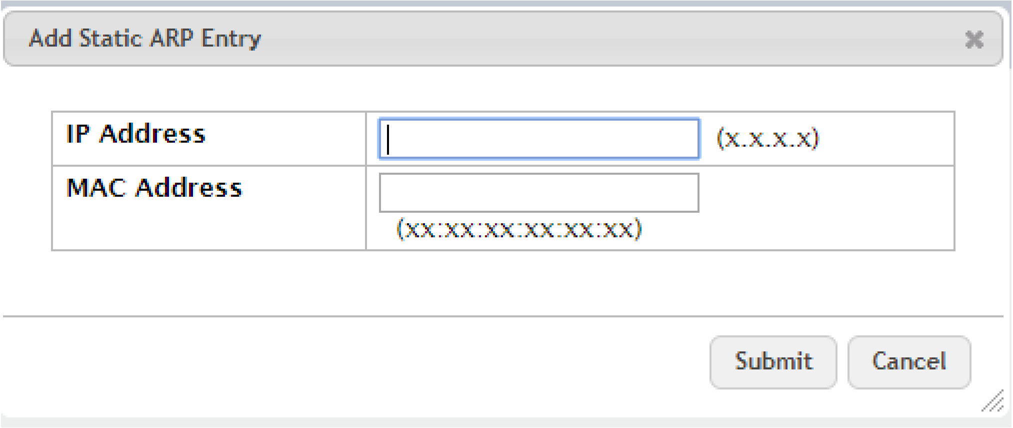
· To delete one or more ARP entries, select each entry to delete and click Remove. Note that ARP entries designated as Local cannot be removed.



ARP Table Summary

Showing 0 to 0 of 0 entries

□	IP Address	MAC Address	Interface	Type	Age
Table is Empty					



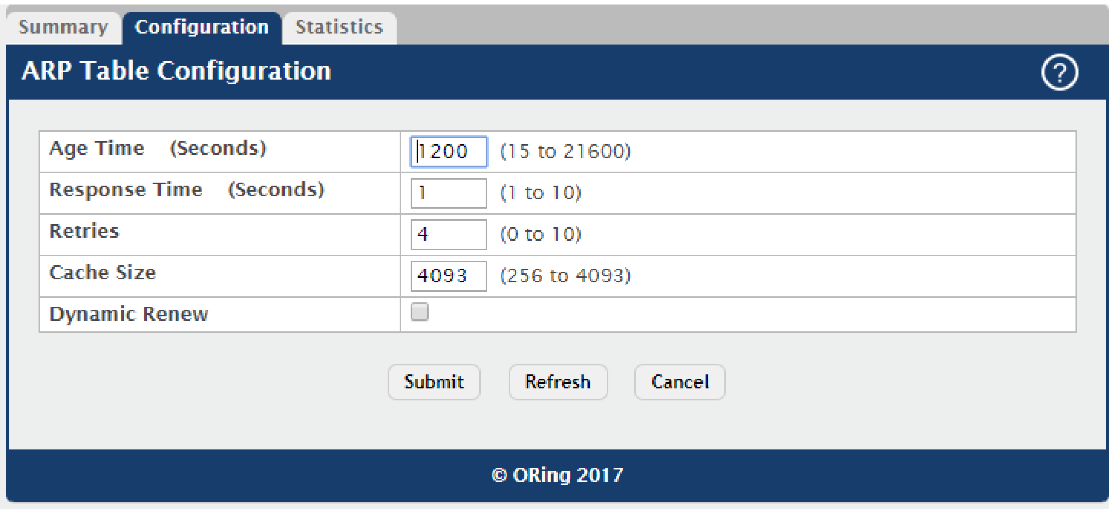
Add Static ARP Entry

IP Address	(x.x.x.x)
MAC Address	(xx:xx:xx:xx:xx:xx)

Field	Description
IP Adddress	The IP address of a network host on a subnet attached to one of the device's routing interfaces. When adding a static ARP entry, specify the IP address for the entry after you click **Add.**
MAC Address	The unicast MAC address (hardware address) associated with the network host. When adding a static ARP entry, specify the MAC address to associate with the IP address in the entry.
Interface	The routing interface associated with the ARP entry. The network host is associated with the device through this interface.
Type	The ARP entry type: ・**Dynamic** – An ARP entry that has been learned by the router ・**Gateway** – A dynamic ARP entry that has the IP address of a routing interface ・**Local** – An ARP entry associated with the MAC address of a routing interface on the device ・**Static** – An ARP entry configured by the user
Age	The age of the entry since it was last learned or refreshed. This value is specified for Dynamic or Gateway entries only (it is left blank for all other entry types).

5.1.1.2 Configuration

Use this page to configure ARP table settings.



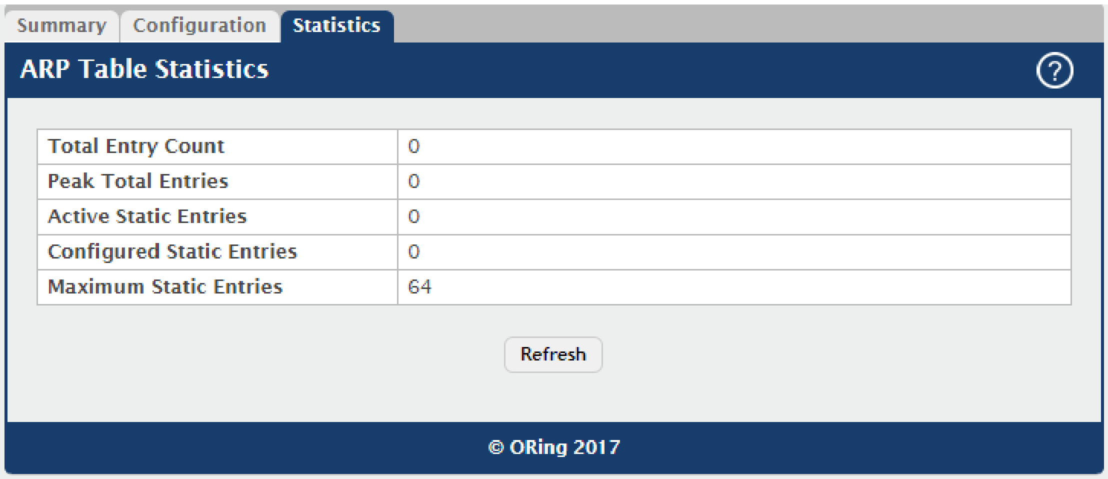
Age Time (Seconds)	1200	(15 to 21600)
Response Time (Seconds)	1	(1 to 10)
Retries	4	(0 to 10)
Cache Size	4093	(256 to 4093)
Dynamic Renew	□	

Field	Description
Age Time	The amount of time, in seconds, that a dynamic ARP entry remains in the ARP table before aging out.

Response Time	The amount of time, in seconds, that the device waits for an ARP response to an ARP request that it sends.
Retries	The maximum number of times an ARP request will be retried after an ARP response is not received. The number includes the initial ARP request.
Cache Size	The maximum number of entries allowed in the ARP table. This number includes all static and dynamic ARP entries.
Dynamic Renew	When selected, this option allows the ARP component to automatically attempt to renew dynamic ARP entries when they age out.

5.1.1.3 Statistics

This page displays information about the number and type of entries in the system ARP table. The ARP table contains entries that map IP addresses to MAC addresses.



Total Entry Count	0
Peak Total Entries	0
Active Static Entries	0
Configured Static Entries	0
Maximum Static Entries	64

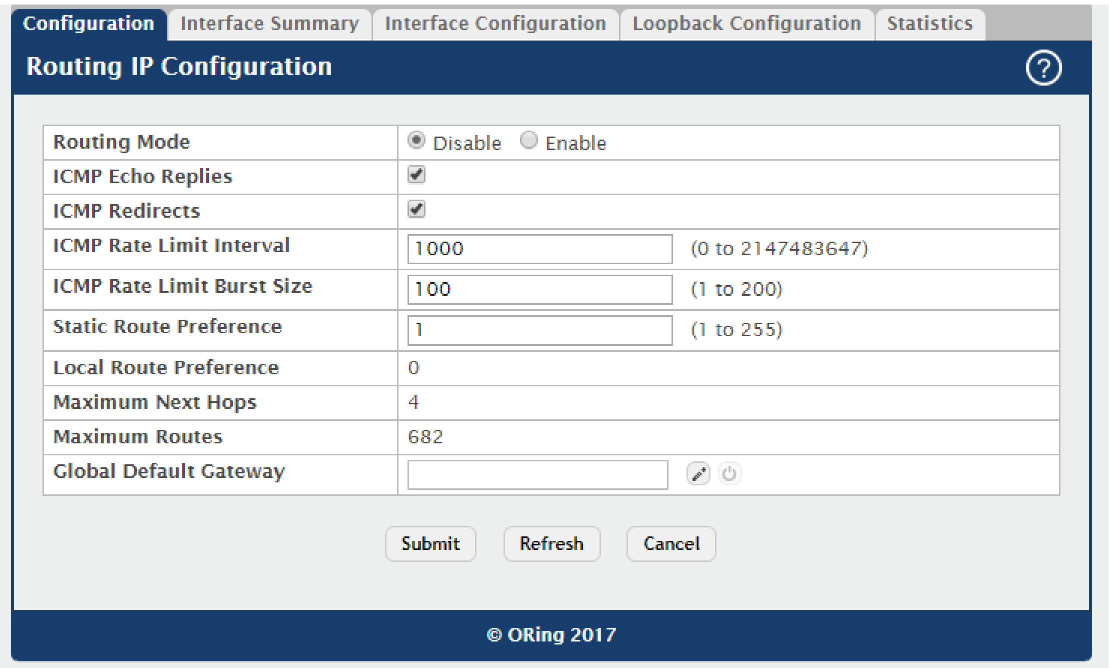
Field	Description
Total Entry Count	The total number of entries currently in the ARP table. The number includes both dynamically learned entries and statically configured entries.
Peak Total Entries	The highest value reached by the Total Entry Count. This value is reset whenever the ARP table Cache Size configuration parameter is changed.
Active Static Entries	The total number of active ARP entries in the ARP table that were statically configured. After a static ARP entry is configured, it might not become active until certain other routing configuration conditions are met.

Configured Static Entries	The total number of static ARP entries that are currently in the ARP table. This number includes static ARP entries that are not active.
Maximum Static Entries	The maximum number of static ARP entries that can be configured in the ARP table.

5.1.2 IP

5.1.2.1 Configuration

Use this page to configure global routing settings on the device. Routing provides a means of transmitting IP packets between subnets on the network. Routing configuration is necessary only if the device is used as a Layer 3 device that routes packets between subnets. If the device is used as a Layer 2 device that handles switching only, it typically connects to an external Layer 3 device that handles the routing functions; therefore, routing configuration is not required on the Layer 2 device.



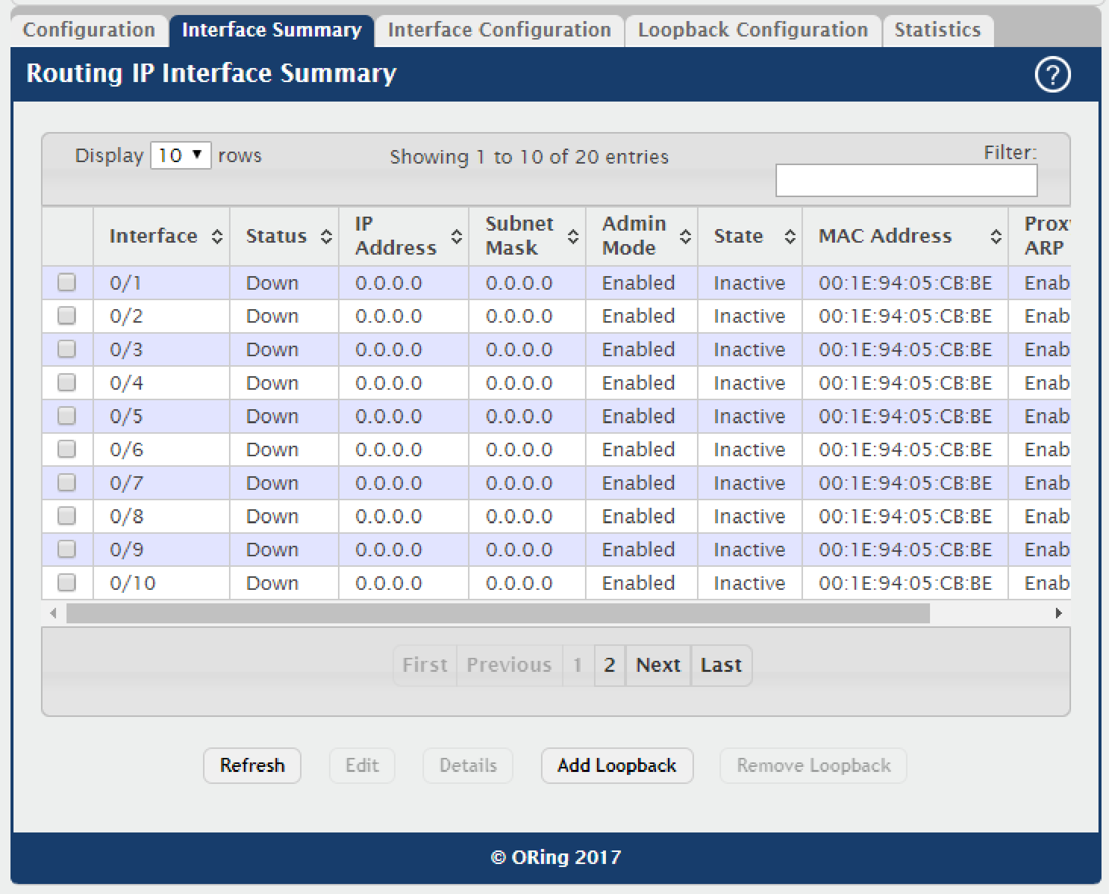
Routing Mode	● Disable ○ Enable
ICMP Echo Replies	☑
ICMP Redirects	☑
ICMP Rate Limit Interval	1000 (0 to 2147483647)
ICMP Rate Limit Burst Size	100 (1 to 200)
Static Route Preference	1 (1 to 255)
Local Route Preference	0
Maximum Next Hops	4
Maximum Routes	682
Global Default Gateway	

Field	Description
Routing Mode	The administrative mode of routing on the device. The options are as follows: · **Enable** – The device can act as a Layer 3 device by routing packets between interfaces configured for IP routing. · **Disable** – The device acts as a Layer 2 bridge and switches traffic between interfaces. The device does not perform any internetwork

	routing.
ICMP Echo Replies	Select this option to allow the device to send ICMP Echo Reply messages in response to ICMP Echo Request (ping) messages it receives.
ICMP Redirects	Select this option to allow the device to send ICMP Redirect messages to hosts. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.
ICMP Rate Limit Interval	The maximum burst interval for ICMP error messages transmitted by the device. The rate limit for ICMP error messages is configured as a token bucket. The ICMP Rate Limit Interval specifies how often the token bucket is initialized with tokens of the size configured in the ICMP Rate Limit Burst Size field.
ICMP Rate Limit Burst Size	The number of ICMP error messages that can be sent during the burst interval configured in the ICMP Rate Limit Interval field.
Static Route Preference	The default distance (preference) for static routes. Lower route-distance values are preferred when determining the best route. The value configured for Static Route Preference is used when using the CLI to configure a static route and no preference is specified. Changing the Static Route Preference does not update the preference of existing static routes.
Local Route Preference	The default distance (preference) for local routes.
Maximum Next Hops	The maximum number of hops the device supports.
Maximum Routes	The maximum number of routes that can exist in the routing table.
Global Default Gateway	The IP address of the default gateway for the device. If the destination IP address in a packet does not match any routes in the routing table, the packet is sent to the default gateway. The gateway specified in this field is more preferred than a default gateway learned from a DHCP server. Use the icons associated with this field to perform the following tasks: · To configure the default gateway, click the **Edit** icon and specify the IP address of the default gateway in the available field. · To reset the IP address of the default gateway to the factory default value, click the Reset icon associated with this field.

5.1.2.2 Interface Summary

This page shows summary information about the routing configuration for all interfaces. To edit any interface, select the interface and click **Edit**. To view additional routing configuration information for an interface, select the interface with the settings to view and click **Details.** To add next available loopback interface click **Add Loopback**. To remove entries, select the entries (only loopback entries can be removed) and click **Remove Loopback**. Multi-select feature is only for loopback interfaces.



Routing IP Interface Summary

Display 10 ▾ rows   Showing 1 to 10 of 20 entries   Filter:

	Interface	Status	IP Address	Subnet Mask	Admin Mode	State	MAC Address	Prox ARP
□	0/1	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab
□	0/2	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab
□	0/3	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab
□	0/4	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab
□	0/5	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab
□	0/6	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab
□	0/7	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab
□	0/8	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab
□	0/9	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab
□	0/10	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:1E:94:05:CB:BE	Enab

Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing details about the routing settings for an interface, this field identifies the interface being viewed.
Status	Indicates whether the interface is capable of routing IP packets (Up) or cannot route packets (Down). For the status to be Up, the routing mode and administrative mode for the interface must be enabled. Additionally, the interface must have an IP address and be physically up (active link).
IP Address	The IP address of the interface.

Subnet Mask	The IP subnet mask for the interface (also known as the network mask or netmask). It defines the portion of the interface's IP address that is used to identify the attached network.
Admin Mode	The administrative mode of the interface, which is either Enabled or Disabled.
State	The state of the interface, which is either Active or Inactive. An interface is considered active if the link is up, and the interface is in a forwarding state.
MAC Address	The burned-in physical address of the interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
Proxy ARP	Indicates whether proxy ARP is enabled or disabled on the interface. When proxy ARP is enabled, the interface can respond to an ARP request for a host other than itself. An interface can act as an ARP proxy if it is aware of the destination and can route packets to the intended host, which is on a different subnet than the host that sent the ARP request.
IP MTU	The largest IP packet size the interface can transmit, in bytes. The IP Maximum Transmission Unit (MTU) is the maximum frame size minus the length of the Layer 2 header. After you click **Edit**, the navigation is redidected to the respective configuration page for the selected interface based on interface type [loopback/non-loopback]. After you click **Details**, the **Details** window opens and displays detailed routing information for the selected interface. The following information describes the fields in this window that are not displayed on the summary page.
Routing Mode	Indicates whether routing is administratively enabled or disabled on the interface.
Link Speed Data Rate	The physical link data rate of the interface.
IP Address Configuration Method	The source of the IP address, which is one of the following: **None** – The interface does not have an IP address. **Manual** – The IP address has been statically configured by an administrator. **DHCP** – The IP address has been learned dynamically through

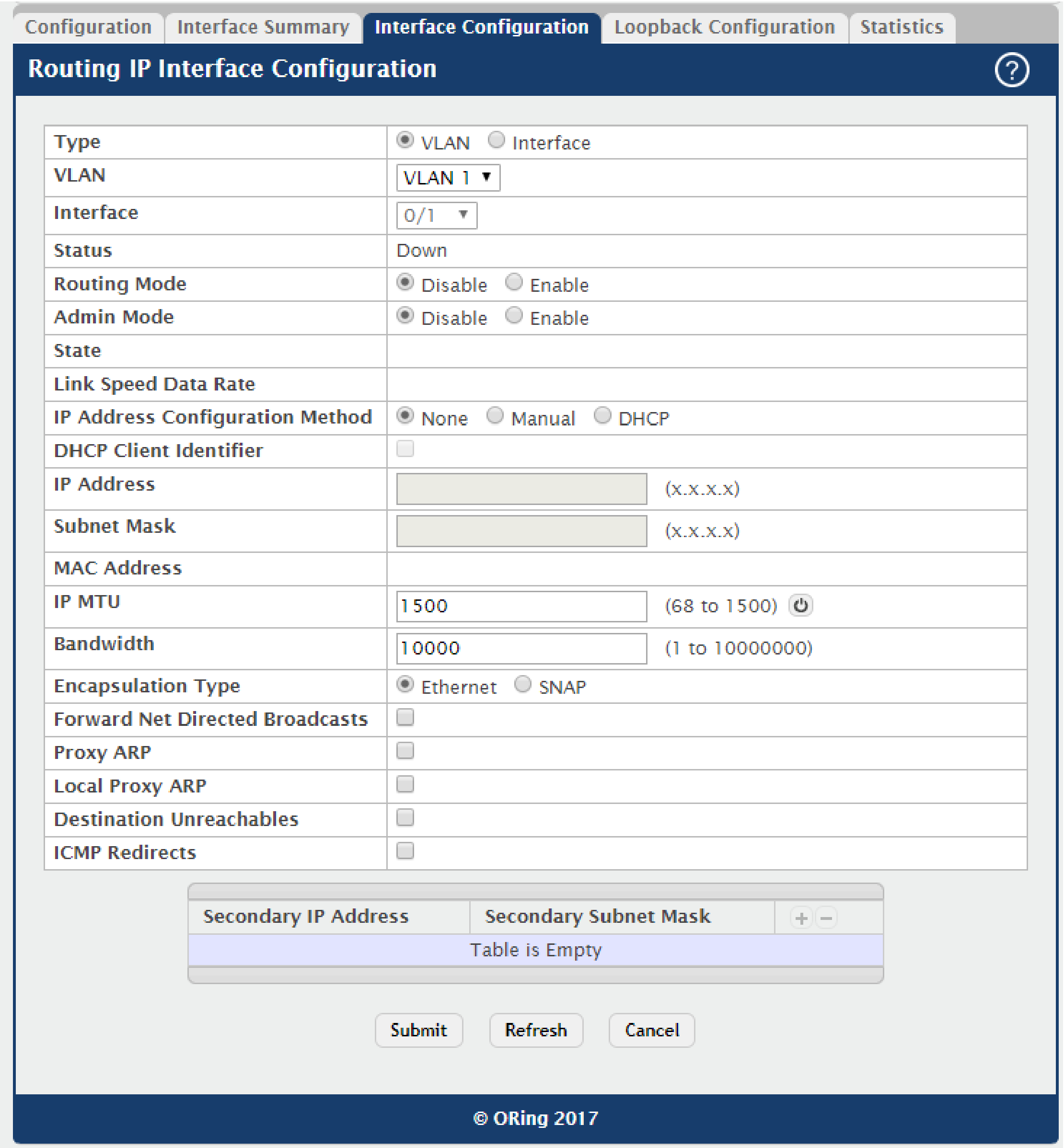
	DHCP. If the method is DHCP but the interface does not have an IP address, the interface is unable to acquire an address from a network DHCP server.
Bandwidth	The configured bandwidth on this interface. This setting communicates the speed of the interface to higher-level protocols.
Encapsulation Type	The link layer encapsulation type for packets transmitted from the interface, which can be either Ethernet or SNAP.
Forward Net Directed Boradcasts	Indicates how the interface handles network-directed broadcast packets. A network-directed broadcast is a broadcast directed to a specific subnet. The possible values are as follows: **Enabled** – Network directed broadcasts are forwarded. **Disabled** – Network directed broadcasts are dropped.
Local Proxy ARP	Indicates whether local proxy ARP is enabled or disabled on the interface. When local proxy ARP is enabled, the interface can respond to an ARP request for a host other than itself. Unlike proxy ARP, local proxy ARP allows the interface to respond to ARP requests for a host that is on the same subnet as the host that sent the ARP request. This feature is useful when a host is not permitted to reply to an ARP request from another host in the same subnet, for example when using the protected ports feature.
Destination Unreachables	Indicates whether the interface is allowed to send ICMP Destination Unreachable message to a host if the intended destination cannot be reached for some reason. If the status of this field is Disabled, this interface will not send ICMP Destination Unreachable messages to inform the host about the error in reaching the intended destination.
ICMP Redirects	Indicates whether the interface is allowed to send ICMP Redirect messages. The device sends an ICMP Redirect message on an interface only if ICMP Redirects are enabled both globally and on the interface. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.

After you click **Add Loopback**, the next available loopback interface is added. The button is disabled, if maximum no of loopback interfaces are configured.

After you click **Remove Loopback**, the selected entries are deleted on confirmation.

5.1.2.3 Interface Configuration

Use this page to configure the IP routing settings for each non-loopback interface.



Routing IP Interface Configuration

Type	● VLAN ○ Interface
VLAN	VLAN 1 ▾
Interface	0/1 ▾
Status	Down
Routing Mode	● Disable ○ Enable
Admin Mode	● Disable ○ Enable
State	
Link Speed Data Rate	
IP Address Configuration Method	● None ○ Manual ○ DHCP
DHCP Client Identifier	□
IP Address	(x.x.x.x)
Subnet Mask	(x.x.x.x)
MAC Address	
IP MTU	1500 (68 to 1500)
Bandwidth	10000 (1 to 10000000)
Encapsulation Type	● Ethernet ○ SNAP
Forward Net Directed Broadcasts	□
Proxy ARP	□
Local Proxy ARP	□
Destination Unreachables	□
ICMP Redirects	□

Secondary IP Address	Secondary Subnet Mask
Table is Empty	

Field	Description
Type	The type of interface that can be configured for routing: **Interface** – Enables list of all non-loopback interfaces that can be configured for routing. **VLAN** – Enables list of all VLANs that can be configured for routing.
VLAN	The menu contains all VLANs that can be configured for routing. To configure routing settings for a VLAN, select it from the menu and then configure the rest of the settings on the page.
Interface	The menu contains all non-loopback interfaces that can be configured

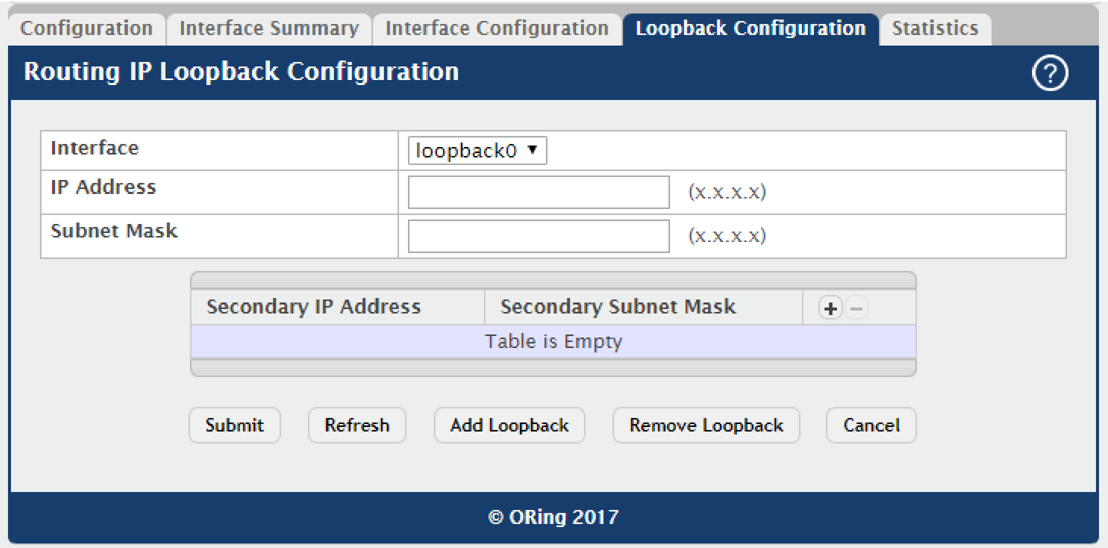
	for routing. To configure routing settings for an interface, select it from the menu and then configure the rest of the settings on the page.
Status	Indicates whether the interface is currently capable of routing IP packets (Up) or cannot route packets (Down). For the status to be Up, the routing mode and administrative mode for the interface must be enabled. Additionally, the interface must have an IP address and be physically up (active link).
Routing Mode	The administrative mode of IP routing on the interface.
Admin Mode	The administrative mode of the interface. If an interface is administratively disabled, it cannot forward traffic.
State	The state of the interface, which is either Active or Inactive. An interface is considered active if the link is up, and the interface is in a forwarding state.
Link Speed Data Rate	The physical link data rate of the interface.
IP Address Configuration Method	The method to use for configuring an IP address on the interface, which can be one of the following: **None** – No address is to be configured. **Manual** – The address is to be statically configured. When this option is selected you can specify the IP address and subnet mask in the available fields. **DHCP** – The interface will attempt to acquire an IP address from a network DHCP server.
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 interface. This field can be configured only when the selected IP Address Configuration Method is Manual. If the method is DHCP, the interface attempts to lease an IP address from a DHCP server on the network, and the IP address appears in this field (read-only) after it is acquired. If this field is blank, the IP Address Configuration Method might be None, or the method might be DHCP and the interface is unable to lease an address.

Subnet Mask	The IP subnet mask for the interface (also known as the network mask or netmask). This field can be configured only when the selected IP Address Configuration Method is Manual.
MAC Address	The burned-in physical address of the interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
IP MTU	The largest IP packet size the interface can transmit, in bytes. The IP Maximum Transmission Unit (MTU) is the maximum frame size minus the length of the Layer 2 header.
Bandwidth	The configured bandwidth on this interface. This setting communicates the speed of the interface to higher-level protocols.
Encapsulation Type	The link layer encapsulation type for packets transmitted from the interface, which can be either Ethernet or SNAP.
Forward Net Directed Broadcasts	Determines how the interface handles network-directed broadcast packets. A network-directed broadcast is a broadcast directed to a specific subnet. If this option is selected, network directed broadcasts are forwarded. If this option is clear, network directed broadcasts are dropped.
Proxy ARP	When this option is selected, proxy ARP is enabled, and the interface can respond to an ARP request for a host other than itself. An interface can act as an ARP proxy if it is aware of the destination and can route packets to the intended host, which is on a different subnet than the host that sent the ARP request.
Local Proxy ARP	When this option is selected, local proxy ARP is enabled, and the interface can respond to an ARP request for a host other than itself. Unlike proxy ARP, local proxy ARP allows the interface to respond to ARP requests for a host that is on the same subnet as the host that sent the ARP request. This feature is useful when a host is not permitted to reply to an ARP request from another host in the same subnet, for example when using the protected ports feature.
Destination Unreachables	When this option is selected, the interface is allowed to send ICMP Destination Unreachable message to a host if the intended destination cannot be reached for some reason. If this option is clear, the interface will not send ICMP Destination Unreachable messages to inform the host about the error in reaching the intended destination.
ICMP Redirects	When this option is selected, the interface is allowed to send ICMP Redirect messages. The device sends an ICMP Redirect message on

	an interface only if ICMP Redirects are enabled both globally and on the interface. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.
Secondary IP Address	To add a secondary IP address on the interface, click the + (plus) symbol in the header row and enter the address in the appropriate field in the **Secondary IP Address Configuration** window. You can add one or more secondary IP addresses to an interface only if the interface already has a primary IP address. To remove a configured secondary IP address, click the – (minus) symbol associated with the entry to remove. To remove all configured secondary IP addresses, click the – (minus) symbol in the header row.
Secondary Subnet Mask	The subnet mask associated with the secondary IP address. You configure this field in the Secondary IP **Address Configuration** window.

5.1.2.4 Loopback Configuration

Use this page to configure the IP routing settings for each loopback interface.



Interface	loopback0 ▼	
IP Address		(x.x.x.x)
Subnet Mask		(x.x.x.x)

Secondary IP Address	Secondary Subnet Mask	+ –
Table is Empty		

Field	Description
Interface	The menu contains all loopback interfaces that can be configured for routing. To configure routing settings for an interface, select it from the menu and then configure the rest of the settings on the page.
IP Address	The IP address of the loopback interface.
Subnet Mask	The IP subnet mask for the interface (also known as the network

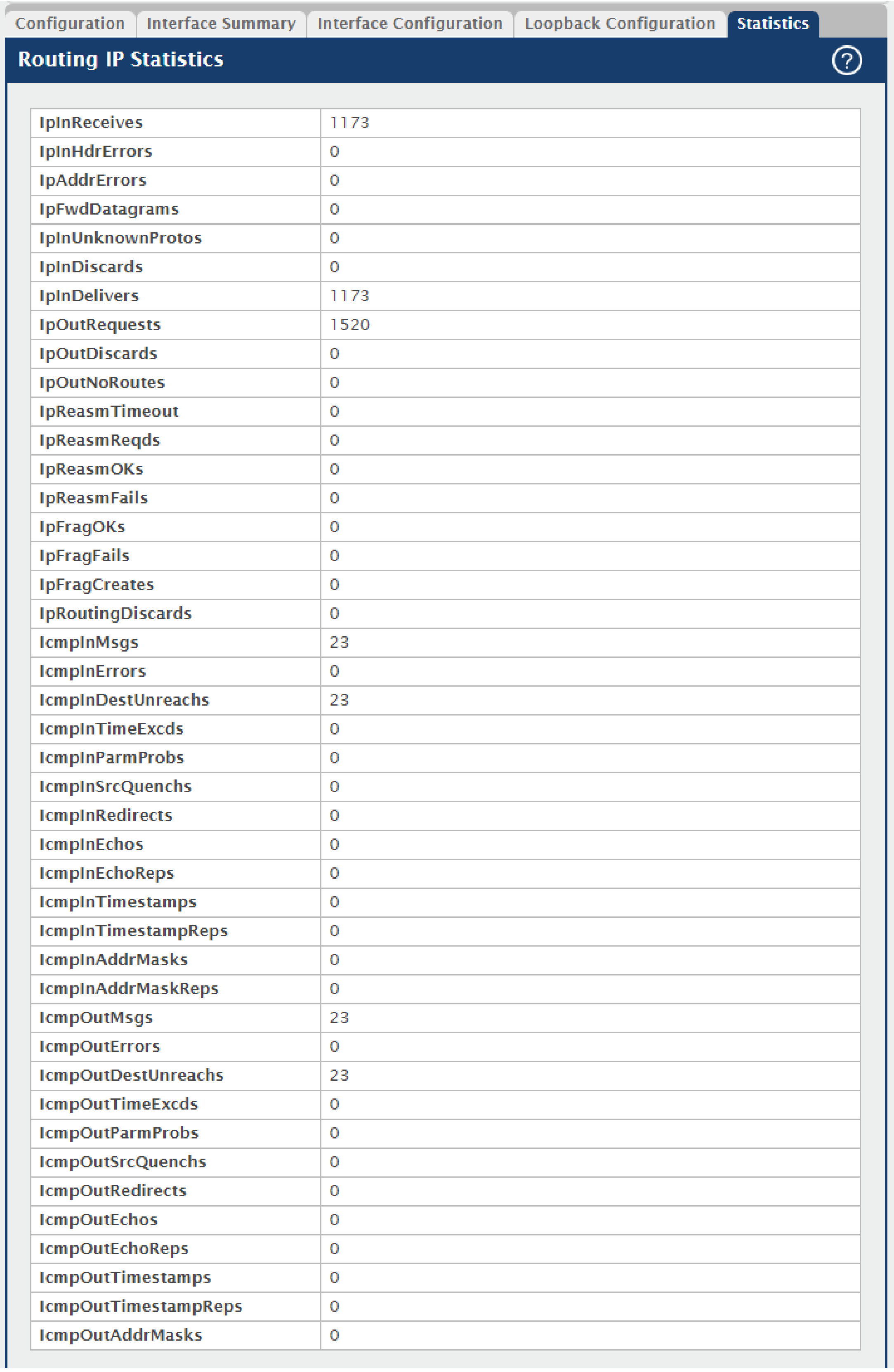
	mask or netmask).
Secondary IP Address	To add a secondary IP address on the interface, click the + (plus) symbol in the header row and enter the address in the appropriate field in the **Secondary IP Address Configuration** window. You can add one or more secondary IP addresses to an interface only if the interface already has a primary IP address. To remove a configured secondary IP address, click the – (minus) symbol associated with the entry to remove. To remove all configured secondary IP addresses, click the – (minus) symbol in the header row.
Secondary Subnet Mask	The subnet mask associated with the secondary IP address. This field is configurable in the Secondary IP **Address Configuration** window.

After clicking **Add Loopback**, the next available loopback interface will be added. If the maximum number of loopback interfaces are configured this button will be disabled.

After you click **Remove Loopback**, the selected entry is deleted on confirmation.

5.1.2.5 Statistics

This page displays information about the number and type of IP packets sent and received by all interfaces on the device. The statistics on this page are specified in RFC 1213.



Routing IP Statistics

IpInReceives	1173
IpInHdrErrors	0
IpAddrErrors	0
IpFwdDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	1173
IpOutRequests	1520
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	23
IcmpInErrors	0
IcmpInDestUnreachs	23
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSrcQuenchs	0
IcmpInRedirects	0
IcmpInEchos	0
IcmpInEchoReps	0
IcmpInTimestamps	0
IcmpInTimestampReps	0
IcmpInAddrMasks	0
IcmpInAddrMaskReps	0
IcmpOutMsgs	23
IcmpOutErrors	0
IcmpOutDestUnreachs	23
IcmpOutTimeExcds	0
IcmpOutParmProbs	0
IcmpOutSrcQuenchs	0
IcmpOutRedirects	0
IcmpOutEchos	0
IcmpOutEchoReps	0
IcmpOutTimestamps	0
IcmpOutTimestampReps	0
IcmpOutAddrMasks	0

Field	Description
IpInReceives	The total number of input datagrams received from all routing interfaces, including those datagrams received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
IpAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported classes (e.g., Class E). For entities which are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpFwdDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP gateways, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.

IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this no-route criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully reassembled.
IpReasmFails	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
IcmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.

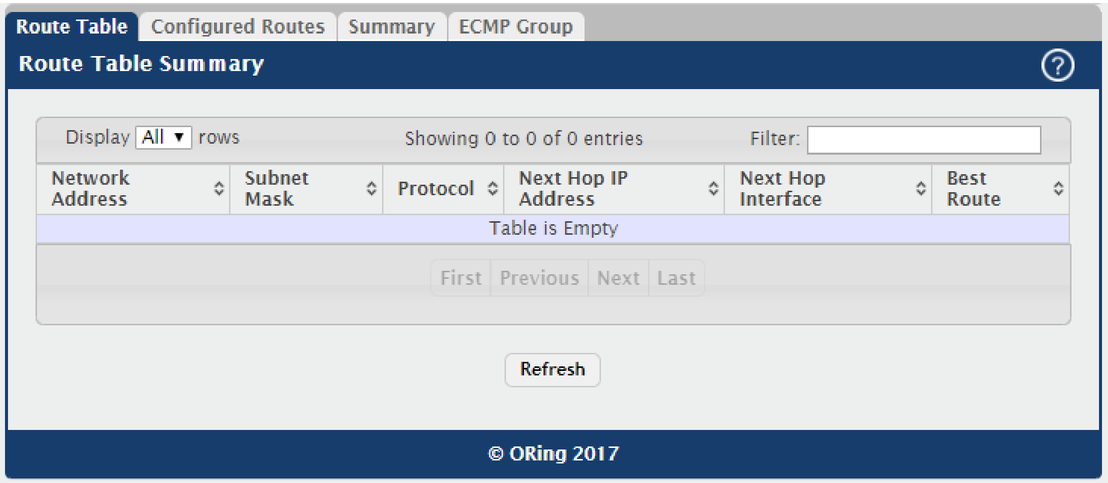
IcmpInErrors	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
IcmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
IcmpInTimeExcds	The number of ICMP Time Exceeded messages received.
IcmpInParmProbs	The number of ICMP Parameter Problem messages received.
IcmpInSrcQuenchs	The number of ICMP Source Quench messages received.
IcmpInRedirects	The number of ICMP Redirect messages received.
IcmpInEchos	The number of ICMP Echo (request) messages received.
IcmpInEchoReps	The number of ICMP Echo Reply messages received.
IcmpInTimestamps	The number of ICMP Timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP, such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no type of error that contributes to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.

IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.

5.1.3 Router

5.1.3.1 Route Table

This page displays the entries in the routing table, including all dynamically learned and statically configured entries. The device uses the routing table to determine how to forward packets.



Network Address	Subnet Mask	Protocol	Next Hop IP Address	Next Hop Interface	Best Route
Table is Empty					

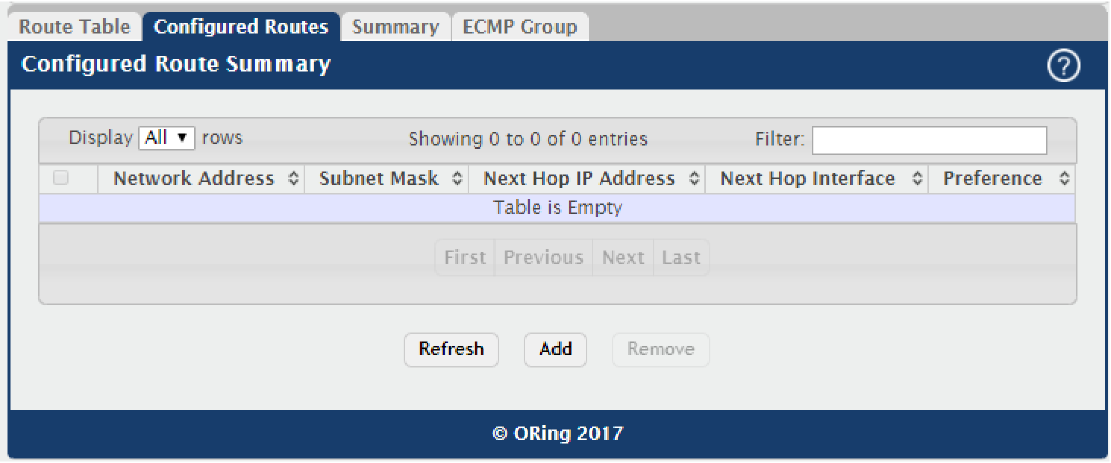
Field	Description
Network Address	The IP route prefix for the destination network.
Subnet Mask	The IP subnet mask (also known as the network mask or netmask) associated with the network address. It defines the portion of the IP address that is used to identify the attached network.
Protocol	Identifies which protocol created the route. A route can be created one of the following ways: · Dynamically learned through a supported routing protocol · Dynamically learned by being a directly-attached local route · Statically configured by an administrator · Configured as a default route by an administrator
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router

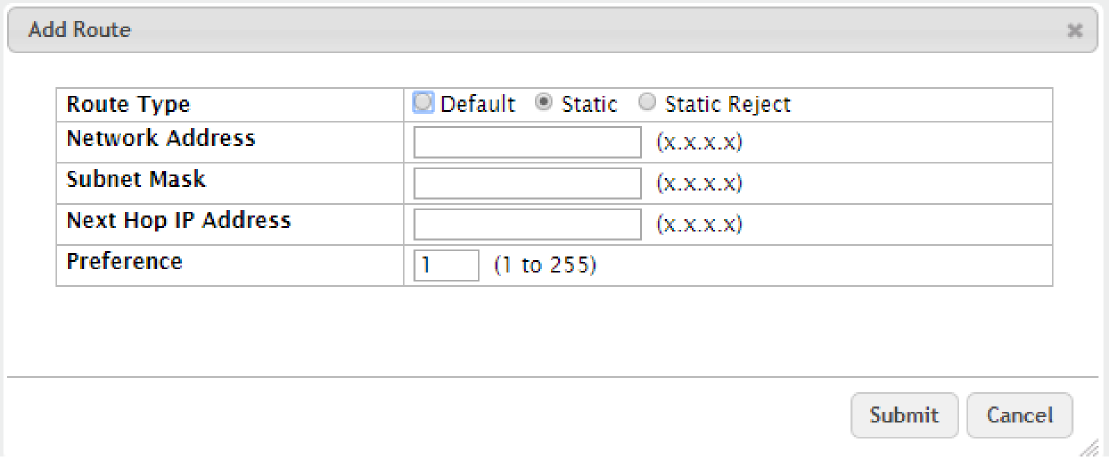
	is always one of the adjacent neighbors or the IP address of the local interface for a directly-attached network.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null.
Best Route	Indicates whether the route is the preferred route to the network. If the field is blank, a better route to the same network exists in the routing table.

5.1.3.2 Configured Routes

Use this page to configure the default route, static routes, and static reject routes in the routing table.Use the buttons to perform the following tasks:

- To configure a route, click Add and specify the desired settings in the available fields.
- To remove a configured route, select each entry to delete and click Remove. You must confirm the action before the entry is deleted.



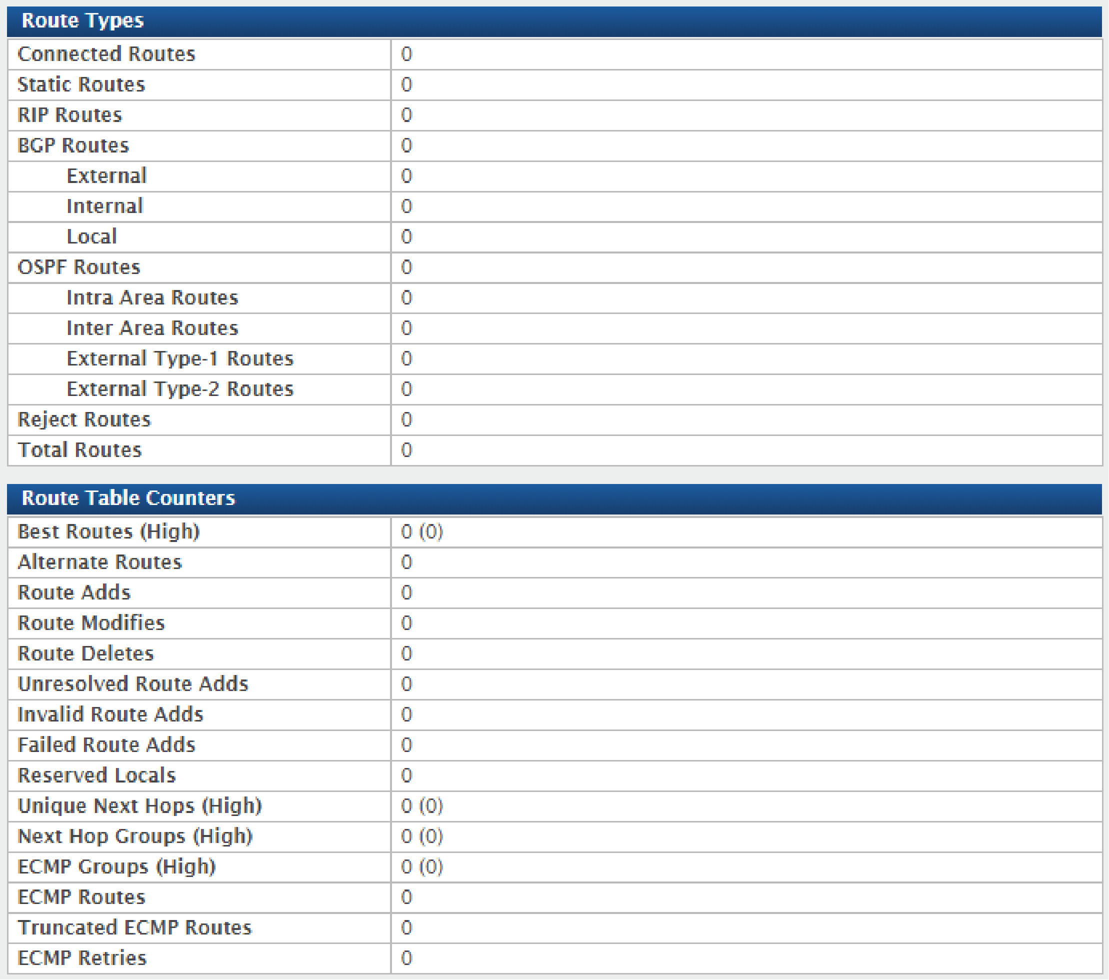


Route Type	○ Default ● Static ○ Static Reject
Network Address	(x.x.x.x)
Subnet Mask	(x.x.x.x)
Next Hop IP Address	(x.x.x.x)
Preference	1 (1 to 255)

Field	Description
Network Address	The IP route prefix for the destination network. This IP address must contain only the network portion of the address and not the host bits. When adding a default route, this field is not available.
Subnet Mask	The IP subnet mask (also known as the network mask or netmask) associated with the network address. The subnet mask defines which portion of an IP address belongs to the network prefix, and which portion belongs to the host identifier. When adding a default route, this field is not available.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly-attached network. When adding a static reject route, this field is not available because the packets are dropped rather than forwarded.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null.
Preference	The preference of the route. A lower preference value indicates a more preferred route. When the routing table has more than one route to the same network, the device selects the route with the best (lowest) route preference.
Route Type	The type of route to configure, which is one of the following: ・**Default** – The route the device uses to send a packet if the routing table does not contain a longer matching prefix for the packet's destination. The routing table can contain only one default route. ・**Static** – A route that is manually added to the routing table by an administrator. ・**Static Reject** – A route where packets that match the route are discarded instead of forwarded. The device might send an ICMP Destination Unreachable message.

5.1.3.3 Summary

This page displays summary information about the entries in the IP routing table.



Route Types	
Connected Routes	0
Static Routes	0
RIP Routes	0
BGP Routes	0
External	0
Internal	0
Local	0
OSPF Routes	0
Intra Area Routes	0
Inter Area Routes	0
External Type-1 Routes	0
External Type-2 Routes	0
Reject Routes	0
Total Routes	0

Route Table Counters	
Best Routes (High)	0 (0)
Alternate Routes	0
Route Adds	0
Route Modifies	0
Route Deletes	0
Unresolved Route Adds	0
Invalid Route Adds	0
Failed Route Adds	0
Reserved Locals	0
Unique Next Hops (High)	0 (0)
Next Hop Groups (High)	0 (0)
ECMP Groups (High)	0 (0)
ECMP Routes	0
Truncated ECMP Routes	0
ECMP Retries	0

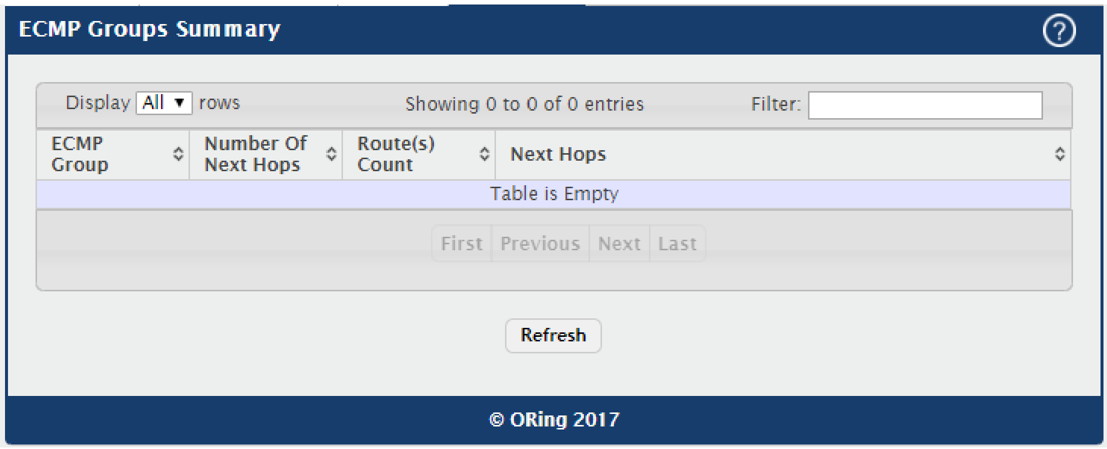
Field	Description
Connected Routes	The total number of connected routes in the IP routing table.
Static Routes	The total number of static routes in the IP routing table.
RIP Routes	The total number of routes installed by the RIP protocol.
BGP Routes	The total number of routes installed by the BGP protocol.
External	The total number of external routes installed by the BGP protocol.
Internal	The total number of internal routes installed by the BGP protocol.
Local	The total number of local routes installed by the BGP protocol.
OSPF Routes	The total number of routes installed by the OSPF protocol.
Intra Area Routes	The total number of intra-area routes installed by the OSPF protocol.
Inter Area	The total number of inter-area routes installed by the OSPF protocol.

Routes	
External Type-1 Routes	The total number of external type-1 routes installed by the OSPF protocol.
External Type-2 Routes	The total number of external type-2 routes installed by the OSPF protocol.
Reject Routes	The total number of reject routes installed by all protocols.
Total Routes	The total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes.
Next Hop Groups (High)	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops.
ECMP Groups	The number of next hop groups with multiple next hops.

(High)	
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hops	The current number of routes with each number of next hops.
Clear Counters	This button resets to zero IPv4 routing table counters reported in this page. This only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

5.1.3.4 ECMP Group

This page displays all current ECMP groups in the IPv4 routing table. An ECMP group is a set of two or more next hops used in one or more routes.



ECMP Group	Number Of Next Hops	Route(s) Count	Next Hops
Table is Empty			

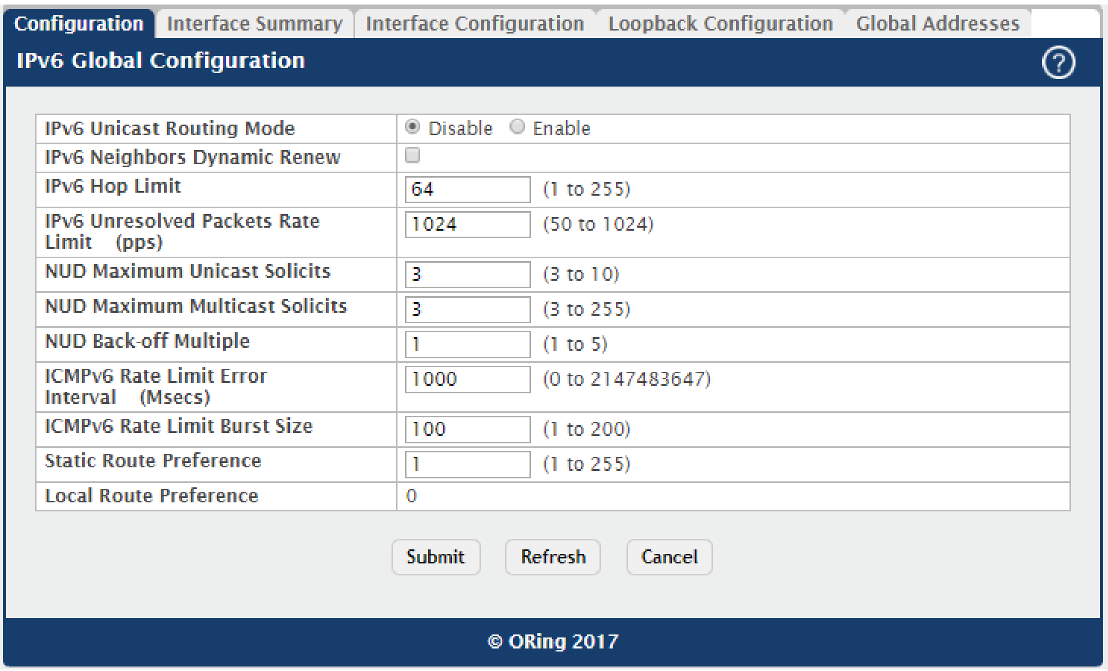
Field	Description
ECMP Group	The ECMP group number associated with the rest of the data in the row. The device assigns an arbitrary ECMP group number from 1 to n to identify the ECMP group.
Number Of Next	The number of next hops in the group.

Hops	
Route(s) Count	The number of routes that use the set of next hops.
Next Hops	The IPv4 address and outgoing interface of each next hop in the group.

5.1.4 IPv6

5.1.4.1 Configuration

Use this page to configure global IPv6 routing settings on the device. IPv6 routing provides a means of transmitting IPv6 packets between subnets on the network. IPv6 routing configuration is necessary only if the device is used as a Layer 3 device that routes IPv6 packets between subnets. IPv6 is the next generation of the Internet Protocol. With 128-bit addresses, versus 32-bit addresses for IPv4, IPv6 solves the address depletion issues seen with IPv4 and removes the requirement for Network Address Translation (NAT), which is used in IPv4 networks to reduce the number of globally unique IP addresses required for a given network.



IPv6 Unicast Routing Mode	● Disable ○ Enable
IPv6 Neighbors Dynamic Renew	□
IPv6 Hop Limit	64 (1 to 255)
IPv6 Unresolved Packets Rate Limit (pps)	1024 (50 to 1024)
NUD Maximum Unicast Solicits	3 (3 to 10)
NUD Maximum Multicast Solicits	3 (3 to 255)
NUD Back-off Multiple	1 (1 to 5)
ICMPv6 Rate Limit Error Interval (Msecs)	1000 (0 to 2147483647)
ICMPv6 Rate Limit Burst Size	100 (1 to 200)
Static Route Preference	1 (1 to 255)
Local Route Preference	0

Field	Description
IPv6 Unicast Routing Mode	The administrative mode of IPv6 routing on the device. The options are as follows: ・**Enable** – The device can act as a Layer 3 device by routing IPv6 packets between interfaces configured for IPv6 routing. ・**Disable** – The device does not support IPv6 routing.

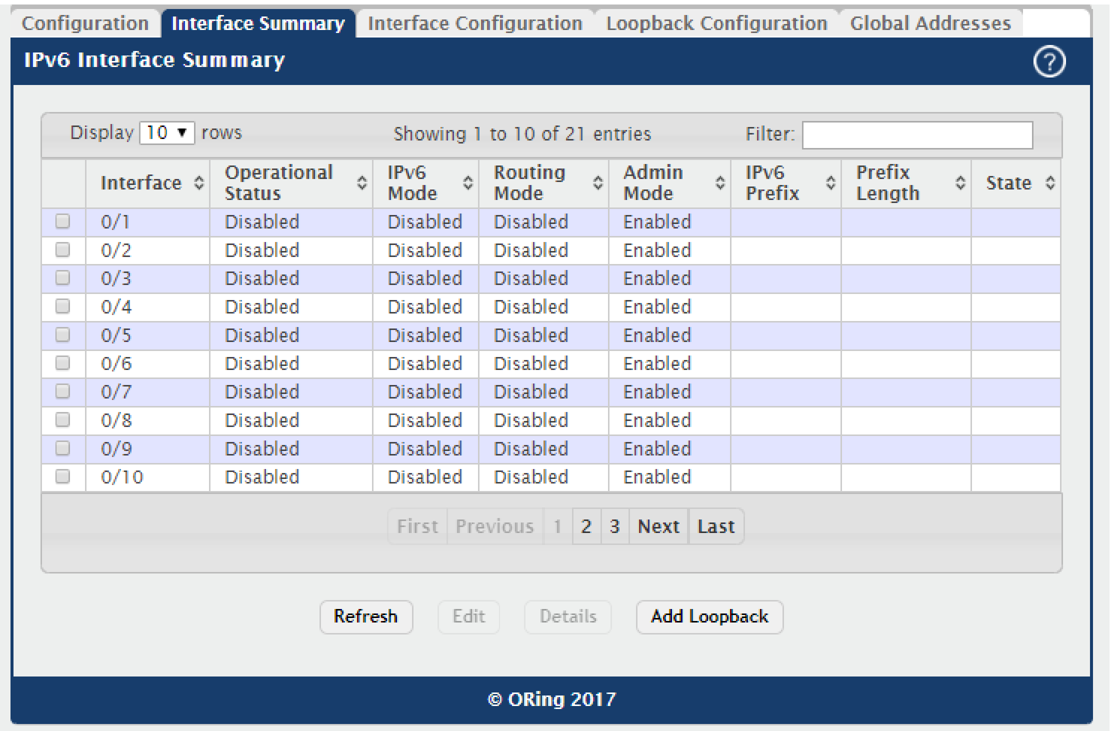
IPv6 Neighbors Dynamic Renew	Select this option to enable dynamic renewal mode for the periodic Neighbor Unreachability Detection (NUD) run on the existing IPv6 neighbor entries in the IPv6 neighbor cache. If NUD attempts to communicate with IPv6 neighbors and no response is received after the maximum number of solicits is reached, its entry is removed from the cache.
IPv6 Hop Limit	The unicast hop count used in IPv6 packets originated by the device. This value is also included in router advertisements.
IPv6 Unresolved Packets Rate Limit	The rate in packets-per-second for the number of IPv6 data packets trapped to the CPU when the packet fails to be forwarded in the hardware due to the unresolved hardware address of the destined IPv6 node.
NUD Maximum Unicast Solicits	The maximum number of unicast neighbor solicitations sent during NUD before switching to multicast neighbor solicitations.
NUD Maximum Multicast Solicits	The maximum number of multicast neighbor solicitations sent during NUD when a neighbor is in the UNREACHABLE state.
NUD Back-off Multiple	The exponential backoff multiplier to be used in the calculation of the next timeout value for neighbor solicitation transmission during NUD following the exponential backoff algorithm.
ICMPv6 Rate Limit Error Interval	The maximum burst interval for ICMPv6 error messages transmitted by the device. The rate limit for ICMPv6 error messages is configured as a token bucket. The ICMPv6 Rate Limit Error Interval specifies how often the token bucket is initialized with tokens of the size configured in the ICMPv6 Rate Limit Burst Size field.
ICMPv6 Rate Limit Burst Size	The number of ICMPv6 error messages that can be sent during the burst interval configured in the ICMPv6 Rate Limit Error Interval field.
Static Route Preference	The default distance (preference) for static IPv6 routes. Lower route-distance values are preferred when determining the best route. The value configured for Static Route Preference is used when using the CLI to configure a static route and no preference is specified. Changing the Static Route Preference does not update the preference of existing static routes.
Local Route Preference	The default distance (preference) for local IPv6 routes.

5.1.4.2 Interface Summary

This page shows summary information about the IPv6 routing configuration for all interfaces. Use the buttons to perform the following tasks:

To edit any interface, select the interface and click Edit. You are redirected to the **IPv6 Interface Configuration** or **IPv6 Loopback Configuration** page for the selected interface. To view additional routing configuration information for an interface, select the interface with the settings to view and click **Details.**

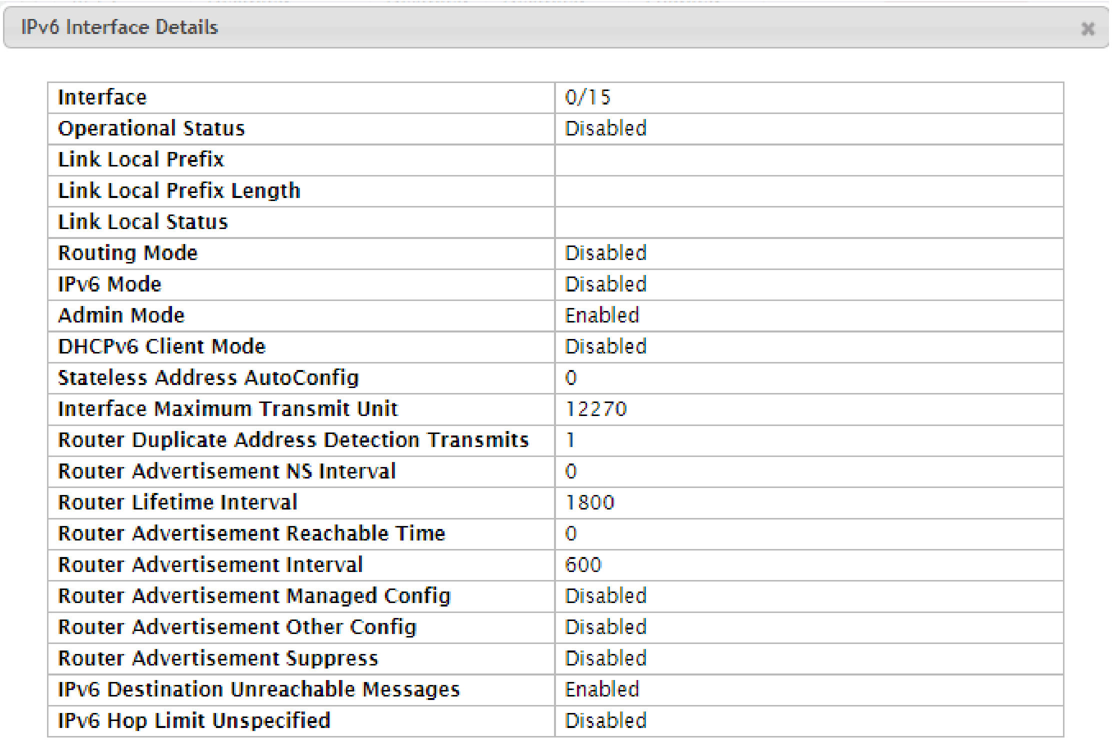
To add the next available loopback interface, click **Add Loopback**. You are redirected to the **IPv6 Loopback Configuration** page.



IPv6 Interface Summary

Display 10 ▾ rows   Showing 1 to 10 of 21 entries   Filter:

	Interface	Operational Status	IPv6 Mode	Routing Mode	Admin Mode	IPv6 Prefix	Prefix Length	State
□	0/1	Disabled	Disabled	Disabled	Enabled			
□	0/2	Disabled	Disabled	Disabled	Enabled			
□	0/3	Disabled	Disabled	Disabled	Enabled			
□	0/4	Disabled	Disabled	Disabled	Enabled			
□	0/5	Disabled	Disabled	Disabled	Enabled			
□	0/6	Disabled	Disabled	Disabled	Enabled			
□	0/7	Disabled	Disabled	Disabled	Enabled			
□	0/8	Disabled	Disabled	Disabled	Enabled			
□	0/9	Disabled	Disabled	Disabled	Enabled			
□	0/10	Disabled	Disabled	Disabled	Enabled			



IPv6 Interface Details

Interface	0/15
Operational Status	Disabled
Link Local Prefix	
Link Local Prefix Length	
Link Local Status	
Routing Mode	Disabled
IPv6 Mode	Disabled
Admin Mode	Enabled
DHCPv6 Client Mode	Disabled
Stateless Address AutoConfig	0
Interface Maximum Transmit Unit	12270
Router Duplicate Address Detection Transmits	1
Router Advertisement NS Interval	0
Router Lifetime Interval	1800
Router Advertisement Reachable Time	0
Router Advertisement Interval	600
Router Advertisement Managed Config	Disabled
Router Advertisement Other Config	Disabled
Router Advertisement Suppress	Disabled
IPv6 Destination Unreachable Messages	Enabled
IPv6 Hop Limit Unspecified	Disabled

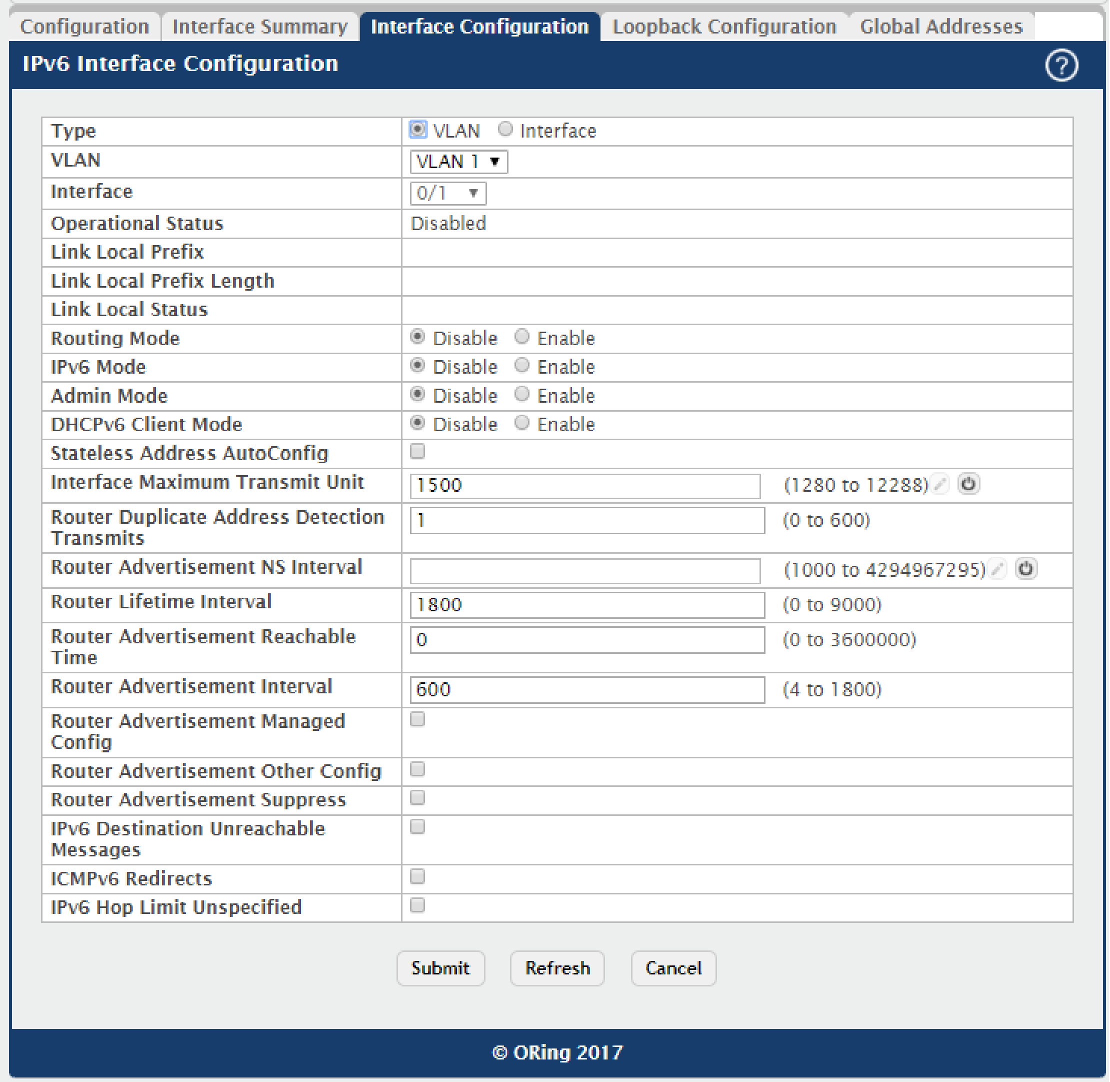
Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing details about the routing settings for an interface, this field identifies the interface being viewed.
Operational Status	The IPv6 routing operational mode on the interface. The operational mode is enabled under the conditions in the following list; otherwise, the mode is disabled: · The IPv6 mode is enabled on the interface. · The routing mode is enabled on the interface. · The administrative mode is enabled on the interface. · The link is up.
IPv6 Mode	The IPv6 mode on the interface. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used.
Routing Mode	Indicates whether Layer 3 routing is administratively enabled or disabled on the interface.
Admin Mode	The administrative mode on the interface.
IPv6 Prefix	The IPv6 routing prefix dynamically or manually configured on the interface.
Prefix Length	The number of bits used for the IPv6 prefix.

State	The state of the IPV6 address. The state is TENT if routing is disabled or Duplicate Address Detection (DAD) fails. The state is Active if the interface is active and DAD is successful. Otherwise, the state is Inactive. After you click **Details**, the **Details** window opens and displays detailed IPv6 routing information for the selected interface. The following information describes the fields in this window that are not displayed on the summary page.
Link Local Prefix	The autoconfigured link-local address which is: · Allocated from part of the IPv6 unicast address space · Not visible off the local link · Not globally unique
Link Local Prefix Lengthl	The number of bits used for the prefix of the link-local IPv6 address.
Link Local Status	The status of the IPV6 link local address. The status is TENT if routing is disabled or Duplicate Address Detection (DAD) fails. The state is Active if the interface is active and DAD is successful. Otherwise, the state is Inactive.
DHCPv6 Client Mode	The administrative mode of the DHCPv6 client on the interface. An interface can acquire an IPv6 address by communicating with a network DHCPv6 server (stateful configuration). An interface can also obtain an IPv6 address through stateless address autoconfiguration or static configuration.
Stateless Address AutoConfig	The administrative mode of stateless address autoconfiguration on the interface. When enabled, the interface can configure itself by using the Neighbor Discovery Protocol.
Interface Maximum Transmit Unit	The largest IPv6 packet size the interface can transmit, in bytes. To change the MTU value, click the Edit icon to the right of the field. To reset the MTU to the default value, click the Reset icon.
Router Duplicate Address Detection Transmits	The number of duplicate address detection probes the interface transmits while doing neighbor discovery.
Router Advertisement NS Interval	The interval between router advertisements for advertised neighbor solicitations. To change the interval, click the Edit icon to the right of the field. To reset the interval to the default value, click the Reset icon.

Router Lifetime Interval	The value that is placed in the Router Lifetime field of the router advertisements sent from the interface.
Router Advertisement Reachable Time	The value that is placed in the Reachable Time field of the router advertisements The amount of time to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	The transmission interval between router advertisements messages sent by the interface.
Router Advertisement Managed Config	The mode of the Managed Address Configuration flag in router advertisements sent from the interface. When enabled, the Managed Address Configuration flag is set in router advertisements, indicating that the interface should use stateful autoconfiguration (DHCPv6) to obtain addresses.
Router Advertisement Other Config	The mode of the Other Stateful Configuration flag in router advertisements sent from the interface. When enabled, the Other Stateful Configuration flag is set in router advertisements, indicating that the interface should use stateful autoconfiguration for information other than addresses.
Router Advertisement Suppress	The mode of router advertisement transmission suppression on an interface. When enabled, the interface does not transmit router advertisements.
IPv6 Destination Unreachable Messages	The mode for ICMPv6 Destination Unreachable messages. When enabled, the interface can send ICMPv6 Destination Unreachable messages back to the source device if a datagram is undeliverable.
IPv6 Hop Limit Unspecified	The mode that controls whether the interface transmits the hop limit value as 0 in Router Advertisements (Enabled) or transmits the global hop limit value (Disabled).

5.1.4.3 Interface Configuration

Use this page to configure the IPv6 routing settings for each non-loopback interface.



Type	● VLAN ○ Interface	
VLAN	VLAN 1 ▾	
Interface	0/1 ▾	
Operational Status	Disabled	
Link Local Prefix		
Link Local Prefix Length		
Link Local Status		
Routing Mode	● Disable ○ Enable	
IPv6 Mode	● Disable ○ Enable	
Admin Mode	● Disable ○ Enable	
DHCPv6 Client Mode	● Disable ○ Enable	
Stateless Address AutoConfig	□	
Interface Maximum Transmit Unit	1500	(1280 to 12288)
Router Duplicate Address Detection Transmits	1	(0 to 600)
Router Advertisement NS Interval		(1000 to 4294967295)
Router Lifetime Interval	1800	(0 to 9000)
Router Advertisement Reachable Time	0	(0 to 3600000)
Router Advertisement Interval	600	(4 to 1800)
Router Advertisement Managed Config	□	
Router Advertisement Other Config	□	
Router Advertisement Suppress	□	
IPv6 Destination Unreachable Messages	□	
ICMPv6 Redirects	□	
IPv6 Hop Limit Unspecified	□	

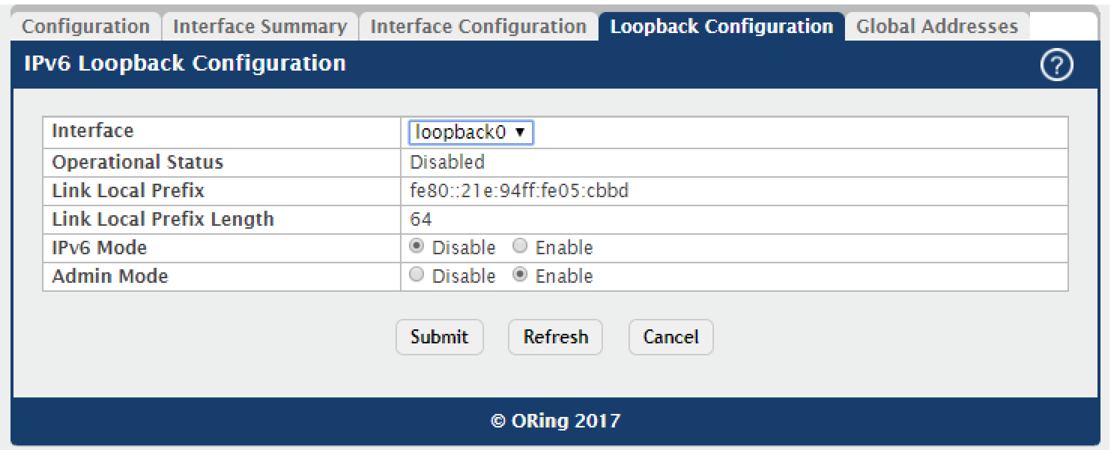
Field	Description
Type	The type of interface that can be configured for IPv6 routing: ・**Interface** – Enables list of all non-loopback interfaces that can be configured for IPv6 routing. ・**VLAN** – Enables list of all VLANs that can be configured for IPv6 routing.
VLAN	The menu contains all VLANs that can be configured for IPv6 routing. To configure routing settings for a VLAN, select it from the menu and then configure the rest of the settings on the page.
Interface	The menu contains all non-loopback interfaces that can be configured for IPv6 routing. To configure routing settings for an interface, select it

	from the menu and then configure the rest of the settings on the page.
Operational Status	The IPv6 routing operational mode on the interface. The operational mode is enabled under the conditions in the following list; otherwise, the mode is disabled: · The IPv6 mode is enabled on the interface. · The routing mode is enabled on the interface. · The administrative mode is enabled on the interface. · The link is up.
Link Local Prefix	The autoconfigured link-local address which is: · Allocated from part of the IPv6 unicast address space · Not visible off the local link · Not globally unique
Link Local Prefix Length	The number of bits used for the prefix of the link-local IPv6 address.
Link Local Status	The status of the IPV6 link local address. The status is TENT if routing is disabled or Duplicate Address Detection (DAD) fails. The state is Active if the interface is active and DAD is successful. Otherwise, the state is Inactive.
Routing Mode	The administrative mode for Layer 3 routing on the interface.
IPv6 Mode	The administrative mode for IPv6 on the interface. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used.
Admin Mode	The administrative mode of the interface. If an interface is administratively disabled, it will not forward traffic.
DHCPv6 Client Mode	The administrative mode of the DHCPv6 client on the interface. An interface can acquire an IPv6 address by communicating with a network DHCPv6 server (stateful configuration). An interface can also obtain an IPv6 address through stateless address autoconfiguration or static configuration.
Stateless Address AutoConfig	When this option is selected, the interface can generate its own IPv6 address by using local interface information and prefix information advertised by routers.
Interface Maximum Transmit Unit	The largest IPv6 packet size the interface can transmit, in bytes. To change the MTU value, click the Edit icon to the right of the field. To reset the MTU to the default value, click the Reset icon.
Router Duplicate Address	The number of duplicate address detection probes the interface transmits while doing neighbor discovery.

Detection Transmits	
Router Advertisement NS Interval	The interval between router advertisements for advertised neighbor solicitations. To change the interval, click the Edit icon to the right of the field. To reset the interval to the default value, click the Reset icon.
Router Lifetime Interval	The value that is placed in the Router Lifetime field of the router advertisements sent from the interface.
Router Advertisement Reachable Time	The value that is placed in the Reachable Time field of the router advertisements The amount of time to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	The transmission interval between router advertisements messages sent by the interface.
Router Advertisement Managed Config	When this option is selected, the Managed Address Configuration flag is set in router advertisements, indicating that the interface should use stateful autoconfiguration (DHCPv6) to obtain addresses.
Router Advertisement Other Config	When this option is selected, the Other Stateful Configuration flag is set in router advertisements, indicating that the interface should use stateful autoconfiguration for information other than addresses.
Router Advertisement Suppress	When this option is selected, the interface does not transmit router advertisements.
IPv6 Destination Unreachable Messages	When this option is selected, the interface can send ICMPv6 Destination Unreachable messages back to the source device if a datagram is undeliverable.
ICMPv6 Redirects	When this option is selected, the interface is allowed to send ICMPv6 Redirect messages. An ICMPv6 Redirect message notifies a host when a better route to a particular destination is available on the network segment.
IPv6 Hop Limit Unspecified	When this option is selected, the device can send Router Advertisements on this interface with an unspecified (0) current hop limit value. This will tell the hosts on the link to ignore the hop limit from this device.

5.1.4.4 LoopBack Configuration

Use this page to configure the IPv6 routing settings for each loopback interface. A loopback interface is a logical interface that is always up (as long as it is administratively enabled) and, because it cannot go down, allows the device to have a stable IPv6 address that other network nodes and protocols can use to reach the device. The loopback can provide the source address for sent packets. The loopback interface does not behave like a network switching port. Specifically, there are no neighbors on a loopback interface; it is a pseudodevice for assigning local addresses so that the other Layer 3 hosts can communicate with the device by using the loopback IPv6 address.



Interface	loopback0 ▾
Operational Status	Disabled
Link Local Prefix	fe80::21e:94ff:fe05:cbbd
Link Local Prefix Length	64
IPv6 Mode	● Disable ○ Enable
Admin Mode	○ Disable ● Enable

Field	Description
Interface	The menu contains all loopback interfaces that can be configured for IPv6 routing. To configure routing settings for an interface, select it from the menu and then configure the rest of the settings on the page.
Operational Status	The operational status of the loopback interface. To be operational, both the IPv6 mode and administrative mode must be enabled.
Link Local Prefix	The autoconfigured link-local address which is: · Allocated from part of the IPv6 unicast address space · Not visible off the local link · Not globally unique
Link Local Prefix Length	The number of bits used for the prefix of the link-local IPv6 address.
IPv6 Mode	The IPv6 mode on the loopback interface. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is use
Admin Mode	The administrative mode of the loopback interface.

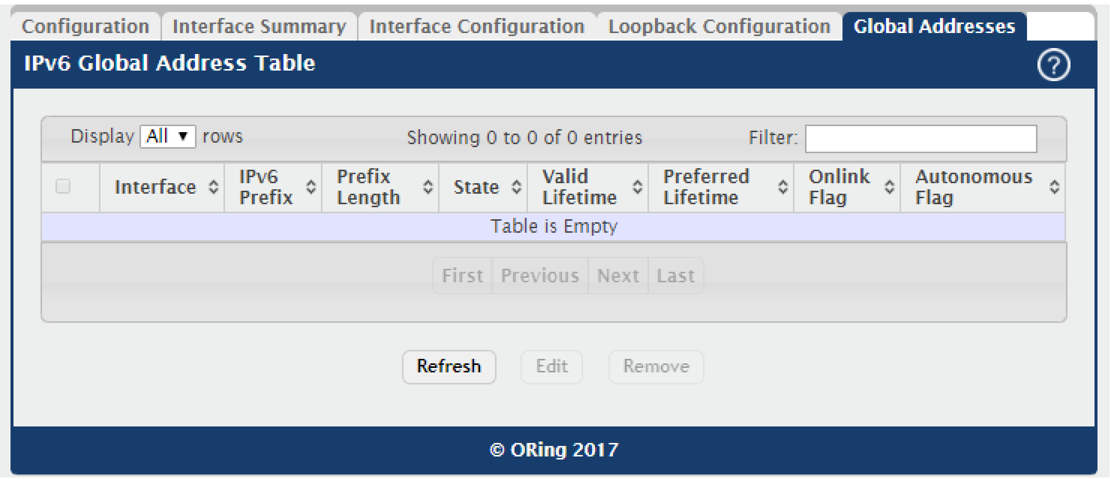
5.1.4.5 Global Address

This page shows information about all global IPv6 addresses configured on all interfaces on the device. From this page, you can also remove a configured IPv6 address from an interface.

Use the buttons to perform the following tasks:

· To edit any interface, select the interface and click **Edit**. You are redirected to the **IPv6 Global Address Configuration** page for the selected interface.

· To delete the IPv6 address configuration from one or more interfaces, select each entry to remove and click **Remove**. You must confirm the action.



□	Interface	IPv6 Prefix	Prefix Length	State	Valid Lifetime	Preferred Lifetime	Onlink Flag	Autonomous Flag
Table is Empty								

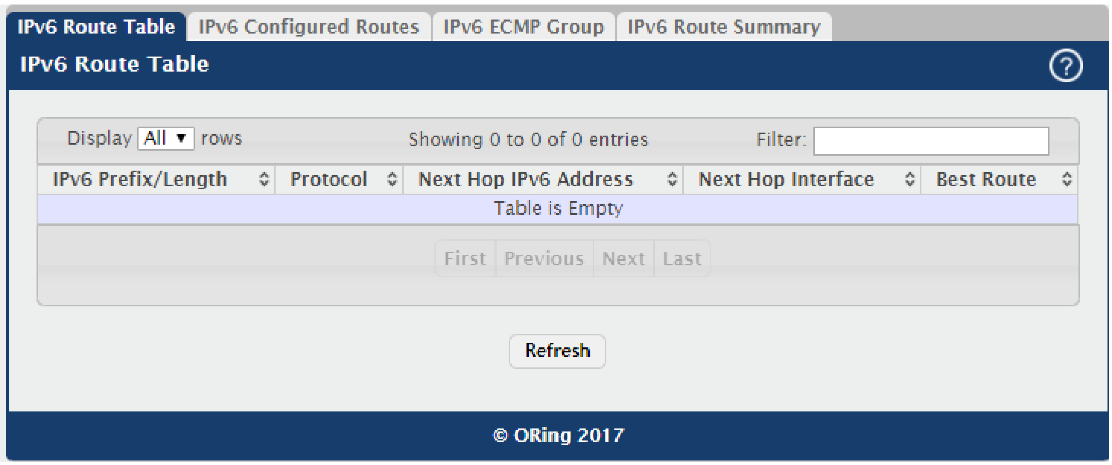
Field	Description
Interface	The interface associated with the rest of the data in the row.
IPv6 Prefix	The IPv6 routing prefix dynamically or manually configured on the interface. This page does not show information about link-local addresses.
Prefix Length	The number of bits used for the IPv6 prefix.
State	The link state, which is either Active or Inactive.
Valid Lifetime	The value, in seconds, to be placed in the Valid Lifetime field of the Prefix Information option in a router advertisement. The prefix is valid for on-link determination for this length of time. Hosts that generate an address from this prefix using stateless address auto-configuration can use those addresses for this length of time. An auto-configured address older than the preferred lifetime but younger than the valid lifetime are considered deprecated addresses. As defined by RFC 2462, a deprecated address is "An address assigned to an interface whose use is discouraged, but not forbidden. A deprecated address

	should no longer be used as a source address in new communications, but packets sent from or to deprecated addresses are delivered as expected. A deprecated address may continue to be used as a source address in communications where switching to a preferred address causes hardship to a specific upper-layer activity (e.g., an existing TCP connection)." If you specify the maximum value, an autoconfigured address may remain preferred indefinitely.
Preferred Lifetime	The value, in seconds, to be placed in the Preferred Lifetime in the Prefix Information option in a router advertisement. Addresses generated from a prefix using stateless address autoconfiguration remain preferred for this length of time. As defined by RFC 2462, a preferred address is "an address assigned to an interface whose use by upper layer protocols is unrestricted. Preferred addresses may be used as the source (or destination) address of packets sent from (or to) the interface." If you specify the maximum value, an autoconfigured address may remain preferred indefinitely
Onlink Flag	The state of the on-link flag in the IPv6 prefix. When enabled, the prefix can be used for on-link determination by other hosts with IPv6 addresses within this prefix.
Autonomous Flag	The state of the autonomous flag in the IPv6 prefix. When enabled, the prefix can be used for autonomous address configuration by other hosts (in combination with an interface identifier on the other hosts).

5.1.5 IPv6 Routes

5.1.5.1 IPv6 Route Table

This page displays the entries in the IPv6 routing table, including all dynamically learned and statically configured entries. The device uses the routing table to determine how to forward IPv6 packets. A statically-configured route does not appear in the table until it is reachable.



IPv6 Prefix/Length	Protocol	Next Hop IPv6 Address	Next Hop Interface	Best Route
Table is Empty				

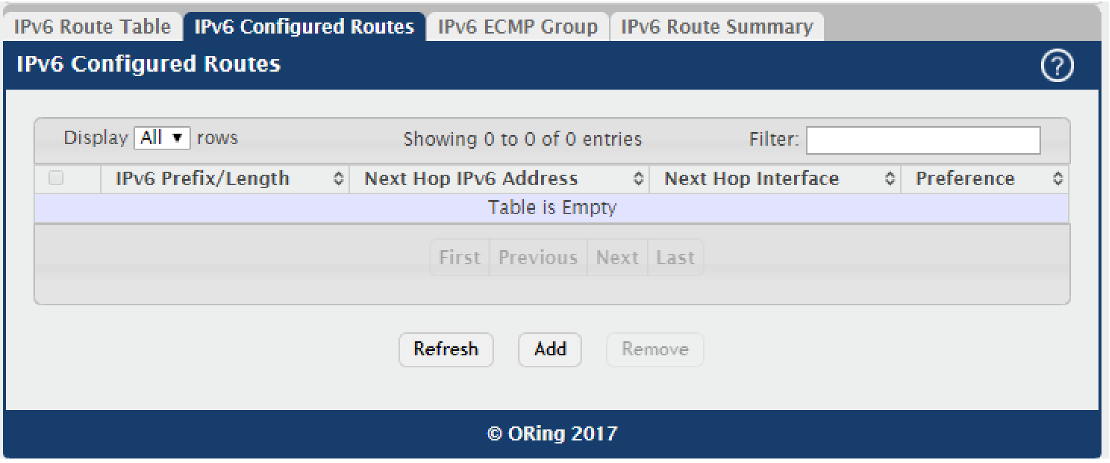
Field	Description
IPv6 Prefix/Length	The IPv6 address, including the prefix and prefix length, for the destination network.
Protocol	Identifies which protocol created the route. A route can be created one of the following ways: · Dynamically learned through a supported routing protocol · Dynamically learned by being a directly-attached local route · Statically configured by an administrator
Next Hop IPv6 Address	The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IPv6 address of the local interface for a directly-attached network.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null.
Best Route	Indicates whether the route is the preferred route to the network. If the field is blank, a better route to the same network exists in the IPv6 routing table.

5.1.5.2 IPv6 Configured Routes

Use this page to configure static IPv6 global, link local, and static reject routes in the routing table. The page shows the routes that have been manually added to the routing table.

Use the buttons to perform the following tasks:

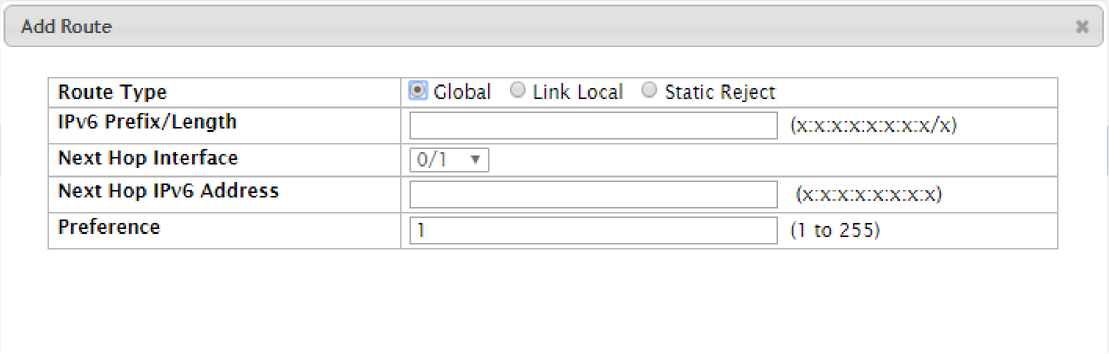
- To configure a new IPv6 route, click Add and specify the desired settings in the available fields.
- To remove a configured IPv6 route, select each entry to delete and click Remove. You must confirm the action before the entry is deleted.



IPv6 Configured Routes

Display All ▾ rows   Showing 0 to 0 of 0 entries   Filter:

□	IPv6 Prefix/Length	Next Hop IPv6 Address	Next Hop Interface	Preference
Table is Empty				



Add Route

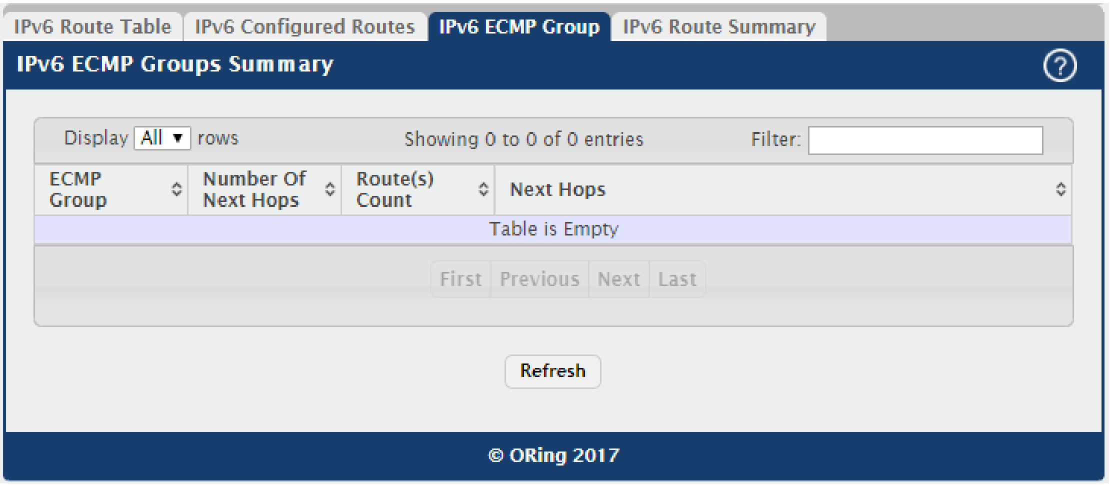
Route Type	● Global ○ Link Local ○ Static Reject
IPv6 Prefix/Length	(x:x:x:x:x:x:x:x/x)
Next Hop Interface	0/1 ▾
Next Hop IPv6 Address	(x:x:x:x:x:x:x:x)
Preference	1 (1 to 255)

Field	Description
IPv6 Prefix/Length	The IPv6 address, including the prefix and prefix length, for the destination network.
Next Hop IPv6 Address	The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IPv6 address of the local interface for a directly-attached network.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null. The next hop

	is Unresolved until the device is able to reach the interface.
Preference	The preference of the route. A lower preference value indicates a more preferred route. When the routing table has more than one route to the same network, the device selects the route with the best (lowest) route preference.
Route Type	The type of route to configure, which is one of the following: ・**Global** – A route with an address that is globally routable and is recognized outside of the local network. ・**Link Local** – A route with an address that is allocated from part of the IPv6 unicast address space. it is not visible off the local link and is not globally unique. ・**Static Reject** – A route where packets that match the route are discarded instead of forwarded. The device might send an ICMPv6 Destination Unreachable message.

5.1.5.3 IPv6 ECMP Group

This page displays all current Equal Cost Multipath (ECMP) groups in the IPv6 routing table. An ECMP group is a set of two or more next hops used in one or more routes.



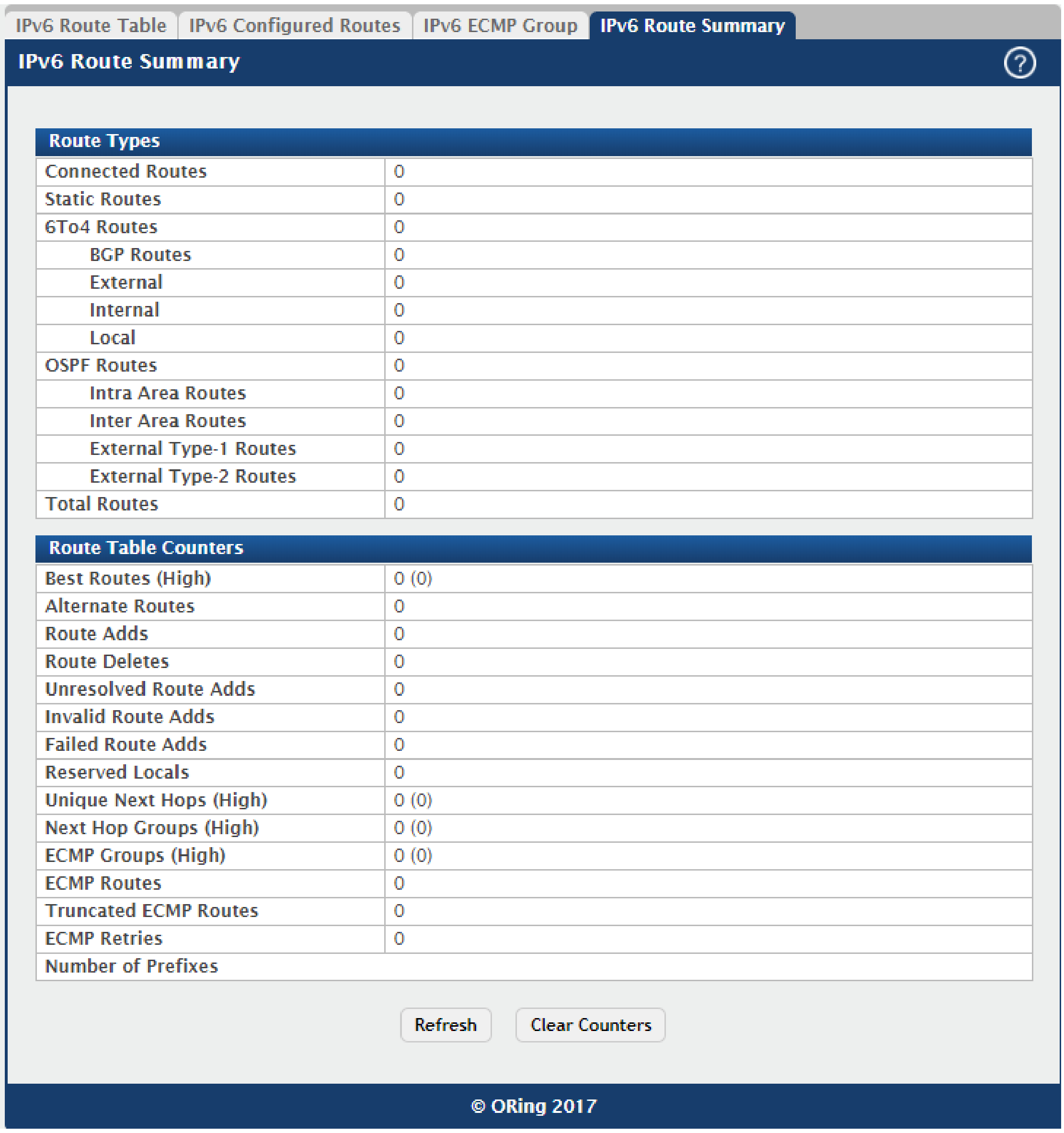
ECMP Group	Number Of Next Hops	Route(s) Count	Next Hops
Table is Empty			

Field	Description
ECMP Group	The ECMP group number associated with the rest of the data in the row. The device assigns an arbitrary ECMP group number from 1 to n to identify the ECMP group.
Number Of Next Hops	The number of next hops in the group.
Route(s) Count	The number of routes that use the set of next hops.

Next Hops	The IPv6 address and outgoing interface of each next hop in the group.

5.1.5.4 IPv6 Route Summary

This page displays summary information about the entries in the IPv6 routing table.



Route Types	
Connected Routes	0
Static Routes	0
6To4 Routes	0
BGP Routes	0
External	0
Internal	0
Local	0
OSPF Routes	0
Intra Area Routes	0
Inter Area Routes	0
External Type-1 Routes	0
External Type-2 Routes	0
Total Routes	0

Route Table Counters	
Best Routes (High)	0 (0)
Alternate Routes	0
Route Adds	0
Route Deletes	0
Unresolved Route Adds	0
Invalid Route Adds	0
Failed Route Adds	0
Reserved Locals	0
Unique Next Hops (High)	0 (0)
Next Hop Groups (High)	0 (0)
ECMP Groups (High)	0 (0)
ECMP Routes	0
Truncated ECMP Routes	0
ECMP Retries	0
Number of Prefixes	

Field	Description
Connected Routes	The total number of connected routes in the IPv6 routing table.
Static Routes	The total number of static routes in the IPv6 routing table.
6To4 Routes	The total number of 6to4 routes in the IPv6 routing table. A 6to4 route allows IPv6 sites to communicate with each other over an IPv4

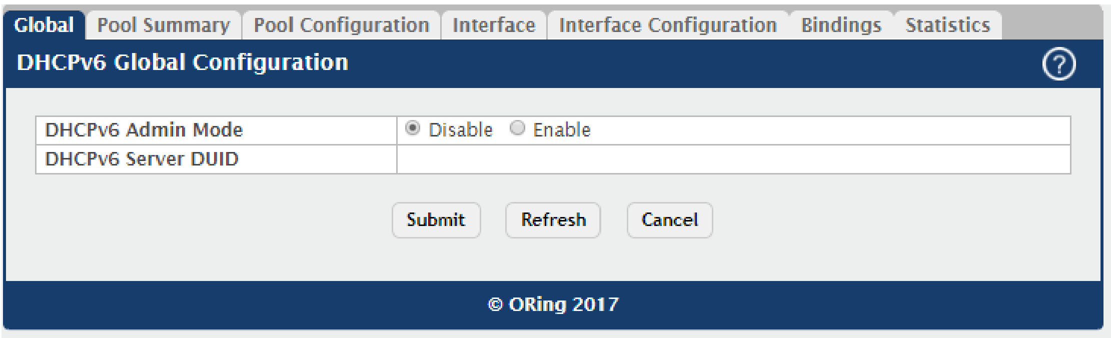
	network by treating the wide-area IPv4 network as a unicast point-to-point link layer.
BGP Routes	The total number of routes installed by the BGP protocol. **External** The total number of external routes installed by the BGP protocol. **Internal** The total number of internal routes installed by the BGP protocol. **Local** The total number of local routes installed by the BGP protocol.
OSPF Routes	The total number of routes installed by the OSPFv3 protocol. **Intra Area Routes** The total number of intra-area routes installed by the OSPFv3 protocol. **Inter Area Routes** The total number of inter-area routes installed by the OSPFv3 protocol. **External Type-1 Routes** The total number of external type-1 routes installed by the OSPFv3 protocol. **External Type-2 Routes** The total number of external type-2 routes installed by the OSPFv3 protocol.
Reject Routes	The total number of reject routes installed by all protocols.
Total Routes	The total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number counts only the best route to each destination.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.

Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes.
Next Hop Groups (High)	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops.
ECMP Groups (High)	The number of next hop groups with multiple next hops.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Number of Prefixes	The unique IPv6 prefixes in the IPv6 routing table.
Clear Counters (Button)	This button resets all IPv6 routing table event counters on this page to zero. Not that only event counters are reset; counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

5.1.6 DHCPv6

5.1.6.1 Global

Use this page to configure the global Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server settings on the device. The device can act as a DHCPv6 server or DHCPv6 relay agent to help assign network configuration information to IPv6 clients.



DHCPv6 Admin Mode	● Disable ○ Enable
DHCPv6 Server DUID	

Field	Description
DHCPv6 Admin Mode	The administrative mode of the DHCPv6 server.
DHCPv6 Server DUID	The DHCP Unique Identifier (DUID) of the DHCPv6 server.

5.1.6.2 Pool Summary

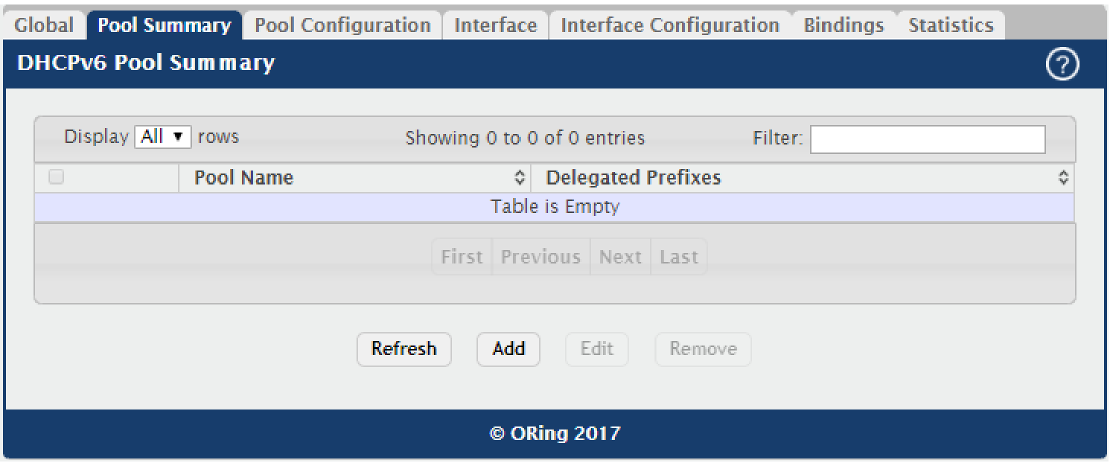
Use this page to view the currently configured DHCPv6 server pools and to add and remove pools. A DHCPv6 server pool is a set of network configuration information available to DHCPv6 clients that request the information.

Use the buttons to perform the following tasks:

· To add a pool, click **Add** and configure the pool information in the available fields.

· To remove a pool, select each entry to delete and click **Remove**. You must confirm the action before the pool is deleted.

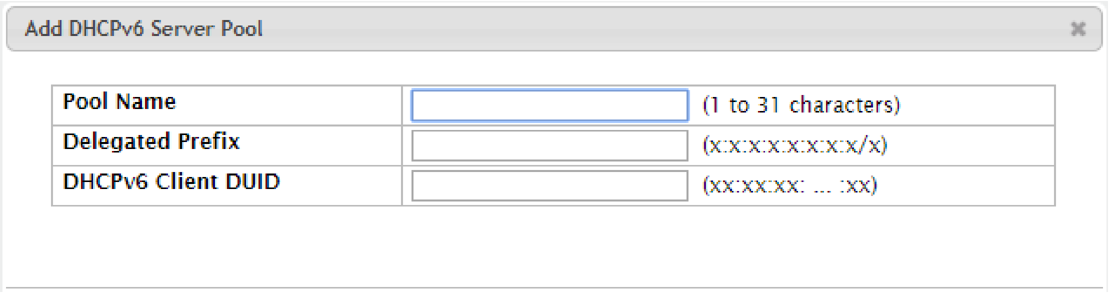
· To change the settings for a pool, select the entry to update and click **Edit**. You are redirected to the **DHCPv6 Pool Configuration** page for the selected pool. From this page, you can configure additional bindings within the pool.



DHCPv6 Pool Summary

Display All ▾ rows Showing 0 to 0 of 0 entries Filter:

□	Pool Name	Delegated Prefixes
Table is Empty		


Add DHCPv6 Server Pool

Pool Name		(1 to 31 characters)
Delegated Prefix		(x:x:x:x:x:x:x:x/x)
DHCPv6 Client DUID		(xx:xx:xx: ... :xx)

Field	Description
Pool Name	The name that identifies the DHCPv6 server pool.
Delegated Prefixes	The general prefix in the pool for use in allocating and assigning addresses to hosts that may be utilizing IPv6 auto-address configuration or acting as DHCPv6 clients.
DHCPv6 Client DUID	The DHCP Unique Identifier (DUID) of the client. The DUID is a combination of the client's hardware address and client identifier.

5.1.6.3 Pool Configuration

Use this page to edit pool settings or to configure additional settings for existing DHCPv6 pools.

To add, remove, or update binding entries within a pool or update other pool configuration information, you must first select the DHCPv6 pool from the Pool Name menu. After you select the pool to configure, use the icons on the page to perform the following tasks:

‧ To add a new binding to the selected DHCPv6 pool, click the + (plus) icon in the header row above the binding entries.

‧ To remove all bindings from the selected pool, click the – (minus) icon in the header row above the binding entries.

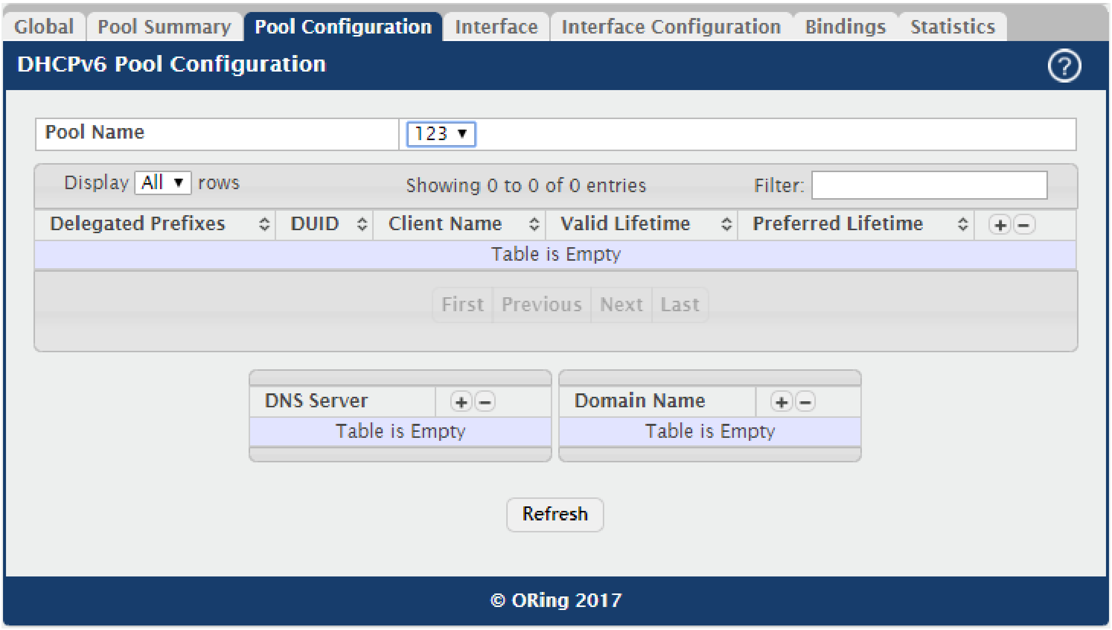
‧ To update the information for a binding, click the Edit icon associated with the binding.

‧ To remove a binding from the selected pool, click the – (minus) icon associated with the binding.

‧To add DNS server or domain name information to a pool, click the + (plus) icon in the header row of the DNS Server or Domain Name field.

‧ To remove all configured DNS server or domain name entries from the selected pool, click the – (minus) icon in the header row of the DNS Server or Domain Name field.

‧ To remove a single DNS or domain name entry, click the – (minus) icon associated with the entry to remove.



DHCPv6 Pool Configuration

Pool Name	123 ▾

Display All ▾ rows   Showing 0 to 0 of 0 entries   Filter:

Delegated Prefixes	DUID	Client Name	Valid Lifetime	Preferred Lifetime	+ –
Table is Empty					

DNS Server	+ –
Table is Empty	

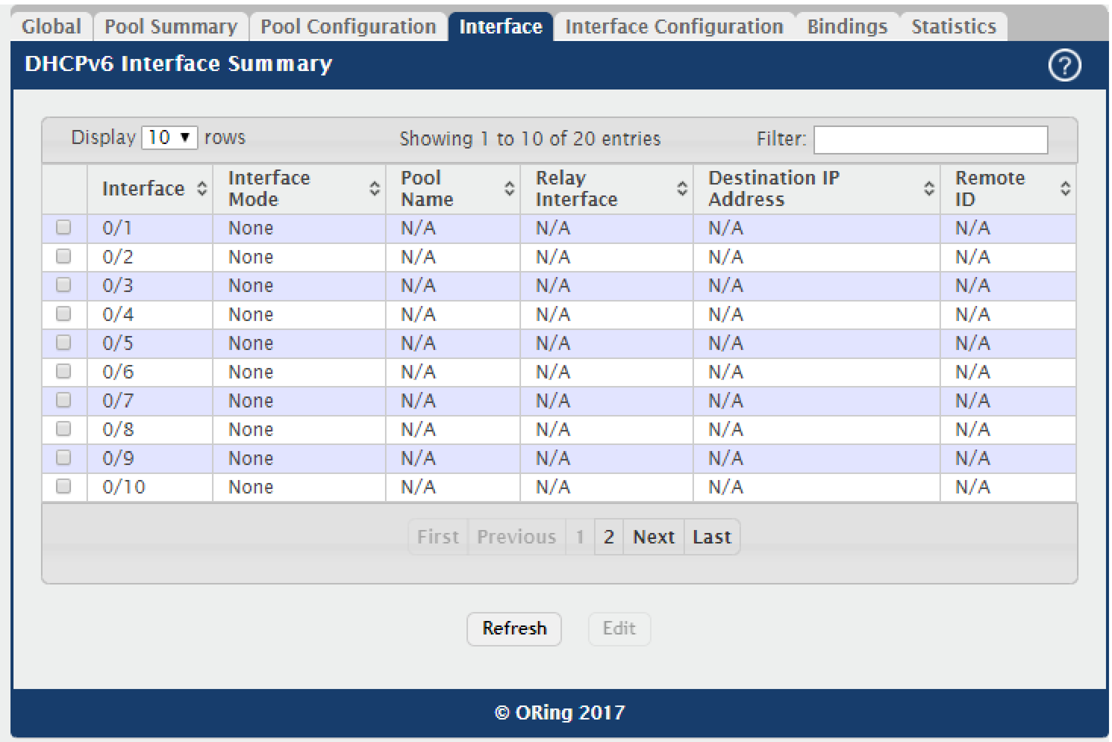
Domain Name	+ –
Table is Empty	

Field	Description
Pool Name	The menu includes all DHCPv6 server pools that have been configured on the device.
Delegated Prefixes	The IPv6 prefix and prefix length to assign the requesting client.
DUID	The DHCP Unique Identifier (DUID) of the client. The DUID is a combination of the client's hardware address and client identifier.
Client Name	The optional system name associated with the client.
Valid Lifetime	The maximum amount of time the requesting client is allowed to use the prefix.
Prefer Lifetime	The preferred amount of time the requesting client is allowed to use the prefix. The value of the **Prefer Lifetime** must be less than the value of the **Valid Lifetime.**
DNS Server	The IPv6 prefix of each DNS server each client in the pool can contact to perform address resolution.
Domain Name	The domain name configured for each client in the pool.
Server	The role of the DHCPv6 server in address assignment, which can be one of the following: ・**Stateful** – The server centrally manages address assignment, and clients must use the server to obtain configuration information, such as address auto configuration and neighbor discovery, that is not available through protocols. ・**Prefix Delegation** – The server does not need to maintain any dynamic state for individual clients, but the server must provide Domain Name System (DNS) server addresses and domain search list options.

After you click the + (plus) icon in the header row above the binding entries or click the **Edit** icon associated with the binding, the **Add Prefix** or **Edit Prefix** window opens and allows you to add or edit entries. The following information describes the additional field in these windows.

5.1.6.4 Interface

Use this page to view the per-interface settings for DHCPv6. To configure the settings, select the interface to configure and click **Edit**. You are redirected to the **DHCPv6 Interface Configuration** page for the selected interface.



DHCPv6 Interface Summary

Display 10 rows   Showing 1 to 10 of 20 entries   Filter:

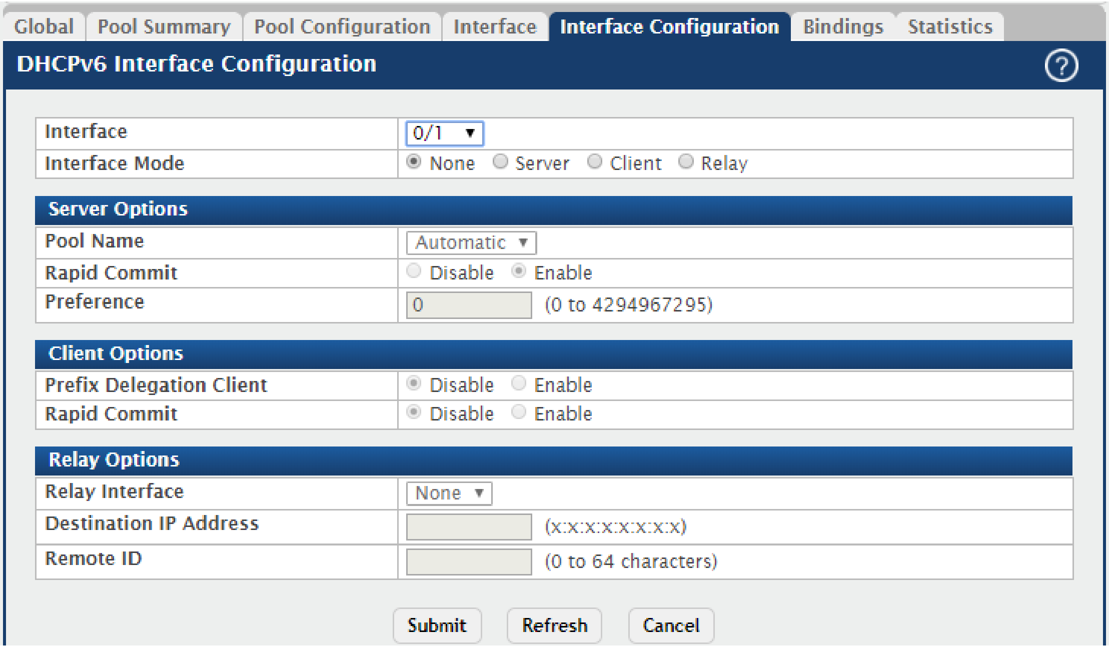
	Interface	Interface Mode	Pool Name	Relay Interface	Destination IP Address	Remote ID
□	0/1	None	N/A	N/A	N/A	N/A
□	0/2	None	N/A	N/A	N/A	N/A
□	0/3	None	N/A	N/A	N/A	N/A
□	0/4	None	N/A	N/A	N/A	N/A
□	0/5	None	N/A	N/A	N/A	N/A
□	0/6	None	N/A	N/A	N/A	N/A
□	0/7	None	N/A	N/A	N/A	N/A
□	0/8	None	N/A	N/A	N/A	N/A
□	0/9	None	N/A	N/A	N/A	N/A
□	0/10	None	N/A	N/A	N/A	N/A

Field	Description
Interface	The interface associated with the rest of the data in the row.
Interface Mode	The DHCPv6 function configured on the interface, which is one of the following: ・**None** – The interface is not configured as a DHCPv6 server or DHCPv6 relay agent. ・**Server** – The interface responds to requests from DHCPv6 clients. ・**Client** – The initiates requests on a link to obtain configuration parameters from one or more DHCPv6 servers. ・**Relay** – The interface acts as an intermediary to deliver DHCPv6 messages between clients and servers. The interface is on the same link as the client.
Pool Name	(DHCPv6 server interface only) The name of the DHCPv6 pool the server uses to assign client information.
Relay Interface	(DHCPv6 relay agent interface only) The interface on the device through which a DHCPv6 server is reached.

Destination IP Address	(DHCPv6 relay agent interface only) The destination IPv6 address of the DHCPv6 server to which client packets are forwarded.
Remote ID	(DHCPv6 relay agent interface only) The relay agent information option remote-ID sub-option to be added to relayed messages. This value is derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

5.1.6.5 Interface Configuration

Use this page to configure the per-interface settings for DHCPv6. With the larger address space inherent to IPv6, addresses within a network can be allocated more effectively in a hierarchical fashion. DHCPv6 introduces the notion of prefix delegation as described in RFC 3633 as a way for devices to centralize and delegate IPv6 address assignment. An interface can act as an IPv6 prefix delegation server that defines one or more general prefixes to delegate to a device lower in the hierarchy acting as a prefix delegation client. The device with an interface configured as a prefix delegation client can then allocate more specific addresses within the given general prefix range to assign to its local router interfaces. This device can, in turn, use the given general prefix in allocating and assigning addresses to host machines that may be utilizing IPv6 auto-address configuration or acting as DHCPv6 clients. An interface can also be configured as a DHCPv6 relay agent that acts as an intermediary to deliver DHCPv6 messages between clients and servers and is on the same link as the client. The DHCPv6 interface modes are mutually exclusive. The fields that can be configured on this page depend on the selected mode for the interface.



DHCPv6 Interface Configuration

Interface	0/1 ▾
Interface Mode	● None ○ Server ○ Client ○ Relay

Server Options

Pool Name	Automatic ▾
Rapid Commit	○ Disable ● Enable
Preference	0 (0 to 4294967295)

Client Options

Prefix Delegation Client	● Disable ○ Enable
Rapid Commit	● Disable ○ Enable

Relay Options

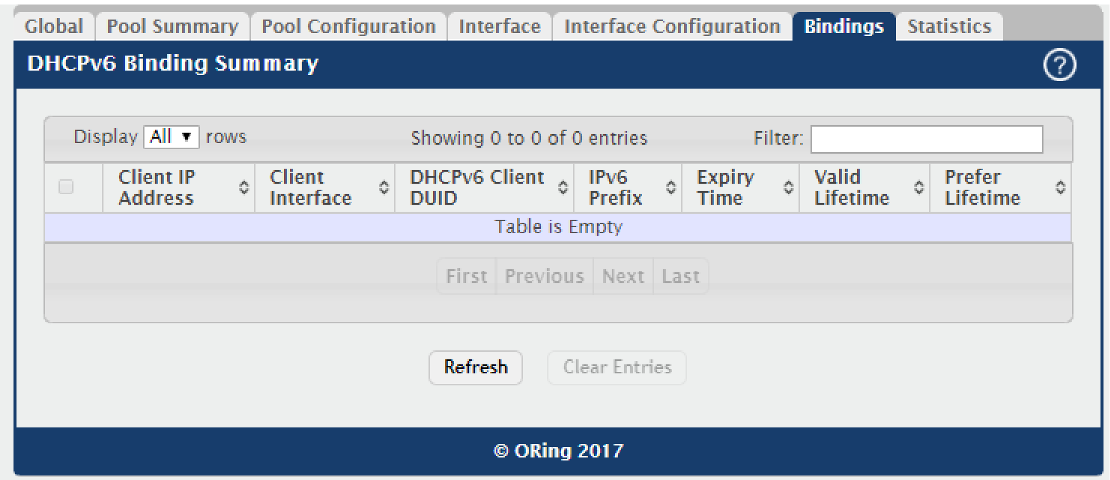
Relay Interface	None ▾
Destination IP Address	(x:x:x:x:x:x:x:x)
Remote ID	(0 to 64 characters)

Field	Description
Interface	Select the interface with the information to view or configure.
Interface Mode	The DHCPv6 function configured on the interface, which is one of the following: ・**None** – The interface is not configured as a DHCPv6 server or DHCPv6 client or DHCPv6 relay agent. ・**Server** – The interface responds to requests from DHCPv6 clients. ・**Client** – The interface initiates requests on a link to obtain configuration parameters from one or more DHCPv6 servers. ・**Relay** – The interface acts as an intermediary to deliver DHCPv6 messages between clients and servers. The interface is on the same link as the client.
Server Options	The information in this section can be configured only if the selected Interface Mode is Server. **Pool Name** The name of the DHCPv6 pool the server can use to assign client information. **Rapid Commit** The mode of the rapid commit message exchange on the DHCPv6 server interface. The DHCPv6 client can obtain configuration parameters from a server either through a rapid two-message exchange (solicit, reply) or through a four-message exchange (solicit, advertise, request, and reply). When this option is disabled on either the client or server, the four-message exchange is used. When this option is enabled on both the client and the server, the two-message exchange is used. **Preference** The preference value to include in DHCPv6 Advertise messages. If a DHCPv6 client receives Advertise messages from multiple DHCPv6 servers, it responds to the server with the highest preference value.
Client Options	The information in this section can be configured only if the selected Interface Mode is Client. **Prefix Delegation Client** When enabled, the interface can receive a general prefix for assignment to local router interfaces. **Rapid Commit**

	The mode of the rapid commit message exchange on the DHCPv6 client interface. The DHCPv6 client can obtain configuration parameters from a server either through a rapid two-message exchange (solicit, reply) or through a four-message exchange (solicit, advertise, request, and reply). When this option is disabled on either the client or server, the four-message exchange is used. When this option is enabled on both the client and the server, the two-message exchange is used.
Relay Options	The information in this section can be configured only if the selected Interface Mode is Relay. **Relay Interface** The interface on the device through which a DHCPv6 server is reached. **Destination IP Address** The destination IPv6 address of the DHCPv6 server to which client packets are forwarded. **Remote ID** The relay agent information option remote-ID sub-option to be added to relayed messages. This value is derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

5.1.6.6 Bindings

Use this page to view entries in the DHCP Bindings table. After a client acquires IPv6 configuration information from the DHCPv6 server, the server adds an entry to its database. The entry is called a binding.



DHCPv6 Binding Summary

Display All rows   Showing 0 to 0 of 0 entries   Filter:

□	Client IP Address	Client Interface	DHCPv6 Client DUID	IPv6 Prefix	Expiry Time	Valid Lifetime	Prefer Lifetime
Table is Empty							

Field	Description
Client IP Address	The IPv6 address associated with the client.
Client Interface	The interface number where the client binding occurred.
DHCPv6 Client DUID	The DHCP Unique Identifier (DUID) of the client. The DUID is a combination of the client's hardware address and client identifier.
IPv6 Prefix	The type of prefix associated with this binding
Expiry Time	The number of seconds until the prefix associated with a binding expires.
Valid Lifetime	The maximum amount of time the client is allowed to use the prefix.
Prefer Lifetime	The preferred amount of time the client is allowed to use the prefix.
Clear Entries (Button)	To remove an entry from the table, select each entry to delete and click Clear Entries. You must confirm the action before the binding is deleted.

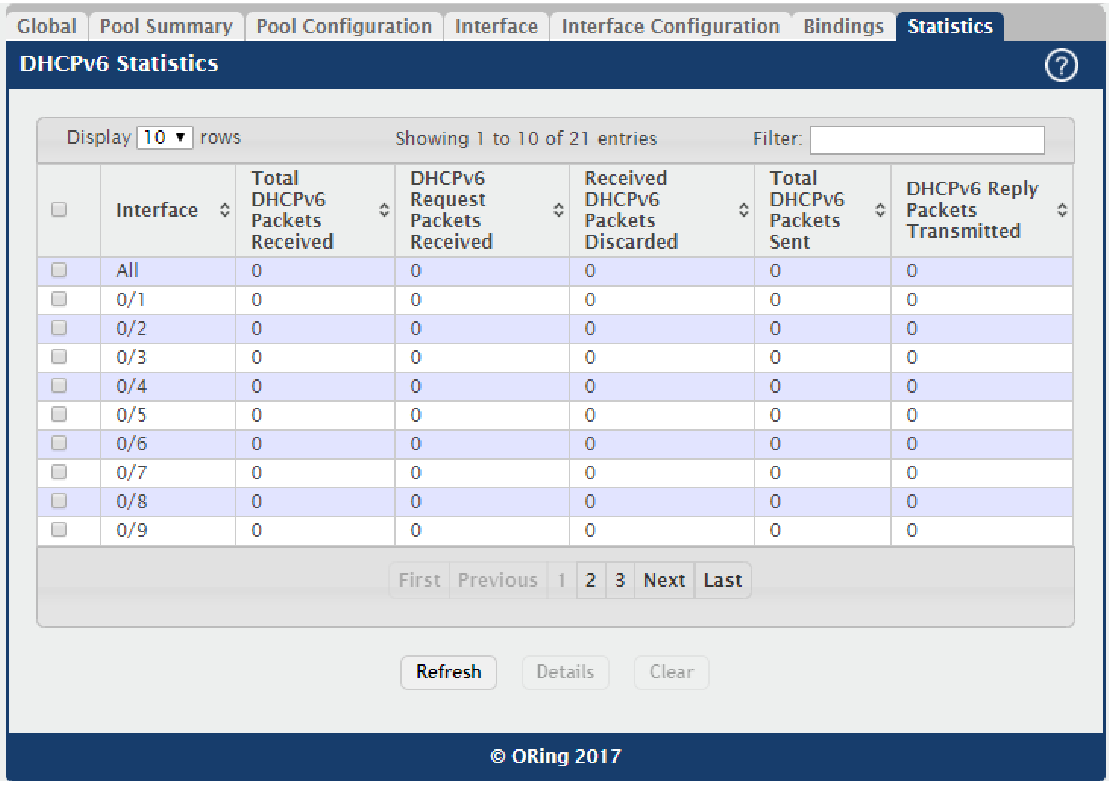
5.1.6.7 Statistics

This page displays the DHCPv6 server statistics for the device, including information about the DHCPv6 messages sent, received, and discarded globally and on each interface. The values on this page indicate the various counts that have accumulated since they were last cleared.

Use the buttons to perform the following tasks:

·To view detailed DHCPv6 statistics for an interface, select the entry with the information to view and click **Details.**

·To reset the DHCPv6 counters for one or more interfaces, select each interface with the statistics to reset and click **Clear.**



□	Interface	Total DHCPv6 Packets Received	DHCPv6 Request Packets Received	Received DHCPv6 Packets Discarded	Total DHCPv6 Packets Sent	DHCPv6 Reply Packets Transmitted
□	All	0	0	0	0	0
□	0/1	0	0	0	0	0
□	0/2	0	0	0	0	0
□	0/3	0	0	0	0	0
□	0/4	0	0	0	0	0
□	0/5	0	0	0	0	0
□	0/6	0	0	0	0	0
□	0/7	0	0	0	0	0
□	0/8	0	0	0	0	0
□	0/9	0	0	0	0	0

Field	Description
Interface	The interface associated with the rest of the data in the row. The row at the top of the table (All) contains cumulative statistics for all interfaces.
Total DHCPv6 Packets Received	The number of DHCPv6 messages received on the interface. The DHCPv6 messages sent from a DHCPv6 client to a DHCPv6 server include Solicit, Request, Confirm, Renew, Rebind, Release, Decline, and Information-Request messages. Additionally, a DHCPv6 relay agent can forward Relay-Forward messages to a DHCPv6 server.
DHCPv6 Request Packets Received	The number of DHCPv6 Request messages received on the interface. DHCPv6 Request messages are sent by a client to request IPv6 configuration information from the server.
Received DHCPv6 Packets Discarded	The number of DHCPv6 messages received on the interface that were discarded due to errors or because they were invalid.
Total DHCPv6 Packets Sent	The number of DHCPv6 messages sent by the interface. The DHCPv6 messages sent from a DHCPv6 server to a DHCPv6 client include Advertise, Reply, Reconfigure, and Relay-Reply messages.
DHCPv6 Reply	The number of DHCPv6 Reply messages sent from the interface to a

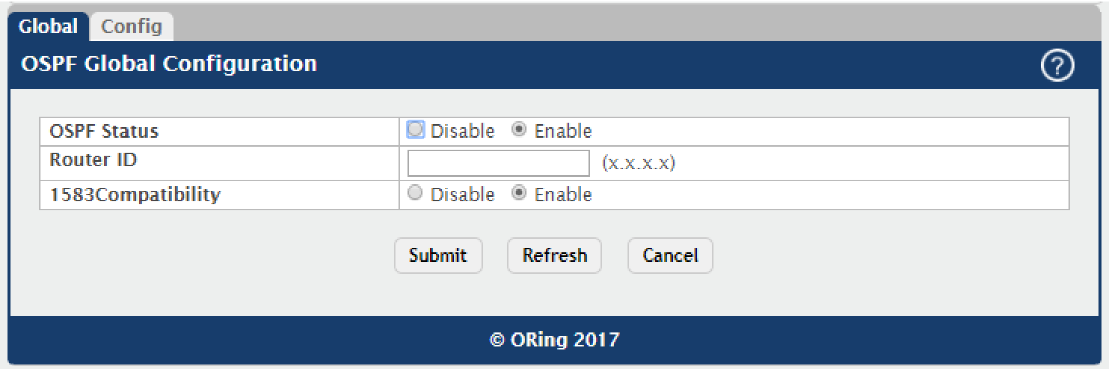
Packets Transmitted	DHCPv6 client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Solicit Packets Received	The number of DHCPv6 Solicit messages received on the interface. This type of message is sent by a client to locate DHCPv6 servers.
DHCPv6 Confirm Packets Received	The number of DHCPv6 Confirm messages received on the interface. This type of message is sent by a client to all DHCPv6 servers to determine whether its configuration is valid for the connected link.
DHCPv6 Renew Packets Received	The number of DHCPv6 Renew messages received on the interface. This type of message is sent by a client to extend and update the configuration information provided by the DHCPv6 server.
DHCPv6 Rebind Packets Received	The number of DHCPv6 Rebind messages received on the interface. This type of message is sent by a client to any DHCPv6 server when it does not receive a response to a Renew message.
DHCPv6 Release Packets Received	The number of DHCPv6 Release messages received on the interface. This type of message is sent by a client to indicate that it no longer needs the assigned address.
DHCPv6 Decline Packets Received	The number of DHCPv6 Decline messages received on the interface. This type of message is sent by a client to the DHCPv6 server to indicate that an assigned address is already in use on the link.
DHCPv6 Inform Packets Received	The number of DHCPv6 Information-Request messages received on the interface. This type of message is sent by a client to request configuration information other than IP address assignment.
DHCPv6 Relay-forward Packets Received	The number of DHCPv6 Relay-Forward messages received on the interface. This type of message is sent by a relay agent to forward messages to servers.
DHCPv6 Relay-reply Packets Received	The number of DHCPv6 Relay-Reply messages received on the interface. This type of message is sent by a server to a DHCPv6 relay agent and contains the message for the relay agent to deliver to the client.
DHCPv6 Malformed Packets Received	The number of DHCPv6 messages that were received on the interface but were dropped because they were malformed.
DHCPv6 Advertisement	The number of DHCPv6 Advertise messages sent by the interface. This type of message is sent by a server to a DHCPv6 client in

Packets Transmitted	response to a Solicit message and indicates that it is available for service.
DHCPv6 Reconfig Packets Transmitted	The number of DHCPv6 Reconfigure messages sent by the interface. This type of message is sent by a server to a DHCPv6 client to inform the client that the server has new or updated information. The client then typically initiates a Renew/Reply or Information-request/Reply transaction with the server to receive the updated information.
DHCPv6 Relay-forward Packets Transmitted	The number of DHCPv6 Relay-Forward messages sent by the interface. This type of message is sent by a relay agent to forward messages to servers.
DHCPv6 Relay-reply Packets Transmitted	The number of DHCPv6 Relay-Reply messages sent by the interface. This type of message is sent by a server to a DHCPv6 relay agent and contains the message for the relay agent to deliver to the client.

5.1.7 OSPF

5.1.7.1 Global

Use this page to configure the global Open Shortest Path First protocol settings on the device. OSPF is a link-state protocol. OSPF supports variable-length subnet masks.

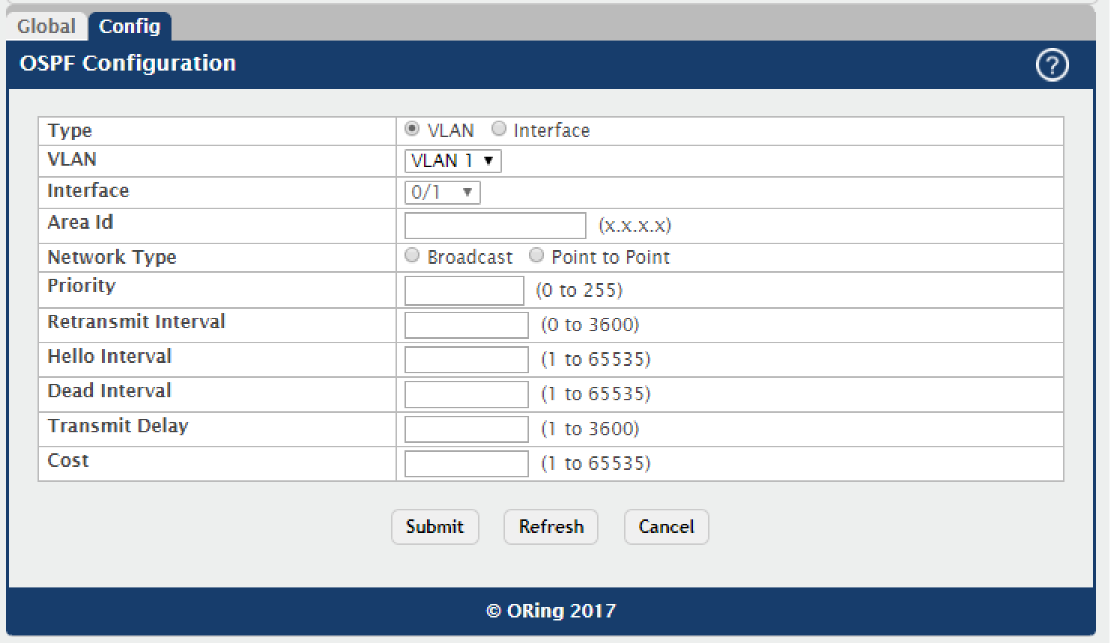


OSPF Status	○ Disable ● Enable
Router ID	(x.x.x.x)
1583Compatibility	○ Disable ● Enable

Field	Description
OSPF Status	The administrative mode of the OSPF.
Router ID	The 4-digit dotted-decimal number uniquely identifying the router ospf id.
1583Compatibility	The mode of OSPF 1583 compatibility.

5.1.7.2 Config

Use this page to configure OSPF settings.



Type	● VLAN ○ Interface
VLAN	VLAN 1 ▾
Interface	0/1 ▾
Area Id	(x.x.x.x)
Network Type	○ Broadcast ○ Point to Point
Priority	(0 to 255)
Retransmit Interval	(0 to 3600)
Hello Interval	(1 to 65535)
Dead Interval	(1 to 65535)
Transmit Delay	(1 to 3600)
Cost	(1 to 65535)

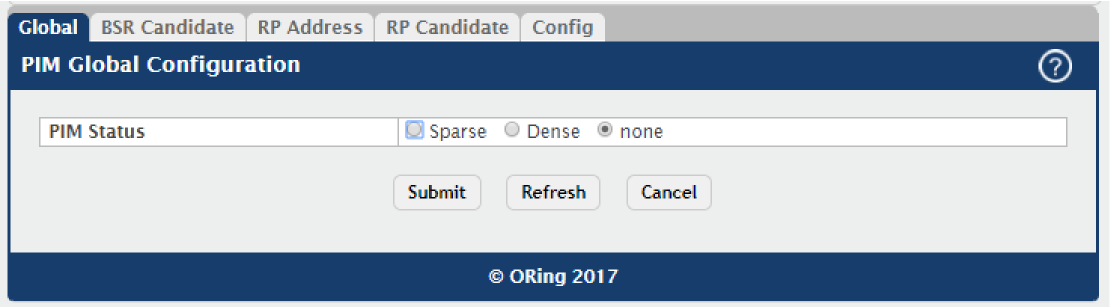
Field	Description
Type	Select type between VLAN or Interface.
VLAN	Select target VLAN.
Interface	Select target interface.
Area Id	The OSPF Area ID for the specified interface. The area-id is an IP address formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0-4294967295.
Network Type	The type of network on this interface that the OSPF is running on. OSPF treats interfaces as broadcast interfaces by default. (Loopback interfaces have a special loopback network type, which cannot be changed.) When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.
Priority	A number representing the OSPF Priority for the specified interface. A value of 0 indicates that the router is not eligible to become the designated router on this network.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface. The value for seconds is the number of seconds between

	link-state advertisement retransmissions for adjacencies belonging to this router interface. This vlaue is also used when retransmitting database description and link-state request packets.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a common network.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4).
Transmit Delay	A number representing the OSPF Transmit Delay for the specified interface. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface.
Cost	The cost on an OSPF interface.

5.1.8 PIM

5.1.8.1 Global

Use this page to configure the global Protocol Independent Multicast protocol settings on the device. Protocol Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol.



PIM Global Configuration

PIM Status ○ Sparse ○ Dense ● none

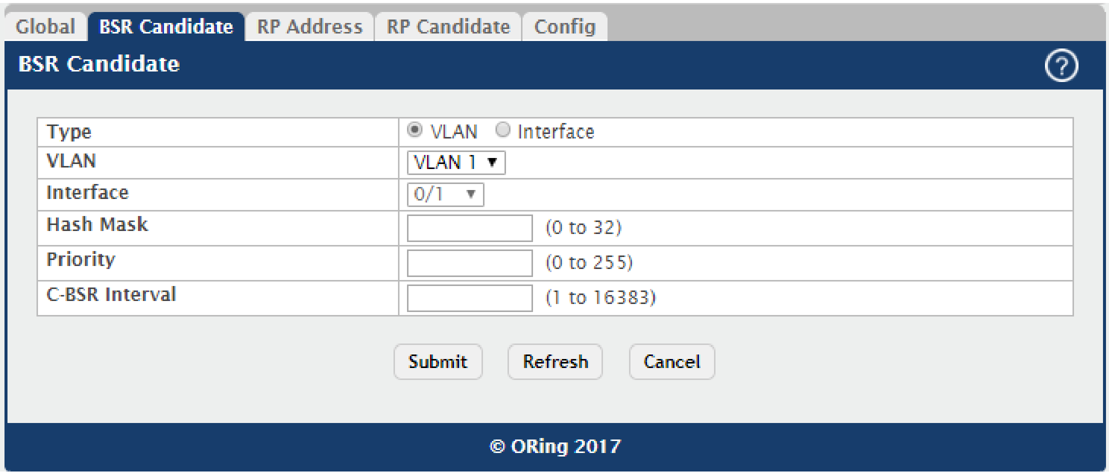
© ORing 2017

Field	Description
Sparse Mode (SM)	used to efficiently route multicast traffic to multicast groups that may span wide area networks where bandwidth is a constraint

Dense Mode (DM)	most appropriate for networks with relatively plentiful bandwidth and with at least one multicast member in each subnet.
None	Disable PIM Function

5.1.8.2 BSR Candidate

Use this page to configure BSR candidate settings.



Type	● VLAN ○ Interface
VLAN	VLAN 1 ▼
Interface	0/1 ▼
Hash Mask	(0 to 32)
Priority	(0 to 255)
C-BSR Interval	(1 to 16383)

Field	Description
Type	Select type between VLAN or Interface.
VLAN	Select target VLAN.
Interface	Select target interface.
Hash Mask	Length of a mask(32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
Priority	Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR.
C-BSR Interval	Indicates the BSR candidate advertisement interval. The range is from 1 to 16383 seconds.

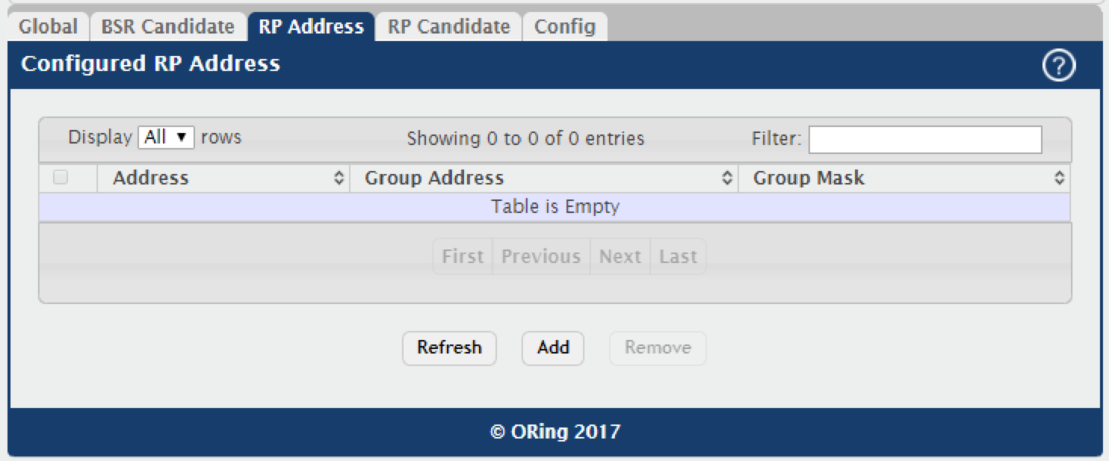
5.1.8.3 RP Address

Use this page to view and manage the contents of the PIM RP address table. The table shows the mapping for the PIM group to the active Rendezvous points (RP) of which the router is a aware.

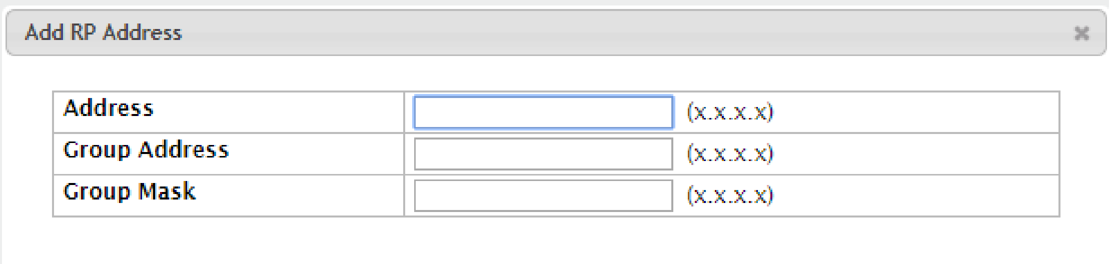
Use the buttons to perform the following tasks:

・To add a static entry, click **Add**. The **Add RP Address** dialog box opens. Specify the new entry information in the available fields.

・To delete one or more entries, select each entry to delete and click Remove.



□	Address	Group Address	Group Mask
Table is Empty			



Address		(x.x.x.x)
Group Address		(x.x.x.x)
Group Mask		(x.x.x.x)

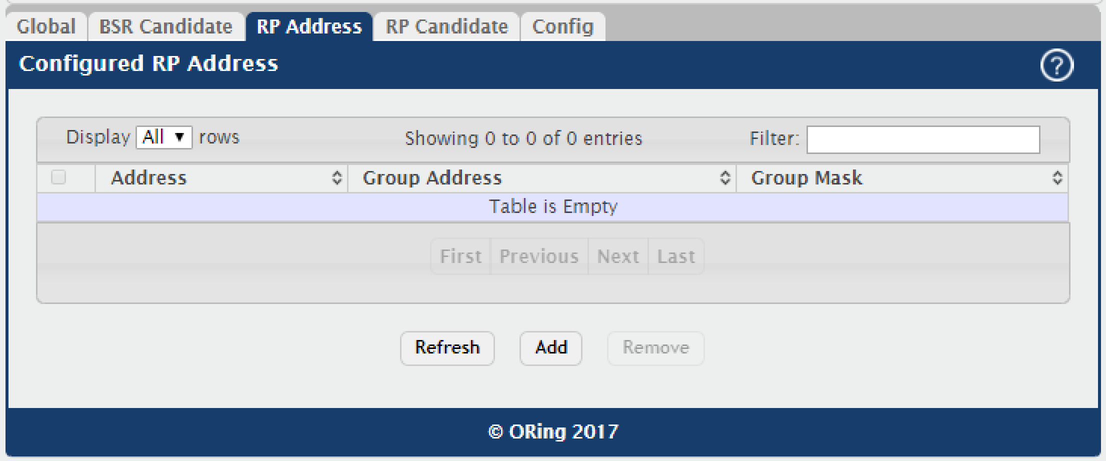
Field	Description
Address	The IP address of the RP.
Group Address	The group address supported by the RP.
Group Mask	The group mask for the group address.

5.1.8.4 RP Candidate

Use this page to view and manage the contents of the PIM RP candidate table. To configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR) for a specific multicast group range.

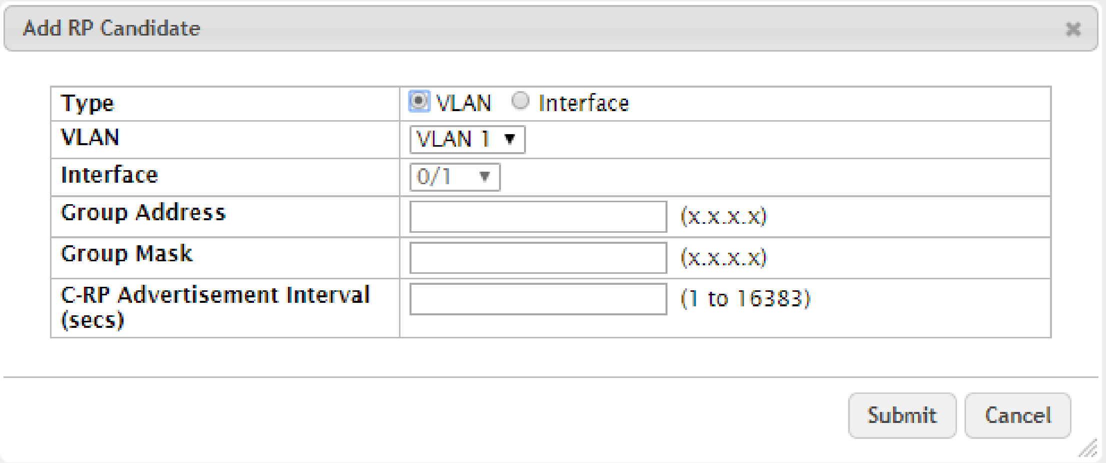
Use the buttons to perform the following tasks:

- To add a static entry, click **Add**. The **Add RP Candidate** dialog box opens. Specify the new entry information in the available fields.
- To delete one or more entries, select each entry to delete and click **Remove.**



Configured RP Address

☐	Address	Group Address	Group Mask
	Table is Empty		



Add RP Candidate

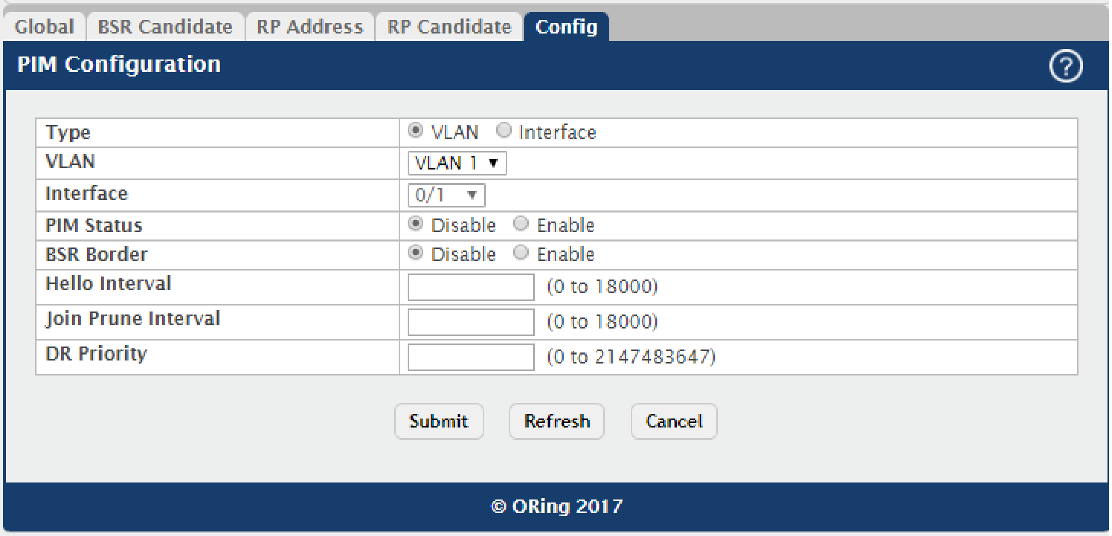
Type	● VLAN ○ Interface
VLAN	VLAN 1 ▾
Interface	0/1 ▾
Group Address	(x.x.x.x)
Group Mask	(x.x.x.x)
C-RP Advertisement Interval (secs)	(1 to 16383)

Field	Description
Type	Select type between VLAN or Interface.
VLAN	Select target VLAN.
Interface	Select target interface.
Group Address	The multicast group address that is advertised in association with the RP adddress.
Group Mask	The multicast group prefix that is advertised in association with the RP

	adddress.
C-RP Advertisement Interval(sec)	Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds.

5.1.8.5 Config

Use this page to configure PIM settings.



Type	● VLAN ○ Interface
VLAN	VLAN 1 ▾
Interface	0/1 ▾
PIM Status	● Disable ○ Enable
BSR Border	● Disable ○ Enable
Hello Interval	(0 to 18000)
Join Prune Interval	(0 to 18000)
DR Priority	(0 to 2147483647)

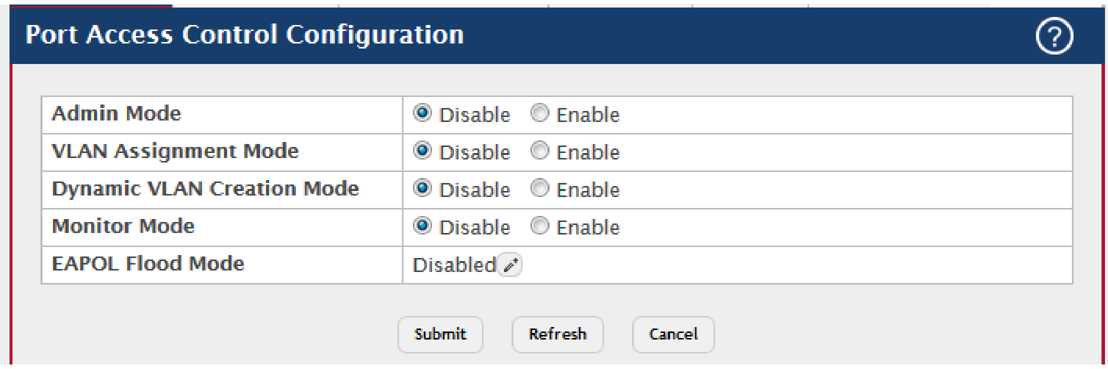
Field	Description
Type	Select type between VLAN or Interface.
VLAN	Select target VLAN.
Interface	Select target interface.
PIM Status	The administrative mode of the PIM.
BSR Border	Configure this interface as a bootstrap router border interface.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface.
Join Prune Interval	The join/prune interval value for the PIM router.
DR Priority	The priority of the Designated Router configured on the interface.

6.1 Security

6.1.1 Port Access Control

6.1.1.1 Configuration

Use this page to configure the global Port Access Control settings on the device. The port-based access control feature uses IEEE 802.1X to enable the authentication of system users through a local internal server or an external server. Only authenticated and approved system users can transmit and receive data. Supplicants (clients connected to authenticated ports that request access to the network) are authenticated using the Extensible Authentication Protocol (EAP). Also supported are PEAP, EAP-TTL, EAP-TTLS, and EAP-TLS.



Port Access Control Configuration

Admin Mode	● Disable ○ Enable
VLAN Assignment Mode	● Disable ○ Enable
Dynamic VLAN Creation Mode	● Disable ○ Enable
Monitor Mode	● Disable ○ Enable
EAPOL Flood Mode	Disabled

Field	Description
Admin Mode	The administrative mode of port-based authentication on the device.
VLAN Assignment Mode	The administrative mode of RADIUS-based VLAN assignment on the device. When enabled, this feature allows a port to be placed into a particular VLAN based on the result of the authentication or type of 802.1X authentication a client uses when it accesses the device. The authentication server can provide information to the device about which VLAN to assign the supplicant.
Dynamic VLAN Creation Mode	The administrative mode of dynamic VLAN creation on the device. If RADIUS-assigned VLANs are enabled, the RADIUS server is expected to include the VLAN ID in the 802.1X tunnel attributes of its response message to the device. If dynamic VLAN creation is enabled on the device and the RADIUS-assigned VLAN does not exist, then the assigned VLAN is dynamically created. This implies that the client can connect from any port and can get assigned to the appropriate VLAN. This feature gives flexibility for clients to move around the network without much additional configuration required.

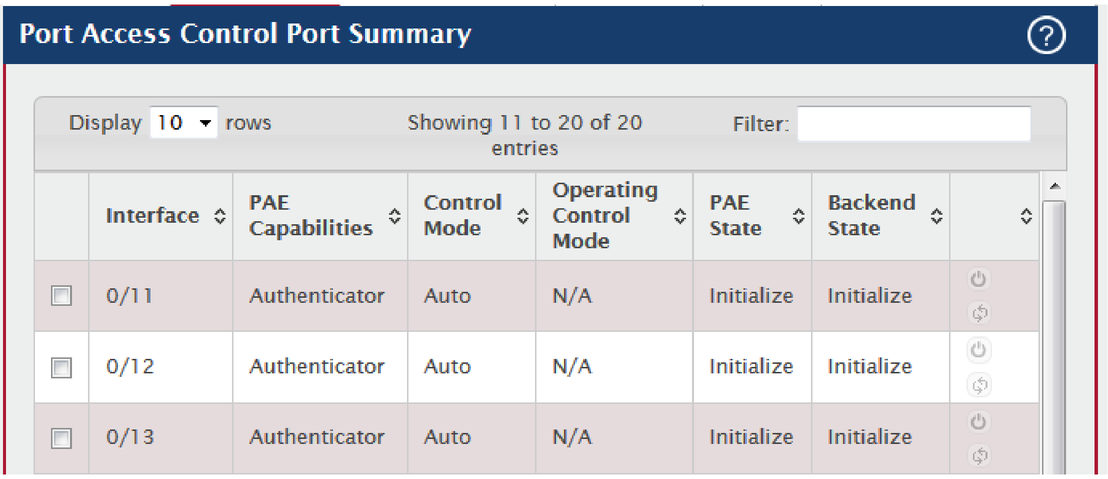
Monitor Mode	The administrative mode of the Monitor Mode feature on the device. Monitor mode is a special mode that can be enabled in conjunction with port-based access control. Monitor mode provides a way for network administrators to identify possible issues with the port-based access control configuration on the device without affecting the network access to the users of the device. It allows network access even in cases where there is a failure to authenticate, but it logs the results of the authentication process for diagnostic purposes. If the device fails to authenticate a client for any reason (for example, RADIUS access reject from the RADIUS server, RADIUS timeout, or the client itself is 802.1X unaware), the client is authenticated and is undisturbed by the failure condition(s). The reasons for failure are logged and buffered into the local logging database for tracking purposes.
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.

6.1.1.2 Port Summary

Use this page to view summary information about the port-based authentication settings for each port.

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.



Port Access Control Port Summary

Display 10 rows Showing 11 to 20 of 20 entries Filter:

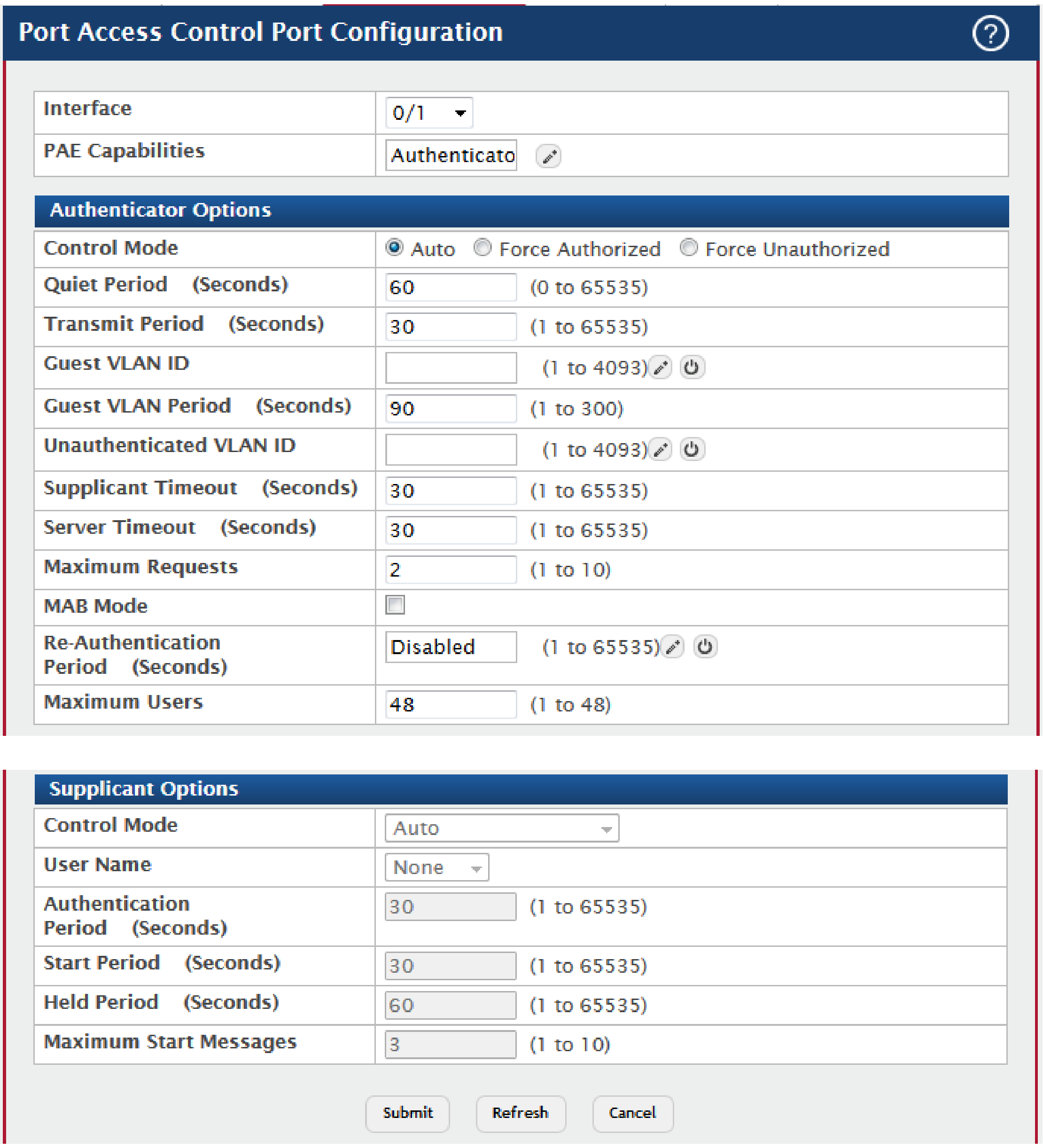
	Interface	PAE Capabilities	Control Mode	Operating Control Mode	PAE State	Backend State	
□	0/11	Authenticator	Auto	N/A	Initialize	Initialize	
□	0/12	Authenticator	Auto	N/A	Initialize	Initialize	
□	0/13	Authenticator	Auto	N/A	Initialize	Initialize	

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.
Operating Control Mode	The control mode under which the port is actually operating, which is one of the following: Auto Force Unauthorized Force Authorized 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 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
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.

6.1.1.3 Port Configuration

Use this page to configure the port-based authentication settings for each port.



Port Access Control Port Configuration

Interface	0/1
PAE Capabilities	Authenticato

Authenticator Options

Control Mode	● Auto ○ Force Authorized ○ Force Unauthorized
Quiet Period (Seconds)	60 (0 to 65535)
Transmit Period (Seconds)	30 (1 to 65535)
Guest VLAN ID	(1 to 4093)
Guest VLAN Period (Seconds)	90 (1 to 300)
Unauthenticated VLAN ID	(1 to 4093)
Supplicant Timeout (Seconds)	30 (1 to 65535)
Server Timeout (Seconds)	30 (1 to 65535)
Maximum Requests	2 (1 to 10)
MAB Mode	□
Re-Authentication Period (Seconds)	Disabled (1 to 65535)
Maximum Users	48 (1 to 48)

Supplicant Options

Control Mode	Auto
User Name	None
Authentication Period (Seconds)	30 (1 to 65535)
Start Period (Seconds)	30 (1 to 65535)
Held Period (Seconds)	60 (1 to 65535)
Maximum Start Messages	3 (1 to 10)

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.

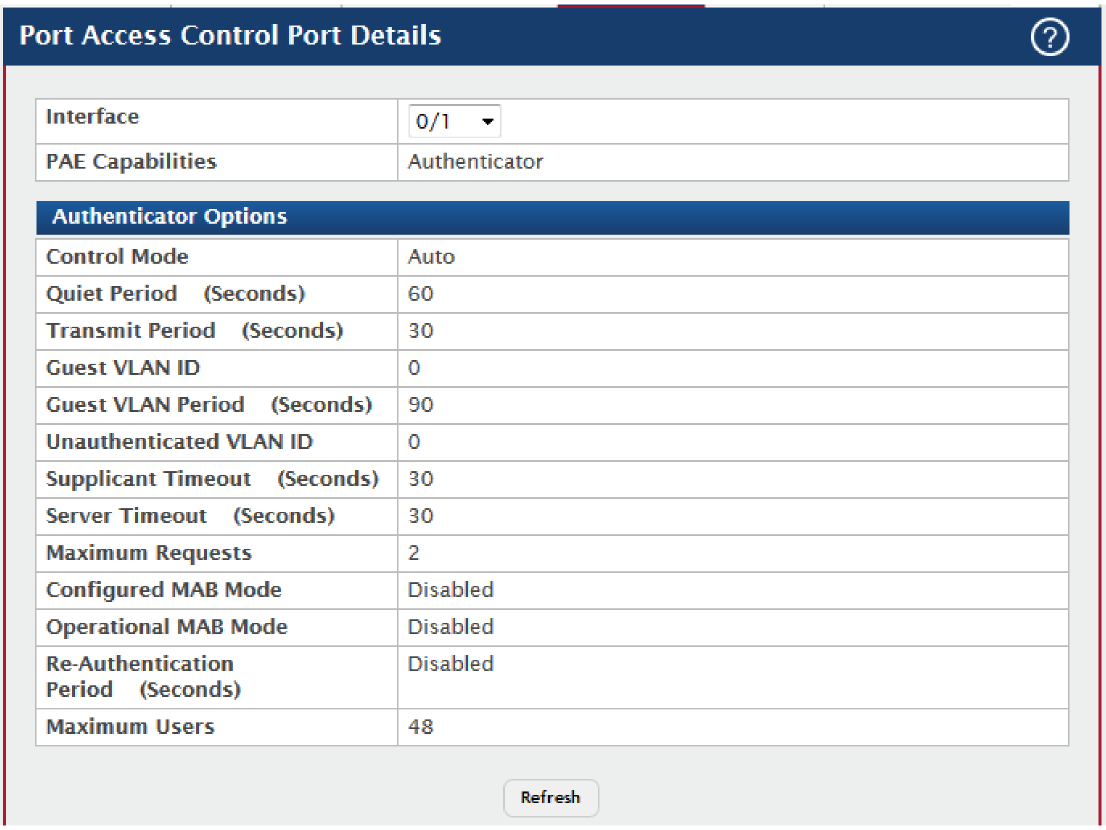
	Supplicant – The port is connected to an authenticator port and must be granted permission by the authentication server before it can send and receive traffic through the remote port. To change the PAE capabilities of a port, click the Edit icon associated with the field and select the desired setting from the menu in the Set PAE Capabilities window.
Authenticator Options	
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. 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.
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. To set the guest VLAN ID, click the Edit icon associated with the field and specify the ID value in the available field. To reset the guest VLAN ID to the default value, click the Reset icon associated with the field and confirm the action.
Guest VLAN Period	The value, in seconds, of the timer used for guest VLAN authentication.
Unauthenticated VLAN ID	The VLAN ID of the unauthenticated VLAN. Hosts that fail the authentication might be denied access to the network or placed on a VLAN created for unauthenticated clients. This VLAN might be configured with limited network access. To set the unauthenticated

	VLAN ID, click the Edit icon associated with the field and specify the ID value in the available field. To reset the unauthenticated VLAN ID to the default value, click the Reset icon associated with the field and confirm the action.
Supplicant Timeout	The amount of time that the port waits for a response before retransmitting an EAP request frame to the client.
Server Timeout	The amount of time the port waits for a response from the authentication server.
Maximum Requests	The maximum number of times that the port sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
MAB Mode	The MAC-based Authentication Bypass (MAB) mode on the port, which can be enabled or disabled.
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 reauthenicate 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.
Maximum Users	The maximum number of clients supported on the port if the Control Mode on the port is MAC-based 802.1X authentication.
Supplicant Options	
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.

6.1.1.4 Port Details

Use this page to view 802.1X information for a specific port.



Port Access Control Port Details

Interface	0/1
PAE Capabilities	Authenticator

Authenticator Options

Control Mode	Auto
Quiet Period (Seconds)	60
Transmit Period (Seconds)	30
Guest VLAN ID	0
Guest VLAN Period (Seconds)	90
Unauthenticated VLAN ID	0
Supplicant Timeout (Seconds)	30
Server Timeout (Seconds)	30
Maximum Requests	2
Configured MAB Mode	Disabled
Operational MAB Mode	Disabled
Re-Authentication Period (Seconds)	Disabled
Maximum Users	48

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

PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: 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	
Control Mode	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.
Unauthenticated VLAN ID	The VLAN ID of the unauthenticated VLAN. Hosts that fail the authentication might be denied access to the network or placed on a VLAN created for unauthenticated clients. This VLAN might be configured with limited network access.
Supplicant Timeout	The amount of time that the port waits for a response before retransmitting an EAP request frame to the client.
Server Timeout	The amount of time the port waits for a response from the authentication server.

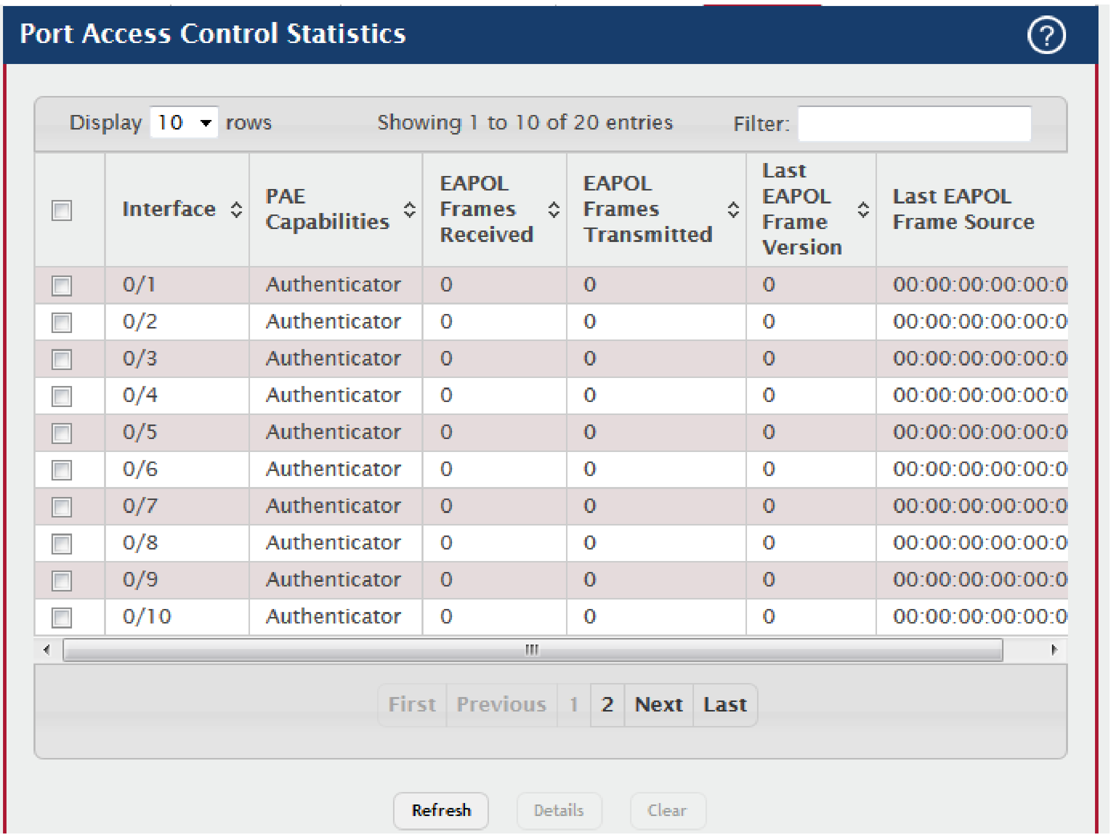
Maximum Requests	The maximum number of times that the port sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
Configured MAB Mode	The configured MAC-based Authentication Bypass (MAB) mode on the port.
Operational MAB Mode	The operational MAC-based Authentication Bypass (MAB) mode on the port.
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 reauthenicate periodically.
Maximum Users	The maximum number of clients supported on the port if the Control Mode on the port is MAC-based 802.1X authentication.
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
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 Unauth Default Not Assigned
Supplicant Options	
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.

6.1.1.5 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.



Port Access Control Statistics

Display 10 rows Showing 1 to 10 of 20 entries Filter:

□	Interface	PAE Capabilities	EAPOL Frames Received	EAPOL Frames Transmitted	Last EAPOL Frame Version	Last EAPOL Frame Source
□	0/1	Authenticator	0	0	0	00:00:00:00:00:0
□	0/2	Authenticator	0	0	0	00:00:00:00:00:0
□	0/3	Authenticator	0	0	0	00:00:00:00:00:0
□	0/4	Authenticator	0	0	0	00:00:00:00:00:0
□	0/5	Authenticator	0	0	0	00:00:00:00:00:0
□	0/6	Authenticator	0	0	0	00:00:00:00:00:0
□	0/7	Authenticator	0	0	0	00:00:00:00:00:0
□	0/8	Authenticator	0	0	0	00:00:00:00:00:0
□	0/9	Authenticator	0	0	0	00:00:00:00:00:0
□	0/10	Authenticator	0	0	0	00:00:00:00:00:0

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.
EAPOL Frames Transmitted	The total number of EAPOL frames sent by the interface.
Last EAPOL Frame Version	The protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address attached to the most recently received EAPOL frame.

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.

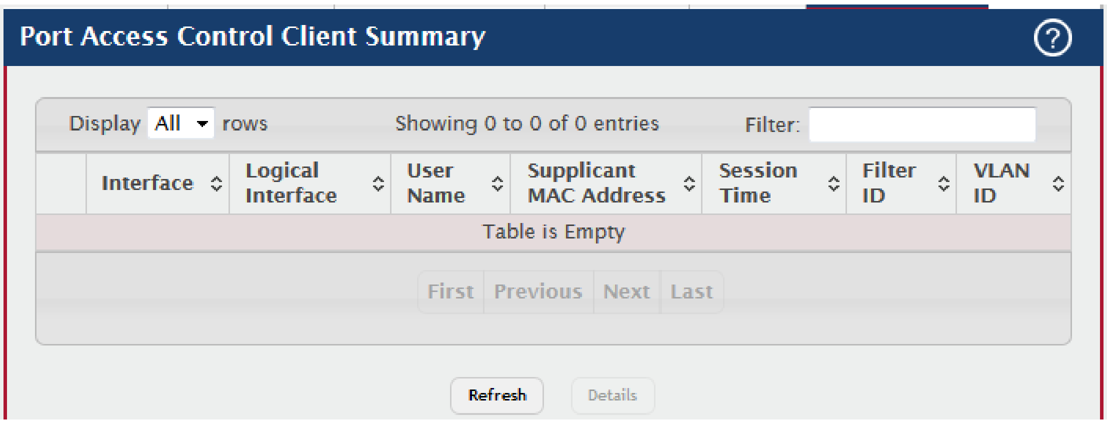
Field	Description
EAPOL Start Frames Received	The total number of EAPOL-Start frames received on the interface. EAPOL-Start frames are sent by a supplicant to initiate the 802.1X authentication process when it connects to the interface. This field is displayed only if the interface is configured as an authenticator.
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.
EAP Request Frames Transmitted	The total number of EAP-Request frames the interface has sent. EAP-Request frames are sent from an authentication server to a supplicant (and translated by the authenticator) during the authentication process. 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 Response Frames Transmitted	The total number of EAP-Response frames the interface has sent. 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 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	The number of EAPOL frames with an invalid packet body length

Error Frames Received	received on the interface.
Clear (Button)	Resets all statistics counters to 0 for the selected interface or interfaces.

6.1.1.6 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.



Port Access Control Client Summary

Display All rows Showing 0 to 0 of 0 entries Filter:

	Interface	Logical Interface	User Name	Supplicant MAC Address	Session Time	Filter ID	VLAN ID
Table is Empty							

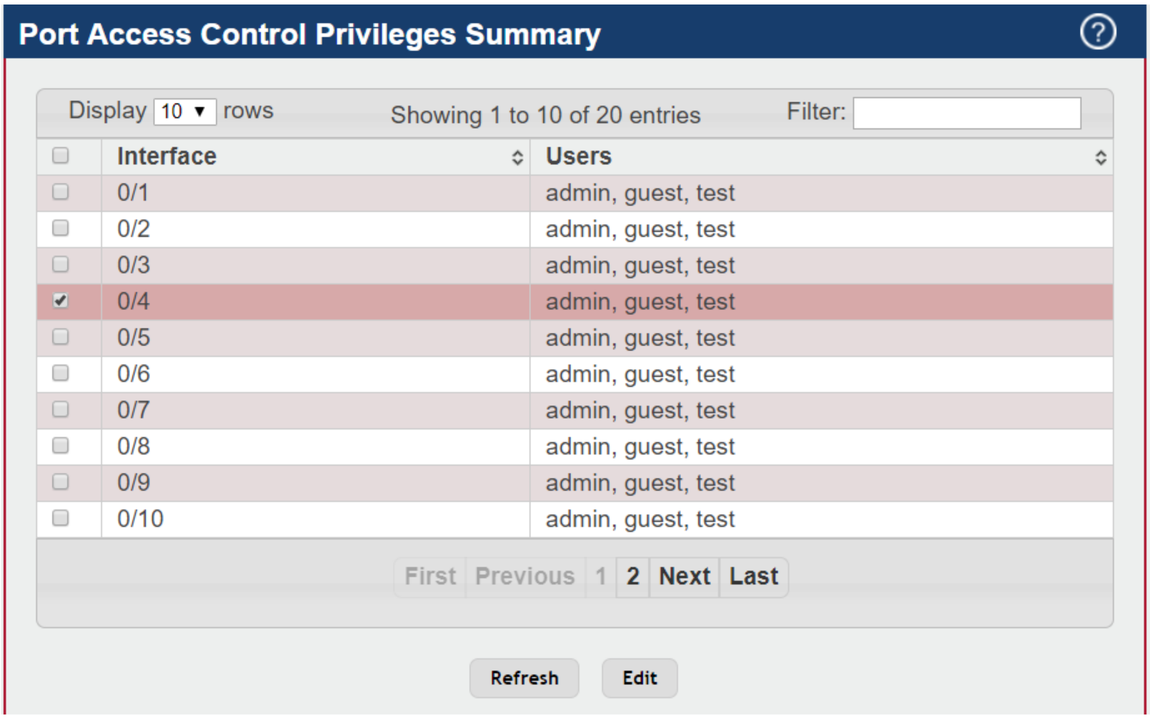
Field	Description
Interface	The local interface associated with the rest of the data in the row. When viewing detailed information for an interface, this field identifies the interface being viewed.
Logical Interface	The logical port number associated with the supplicant that is connected to the port.
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.

Field	Description
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.

6.1.1.7 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.



Port Access Control Privileges Summary

Display 10 rows Showing 1 to 10 of 20 entries Filter:

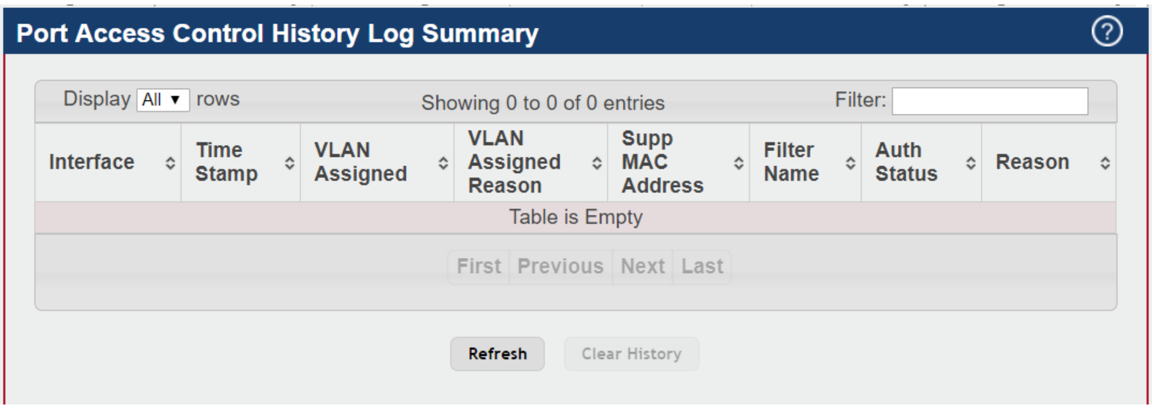
□	Interface	Users
□	0/1	admin, guest, test
□	0/2	admin, guest, test
□	0/3	admin, guest, test
☑	0/4	admin, guest, test
□	0/5	admin, guest, test
□	0/6	admin, guest, test
□	0/7	admin, guest, test
□	0/8	admin, guest, test
□	0/9	admin, guest, test
□	0/10	admin, guest, test

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.

6.1.1.8 History Log Summary

This page displays information about the 802.1X entries in the history log table.



Port Access Control History Log Summary

Display All ▾ rows　　Showing 0 to 0 of 0 entries　　Filter:

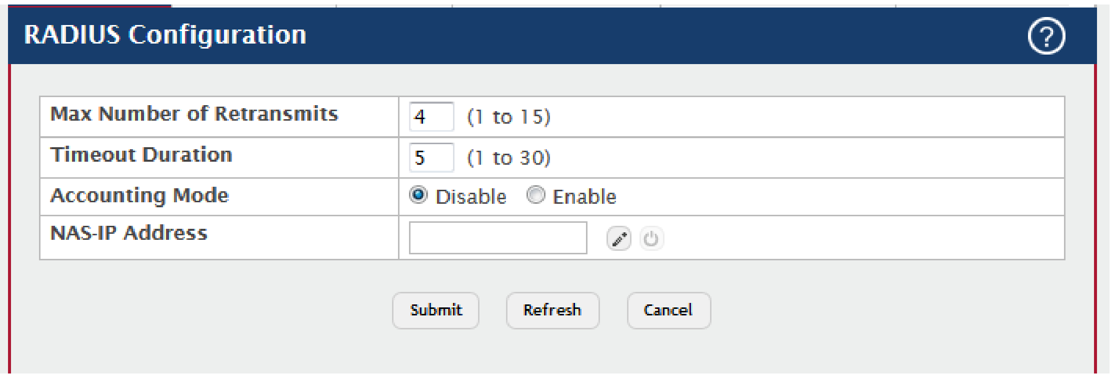
Interface	Time Stamp	VLAN Assigned	VLAN Assigned Reason	Supp MAC Address	Filter Name	Auth Status	Reason
Table is Empty							

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 Unauth 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.

6.1.2 RADIUS

6.1.2.1 Configuration

Use this page to configure global settings for the Remote Authentication Dial-In User Service (RADIUS) feature. The device includes a RADIUS client that can contact one or more RADIUS servers for various Authentication, Authorization, and Accounting (AAA) services. The RADIUS server maintains a centralized database that contains per-user information.



RADIUS Configuration

Max Number of Retransmits	4 (1 to 15)
Timeout Duration	5 (1 to 30)
Accounting Mode	● Disable ○ Enable
NAS-IP Address	

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.
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

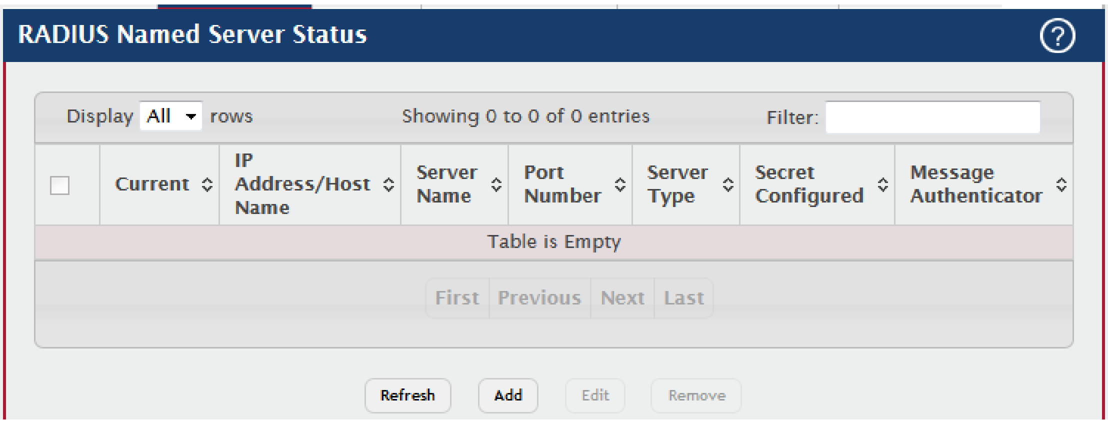
	used only in Access-Request packets. To reset the NAS IP address to the default value, click the Reset icon and confirm the action.

6.1.2.2 Named Server

Use this page to view and configure information about the RADIUS server(s) the RADIUS client on the device uses for authentication services.

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.



RADIUS Named Server Status

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Current	IP Address/Host Name	Server Name	Port Number	Server Type	Secret Configured	Message Authenticator
Table is Empty							

Field	Description
Current	Indicates whether the RADIUS server is the current server (True) or a backup server (False) within its group. If more than one RADIUS server is configured with the same Server Name, the device selects one of the servers to be the current server in the named server group. When the device 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. If no server is configured as the primary server, the current server is the RADIUS server that is added to the group first.

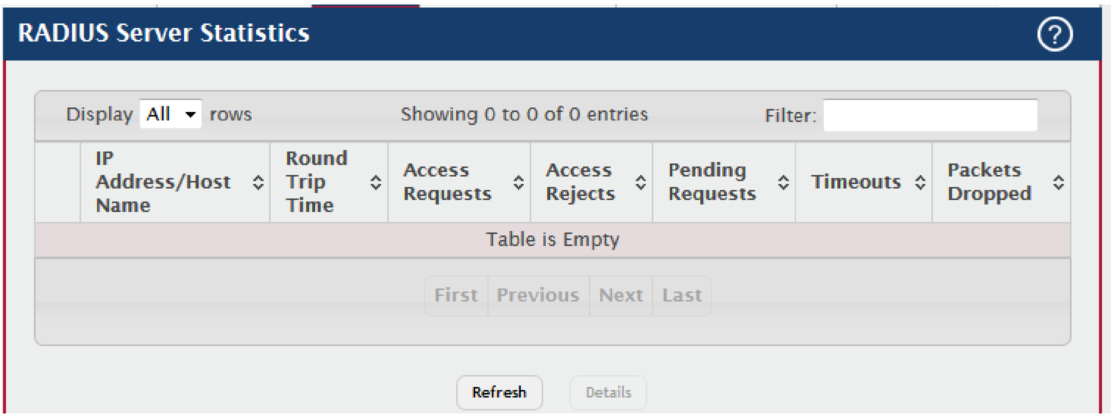
IP Address/Host Name	The IP address or host name of the RADIUS server. Host names must be resolvable by DNS and are composed of a series of labels separated by dots.
Server Name	The name of the RADIUS server. RADIUS authentication servers that are configured with the same name are members of the same named RADIUS server group. RADIUS servers in the same group serve as backups for each other.
Port Number	The UDP port on the RAIDUS authentication server to which the local RADIUS client sends request packets.
Server Type	Indicates whether the server is the Primary or a Secondary RADIUS authentication server. When multiple RADIUS servers have the same Server Name value, the RADIUS client attempts to use the primary server first. If the primary server does not respond, the RADIUS client attempts to use one of the backup servers within the same named server group.
Secret Configured	Indicates whether the shared secret for this server has been configured.
Message Authenticator	Indicates whether the RADIUS server requires the Message Authenticator attribute to be present. The Message Authenticator adds protection to RADIUS messages by using an MD5 hash to encrypt each message. The shared secret is used as the key, and if the message fails to be verified by the RADIUS server, it is discarded.

After you click Add or Edit, a window opens and allows you to add or update information about a RADIUS server. The following information describes the additional field available in the Add RADIUS Server and Edit RADIUS Server windows.

Field	Description
Secret	The shared secret text string used for authenticating and encrypting all RADIUS communications between the RADIUS client on the device and the RADIUS server. The secret specified in this field must match the shared secret configured on the RADIUS server.

6.1.2.3 Statistics

Use this page to view summary information about the number and type of RADIUS messages sent between the RADIUS client on the device and the configured RADIUS authentication servers. To view additional statistics, select the RADIUS server with the statistics to view and click Details.



RADIUS Server Statistics

Display All rows Showing 0 to 0 of 0 entries Filter:

	IP Address/Host Name	Round Trip Time	Access Requests	Access Rejects	Pending Requests	Timeouts	Packets Dropped
Table is Empty							

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.

After you click Details, a window opens and displays additional statistics about the number and type of messages sent between the selected RADIUS server and the RADIUS client on the device. The following information describes the additional fields that appear in the RADIUS

Server Detailed Statistics window.

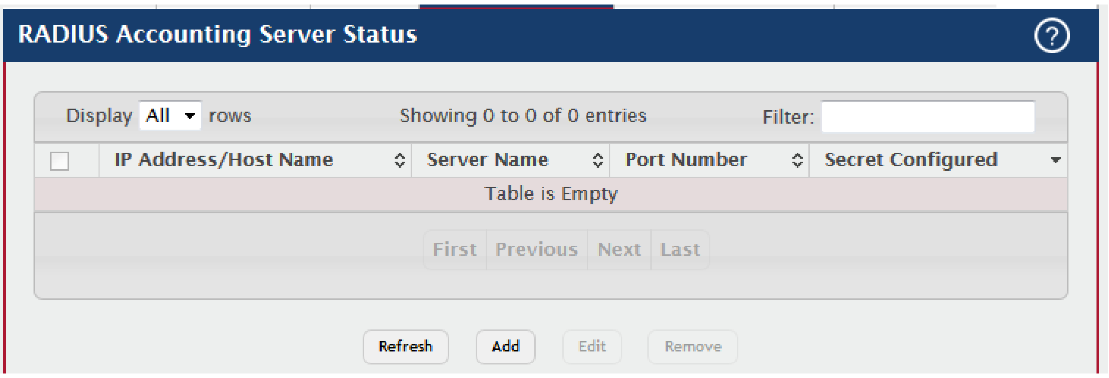
Field	Description
Access Retransmissions	The number of RADIUS Access-Request packets that had to be retransmitted to the server because the initial Access-Request packet failed to be successfully delivered.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, 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.

6.1.2.4 Accounting Server

Use this page to view and configure information about the RADIUS server(s) the RADIUS client on the device uses for accounting services. RADIUS accounting must be globally enabled for the RADIUS client on the device to contact any configured RADIUS accounting servers.

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.



RADIUS Accounting Server Status

Display All rows   Showing 0 to 0 of 0 entries   Filter:

☐	IP Address/Host Name	Server Name	Port Number	Secret Configured
Table is Empty				

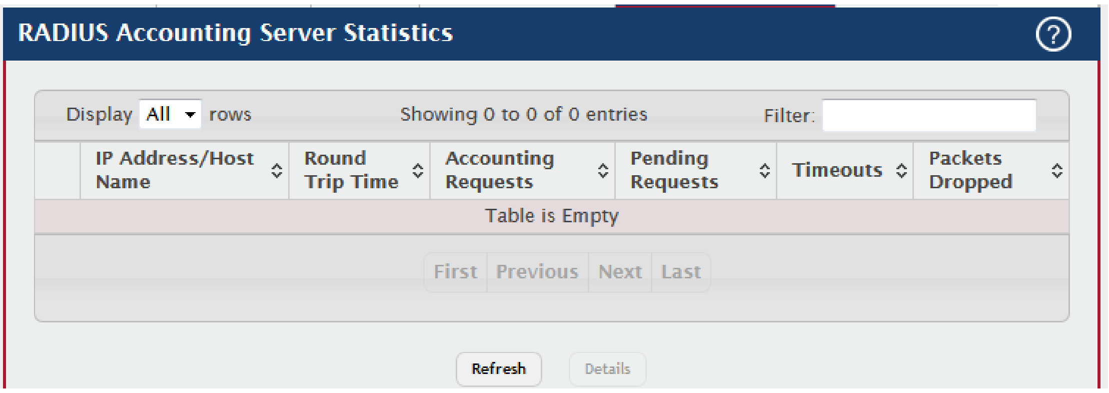
Field	Description
IP Address/Host Name	The IP address or host name of the RADIUS accounting server. Host names must be resolvable by DNS and are composed of a series of labels separated by dots.
Server Name	The name of the RADIUS accounting server. The server name must be unique among all configured RADIUS accounting servers.
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.

After you click Add or Edit, a window opens and allows you to add or update information about a RADIUS accounting server. The following information describes the additional field available in the Add RADIUS Accounting Server and Edit RADIUS Accounting Server windows.

Field	Description
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.

6.1.2.5 Accounting Statistics

Use this page to view summary information about the number and type of RADIUS messages sent between the RADIUS client on the device and the configured RADIUS accounting servers. To view additional statistics, select the RADIUS accounting server with the statistics to view and click Details.



RADIUS Accounting Server Statistics

Display All rows Showing 0 to 0 of 0 entries Filter:

	IP Address/Host Name	Round Trip Time	Accounting Requests	Pending Requests	Timeouts	Packets Dropped
Table is Empty						

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	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.
Accounting Requests	The number of RADIUS Accounting-Request packets sent to the 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.

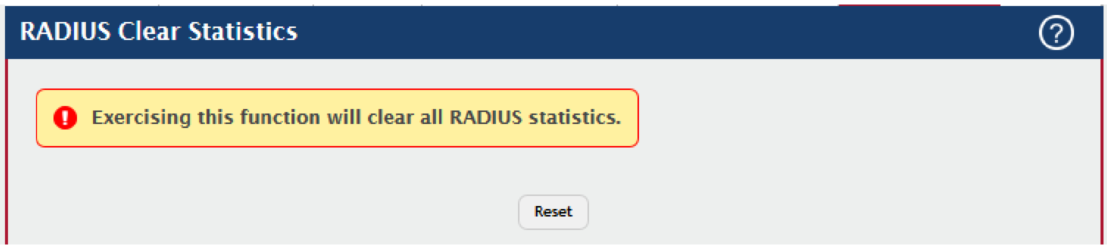
After you click Details, a window opens and displays additional statistics about the number and type of messages sent between the selected RADIUS server and the RADIUS client on the device. The following information describes the additional fields that appear in the RADIUS Accounting Server Detailed Statistics window.

Field	Description
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.
Malformed Access	The number of malformed RADIUS Accounting-Response packets received from the server. Malformed packets include packets with an

Responses	invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets that contained invalid authenticators received from the accounting server.
Unknown Types	The number of RADIUS packets of unknown type which were received from the server on the accounting port.

6.1.2.6 Clear Statistics

Click this button to clear all RADIUS authentication and RAIDUS accounting server statistics. After you confirm the action, the statistics on both the RADIUS Server Statistics and RADIUS Accounting Server Statistics pages are reset.

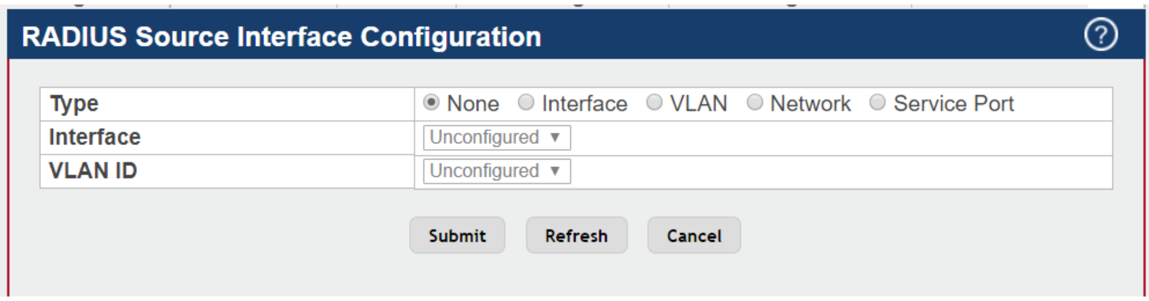


RADIUS Clear Statistics

Exercising this function will clear all RADIUS statistics.

6.1.2.7 Source Interface Configuration

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



RADIUS Source Interface Configuration

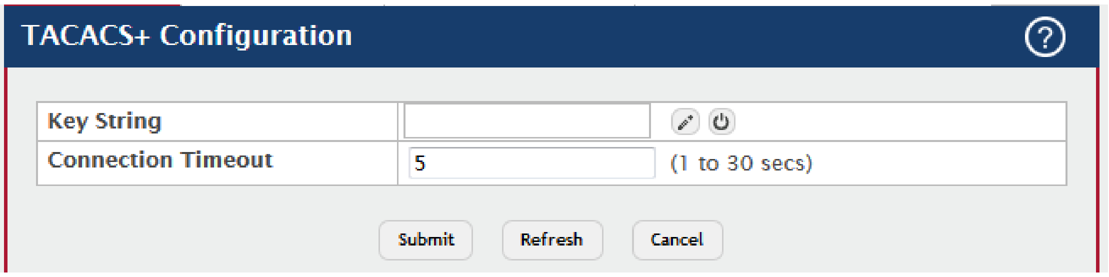
Type	● None ○ Interface ○ VLAN ○ Network ○ Service Port
Interface	Unconfigured ▾
VLAN ID	Unconfigured ▾

Field	Description
Type	The type of interface to use as the source interface: None – The primary IP address of the originating (outbound) interface is used as the source address. Interface – The primary IP address of a physical port is used as the source address.

	VLAN – The primary IP address of a VLAN routing interface is used as the source address. Network – The network source IP is used as the source address. Service Port – The management port source IP is used as the source address.
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.

6.1.3 TACACS+

6.1.3.1 Configuration


TACACS+ Configuration

Key String	
Connection Timeout	5 (1 to 30 secs)

Field	Description
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The key must match the key configured on the TACACS+ server.
Connection Timeout	The maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server.

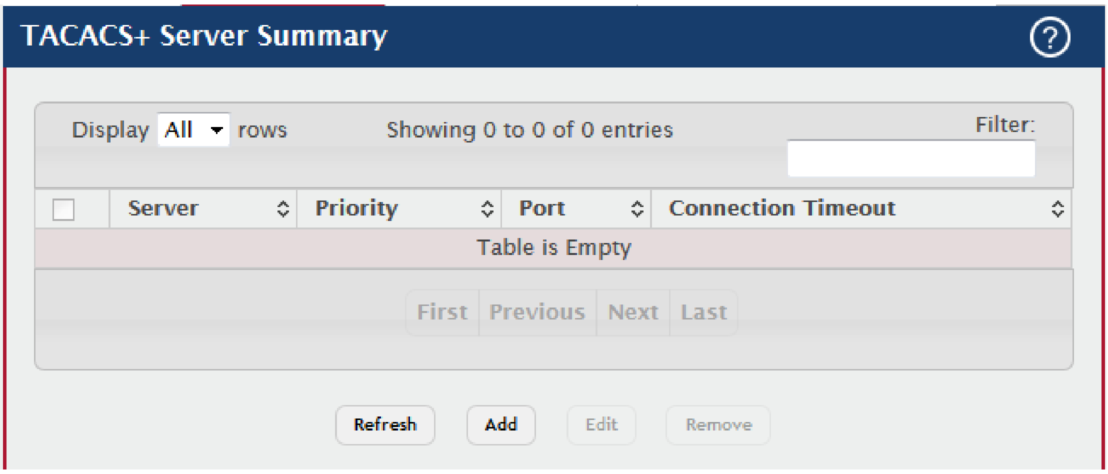
6.1.3.2 Server Summary

Use this page to view and configure information about the TACACS+ Server(s).

Use the buttons to perform the following tasks:

- To add a TACACS+ Server to the list of servers the TACACS+ client can contact, click **Add**. If maximum number of server is added, the button will be disabled
- To edit a configured TACACS+ server from the list, select the entry and click **Edit**.

- To remove a configured TACACS+ server from the list, select the entry to delete and click **Remove**. You must confirm the action before the entry is deleted.



TACACS+ Server Summary

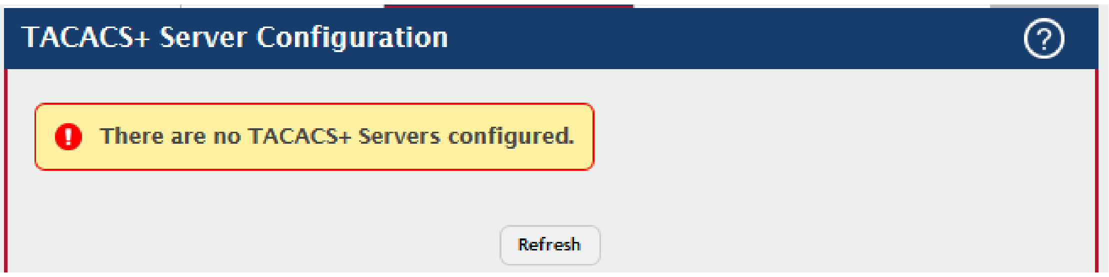
Display All rows Showing 0 to 0 of 0 entries Filter:

□	Server	Priority	Port	Connection Timeout
Table is Empty				

Field	Description
Server	Specifies the TACACS+ Server IP address or Hostname.
Priority	Specifies the order in which the TACACS+ servers are used.
Port	Specifies the authentication port.
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The key must match the encryption used on the TACACS+ server.
Connection Timeout	The amount of time that passes before the connection between the device and the TACACS+ server time out.

6.1.3.3 Server Configuration

Use this page to view and configure information about the TACACS+ Server(s).



TACACS+ Server Configuration

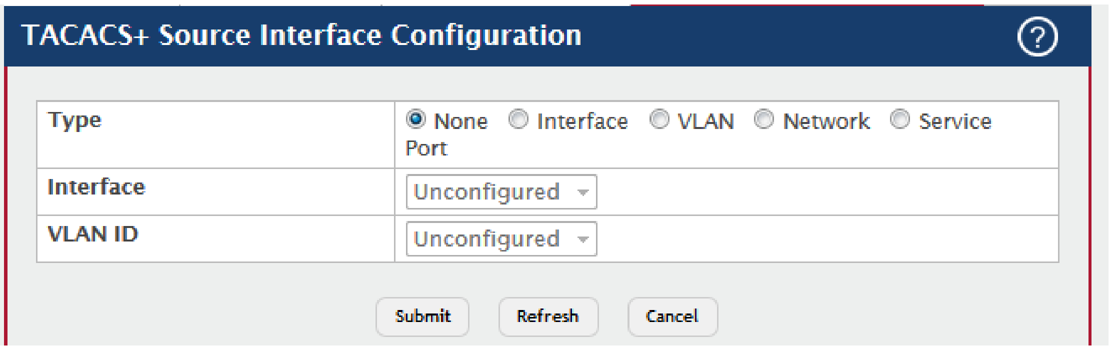
There are no TACACS+ Servers configured.

Field	Description
Server	Specifies the TACACS+ Server IP address or Hostname.
Priority	Specifies the order in which the TACACS+ servers are used.
Port	Specifies the authentication port.

Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The key must match the encryption used on the TACACS+ server.
Connection Timeout	The amount of time that passes before the connection between the device and the TACACS+ server time out.

6.1.3.4 Source Interface Configuration

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



TACACS+ Source Interface Configuration

Type	● None ○ Interface ○ VLAN ○ Network ○ Service Port
Interface	Unconfigured
VLAN ID	Unconfigured

Field	Description
Type	The type of interface to use as the source interface: None – The primary IP address of the originating (outbound) interface is used as the source address. Interface – The primary IP address of a physical port is used as the source address. VLAN – The primary IP address of a VLAN routing interface is used as the source address. Network – The network source IP is used as the source address. Service Port – The management port source IP is used as the source address.
Interface	When the selected Type is Interface, select the physical port to use as the source interface.
VLAN ID	When the selected Type is VLAN, select the VLAN to use as the source interface. The menu contains only the VLAN IDs for VLAN routing interfaces.

7.1 QoS

7.1.1 Access Control Lists

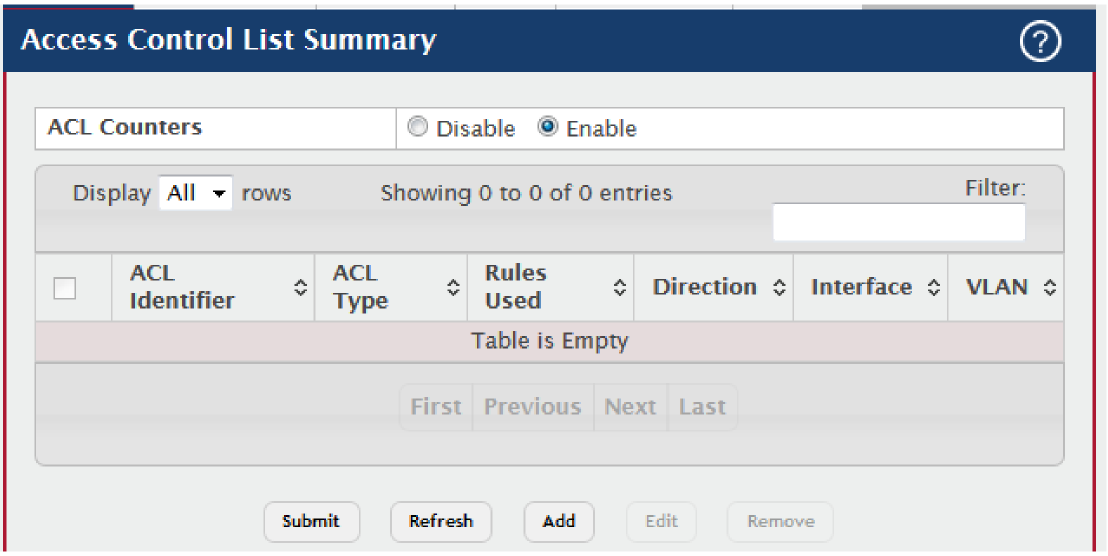
7.1.1.1 Summary

Use this page to add and remove Access Control Lists (ACLs). 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. There are three main steps to configuring an ACL:

1. Create an ACL. (Use the current page.)
2. Add rules to the ACL and configure the rule criteria. (Use the **Access Control List Configuration** page.)
3. Apply the ACL to one or more interfaces. (Use the **Access Control List Interface Summary**page.)

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

- To configure ACL counters, select enable or disable for ACL counters and click **Submit**.
- 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.



Access Control List Summary

ACL Counters ○ Disable ● Enable

Display All rows Showing 0 to 0 of 0 entries Filter:

□	ACL Identifier	ACL Type	Rules Used	Direction	Interface	VLAN
Table is Empty						

Field	Description
ACL Counters	The ACL Counters enabled or disabled status.
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. The ID of a Named IPv4 ACL must begin with a letter, and not a number.
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

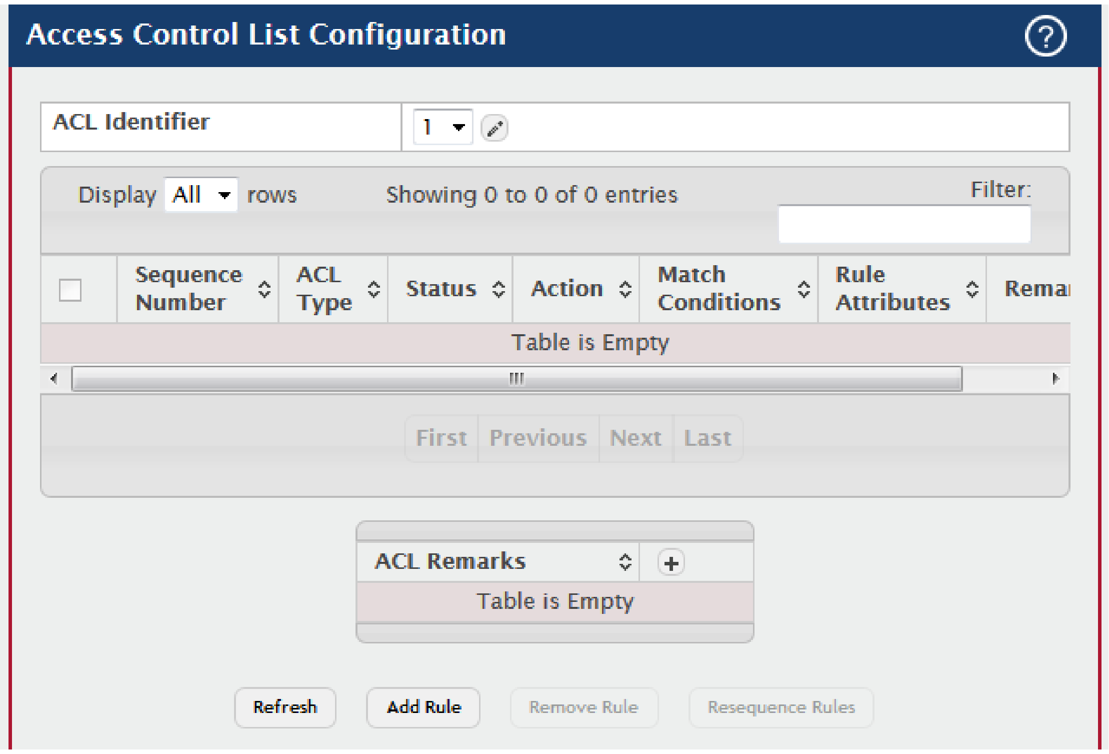
	EtherType value within Ethernet frames.
Rules Used	The number of rules currently configured for the ACL.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on an interface (Inbound) or after it has been received, routed, and is ready to exit an interface (Outbound).
Interface	Each interface to which the ACL has been applied.
VLAN	Each VLAN to which the ACL has been applied.

7.1.1.2 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.

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 one or more configured rules for an ACL, select the ID of the appropriate ACL from the ACL Identifier menu and click **Remove 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**.



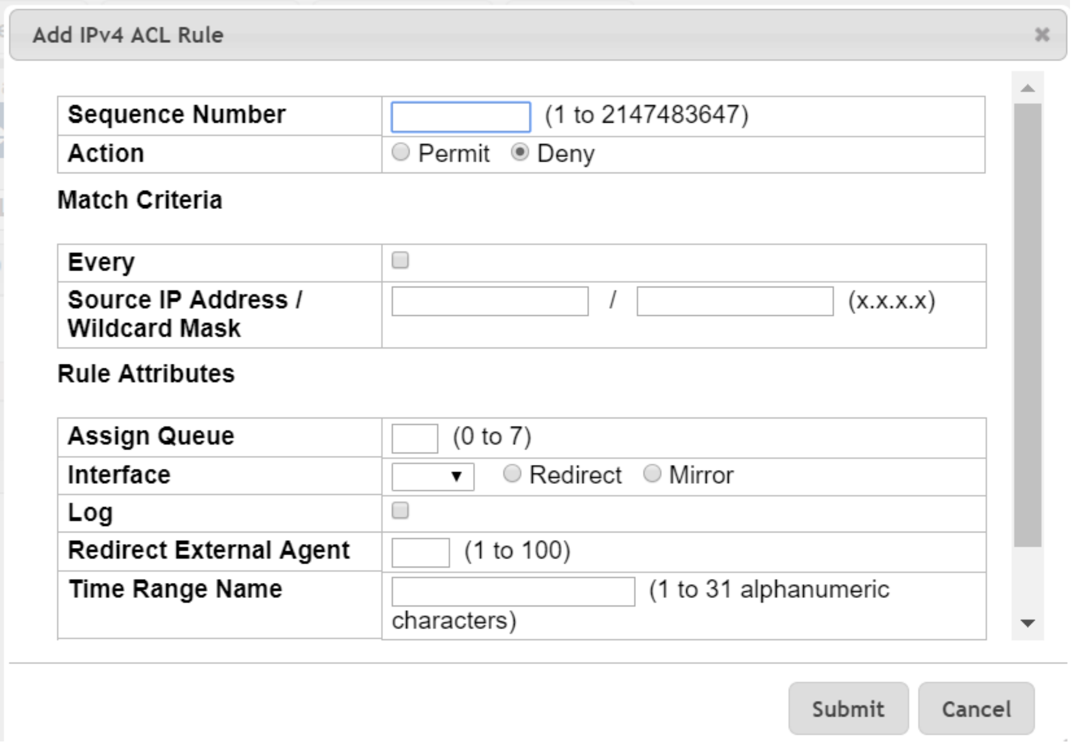
Access Control List Configuration

ACL Identifier	1

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Sequence Number	ACL Type	Status	Action	Match Conditions	Rule Attributes	Remai
Table is Empty							

ACL Remarks
Table is Empty



Add IPv4 ACL Rule

Sequence Number	(1 to 2147483647)
Action	○ Permit ● Deny

Match Criteria

Every	□
Source IP Address / Wildcard Mask	/ (x.x.x.x)

Rule Attributes

Assign Queue	(0 to 7)
Interface	○ Redirect ○ Mirror
Log	□
Redirect External Agent	(1 to 100)
Time Range Name	(1 to 31 alphanumeric characters)

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 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.
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
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.

After you click the + (plus) button, the Add ACL Remark window opens and allows you to add a remark.

After you click the Add Rule button, 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.

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, IPIP, 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. For example, enter a wildcard mask of 0.0.0.0 to specify a host. 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. 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 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. For example, enter a wildcard mask of 0.0.0.0 to specify a host. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A 1 in a bit position of the ACL mask indicates the corresponding bit can be ignored. This field is required when you configure a destination IP address.
Destination L4 Port	(IPv4 Extended and IPv4 Named ACLs) The TCP/UDP destination port to match in the packet header. 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.
TTL Field Value	(IPv4 Extended and IPv4 Named ACLs) IP ACL rule to match on the specified 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.
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. Specifying TOS Mask is optional.
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: ICMPv6, IPv6, TCP, or UDP.
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. To indicate a destination host, specify an IPv6 prefix length of 128.
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.
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.
TTL Field Value	(IPv6 Named ACLs) IP ACL rule to match on the specified TTL field value.
ICMP Type	IPv6 ACL rule to match on the specified ICMP message type. This option is available only if the protocol is ICMPv6.
ICMP Code	IPv6 ACL rule to match on the specified ICMP message code. This option is available only if the protocol is ICMPv6.
ICMP Message	IPv6 ACL rule to match on the ICMP message type and code. Specify one of the following supported ICMPv6 messages: Destination-Unreachable, Echo-Request, Echo-Reply, Header, Hop-Limit, MLD-Query, MLD-Reduction, MLD-Report, ND-NA, ND-NS, Next-Header, No-Admin, No-Route, Packet-Too-Big, Port-Unreachable, Router-Solicitation, Router-Advertisement, Router-Renumbering, Time-Exceeded, and Unreachable. This option is available only if the protocol is ICMPv6.

TCP Flags	IPv6 ACL rule to match on the TCP flags. When a + flag is specified, a match occurs if the flag is set in the TCP header. When a - flag is specified, a match occurs if the flag is not set in the TCP header. When Established is specified, a match occurs if either RST or ACK bits are set in the TCP header. This option is available only if the protocol is TCP.
Flow Label	A 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers.
IP DSCP	The IP DSCP value in the IPv6 packet to match to the rule. The DSCP value is defined as the high-order six bits of the Service Type octet in the IPv6 header.
Routing	IPv6 ACL rule to match on routed packets.
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).
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.
Redirect External Agent	The number that identifies the external agent that will receive all packets matching this rule.
Time Range Name	The name of the time range that will impose a time limitation on the ACL rule. If a time range with the specified name does not exist, and the ACL containing this ACL rule is associated with an interface, the

	ACL rule is applied immediately. If a time range with specified name exists, and the ACL containing this ACL rule is associated with an interface, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
Committed Rate / Burst Size	The allowed transmission rate for packets 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.

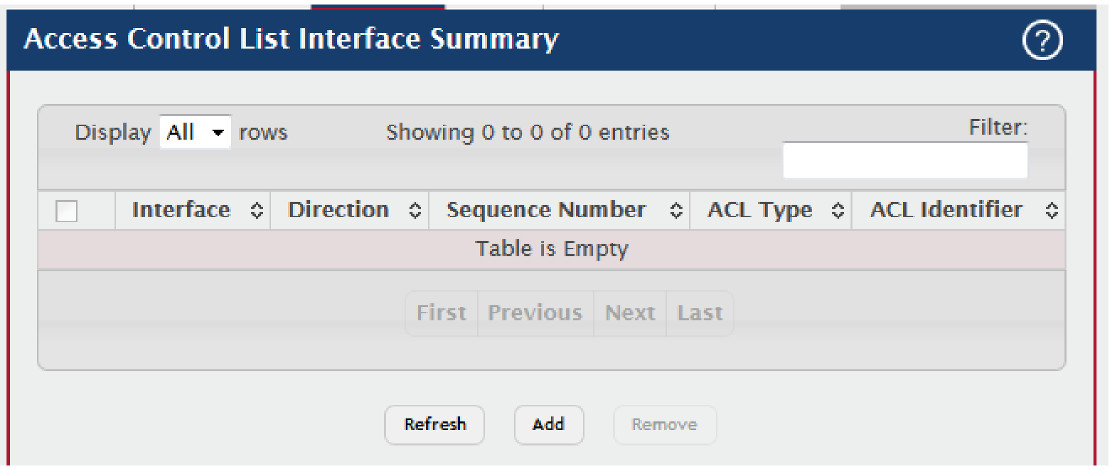
Field	Description
Sequence Start	The starting sequence number for resequencing the existing rules.
Sequence Step	The increment of sequence numbers for resequencing the existing rules.

7.1.1.3 Interface

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.

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.



Access Control List Interface Summary

Display All rows Showing 0 to 0 of 0 entries Filter:

☐	Interface	Direction	Sequence Number	ACL Type	ACL Identifier
Table is Empty					

Field	Description
Interface	The interface that has an associated ACL.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on an interface (Inbound) or after it has been received, routed, and is ready to exit an interface (Outbound).
Sequence Number	The order the ACL is applied to traffic on the interface relative to other ACLs associated with the interface in the same direction. When multiple ACLs are applied to the same interface in the same direction, the ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.
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

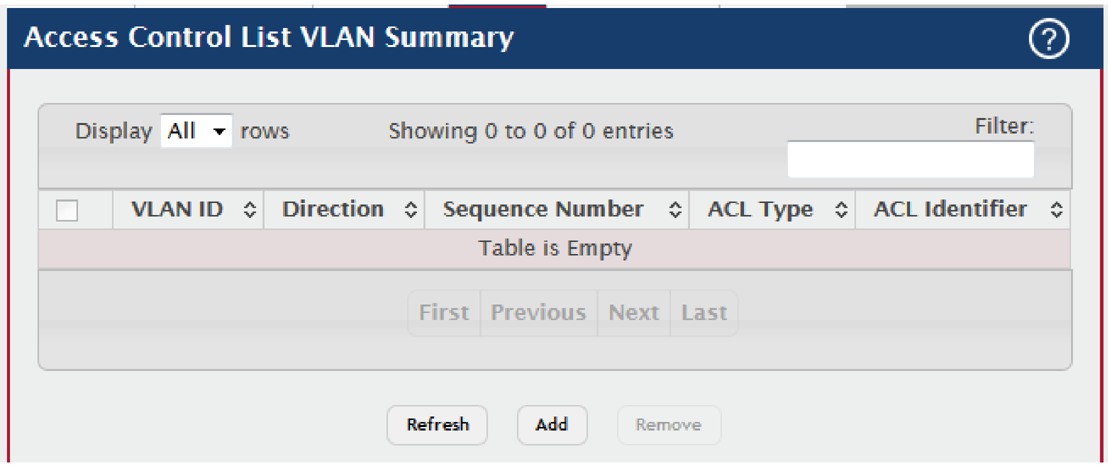
	destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.
ACL Identifier	The name or number that identifies the ACL. When applying an ACL to an interface, the ACL Identifier menu includes only the ACLs within the selected ACL Type.

7.1.1.4 VLANS

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

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.



Access Control List VLAN Summary

Display All rows Showing 0 to 0 of 0 entries Filter:

□	VLAN ID	Direction	Sequence Number	ACL Type	ACL Identifier
Table is Empty					

Field	Description
VLAN ID	The ID of the VLAN associated with the rest of the data in the row. When associating a VLAN with an ACL, use this field to select the desired VLAN.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on a VLAN (Inbound) or after it has been received, routed, and is ready to exit a VLAN (Outbound).
Sequence Number	The order the ACL is applied to traffic on the VLAN relative to other ACLs associated with the VLAN in the same direction. When multiple ACLs are applied to the same VLAN in the same direction, the ACL with the lowest sequence number is applied first, and the other ACLs

	are applied in ascending numerical order.
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows: 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. ACL Identifier
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.

7.1.1.5 Control Plane

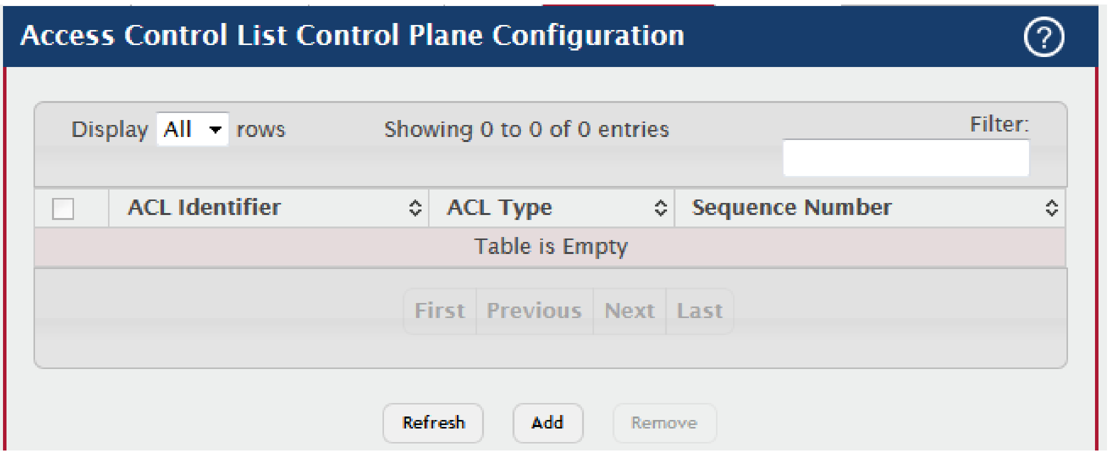
Use this page to define controlled management access to the device. Control plane ACLs allow you to determine which addresses or protocols are allowed to access the management interface on the device. The control plane ACLs are applied to management access through the in-band (production network) ports 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.

Note: Control-plane ACLs are applied only on the designated CPU management port. In stacking environment, some of the packets gets copied to local CPU on the remote unit, and then gets tunneled to designated management CPU interface. So it possible that remote CPU gets slammed with undesired traffic since control-plane ACLs are not present on the remote

CPU. Also, on platforms with multiple silicones attached to CPU via PCI/SPI interface, control plane ACLs are applied only on the silicon that has designated CPU port.

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.



Access Control List Control Plane Configuration

Display All rows Showing 0 to 0 of 0 entries Filter:

□	ACL Identifier	ACL Type	Sequence Number
Table is Empty			

Field	Description
ACL Identifier	The name or number that identifies the ACL.
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows: 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

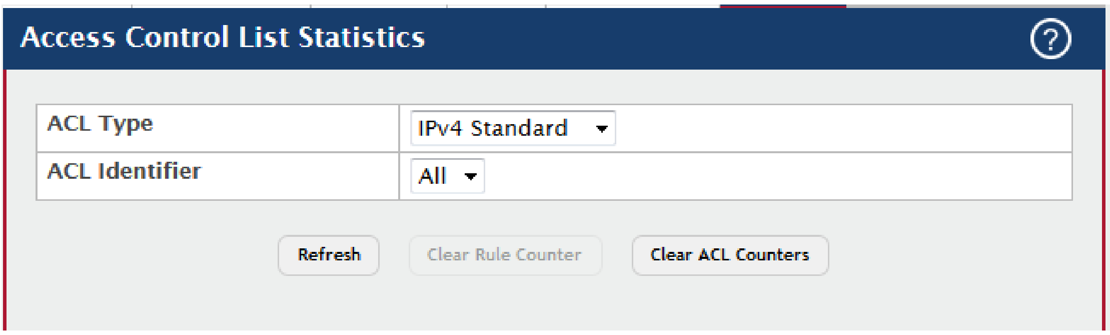
	Layer 4 ports, and protocol type within IPv6 packets. Extended MAC – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.
Sequence Number	The order the ACL is applied to traffic on the interface relative to 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.

7.1.1.6 Statistics

This page displays the statistical information about the packets forwarded or discarded by the port that match 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.

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.



Access Control List Statistics

ACL Type	IPv4 Standard
ACL Identifier	All

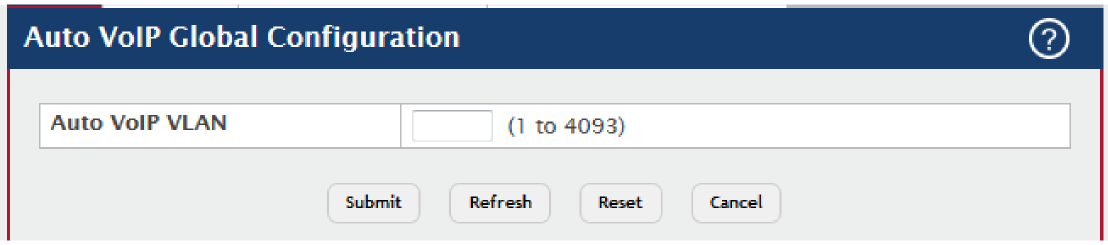
Field	Description
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and 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.

7.1.2 Auto VoIP

7.1.2.1 System

Use this page to configure the VLAN ID for the Auto VoIP VLAN or to reset the current Auto VoIP VLAN ID to the default value. Voice over Internet Protocol (VoIP) enables telephone calls over a data network. Because voice traffic is typically more time-sensitive than data traffic, the Auto VoIP feature helps provide a classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better Quality of Service (QoS). With the Auto VoIP feature, voice prioritization is provided based on call-control protocols (SIP, SCCP, H.323) and/or OUI bits. When the device identifies voice traffic, it is placed in the VLAN specified on this page. The Auto VoIP feature does not rely on LLDP-MED support in connected devices.



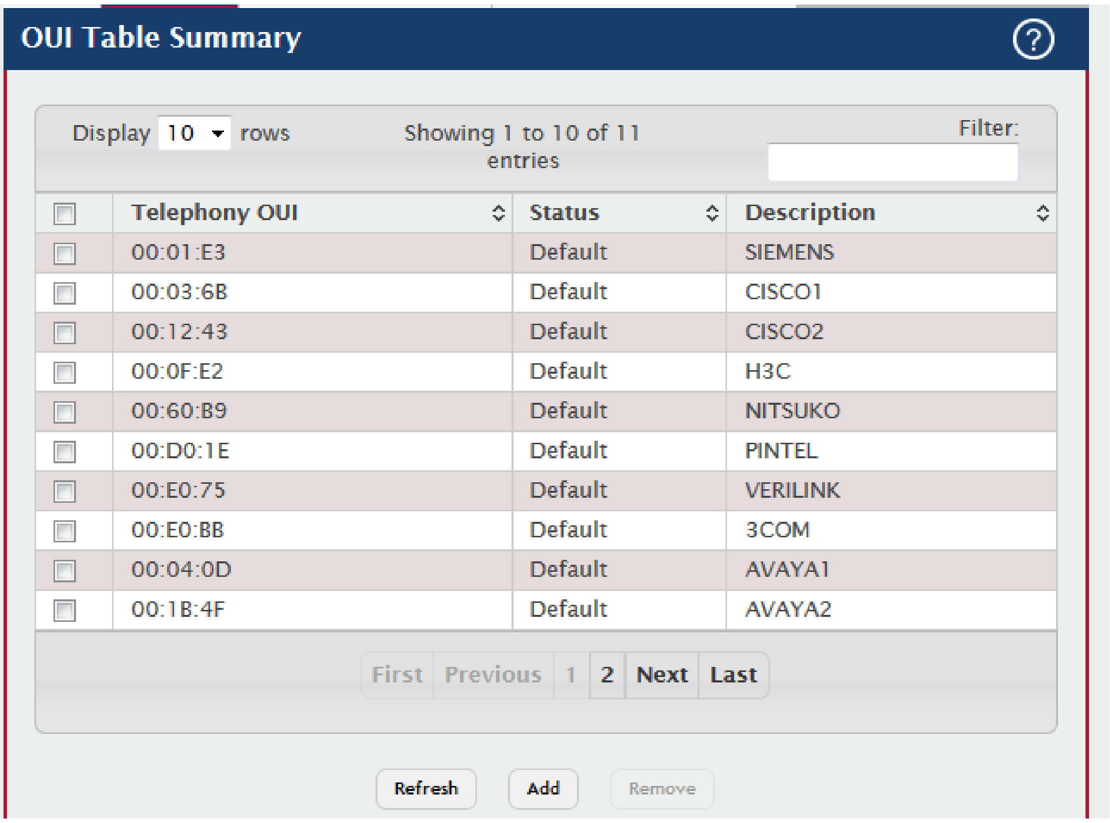
Field	Description
Auto VoIP VLAN	The VLAN used to segregate VoIP traffic from other non-voice traffic.
Reset (Button)	Click this button to reset the voice VLAN to the default value.

7.1.2.2 OUI Table

Use this page to add and remove Organizationally Unique Identifiers (OUIs) from the OUI database the device maintains. Device hardware manufacturers can include an OUI in a network adapter to help identify the device. The OUI is a unique 24-bit number assigned by the IEEE registration authority. Several default OUIs have been preconfigured in the OUI database on the device.

Use the buttons to perform the following tasks:

- To add an OUI, click **Add** and specify an OUI and its description in the available fields.
- To remove one or more configured OUIs, select each entry to delete and click **Remove.** You must confirm the action before the entry is deleted.



OUI Table Summary

Display 10 rows   Showing 1 to 10 of 11 entries   Filter:

□	Telephony OUI	Status	Description
□	00:01:E3	Default	SIEMENS
□	00:03:6B	Default	CISCO1
□	00:12:43	Default	CISCO2
□	00:0F:E2	Default	H3C
□	00:60:B9	Default	NITSUKO
□	00:D0:1E	Default	PINTEL
□	00:E0:75	Default	VERILINK
□	00:E0:BB	Default	3COM
□	00:04:0D	Default	AVAYA1
□	00:1B:4F	Default	AVAYA2

Field	Description
Telephony OUI	The unique OUI that identifies the device manufacturer or vendor. The OUI is specified in three octet values (each octet is represented as two hexadecimal digits) separated by colons.
Status	Identifies whether the OUI is preconfigured on the system (Default) or added by a user (Configured).
Description	Identifies the manufacturer or vendor associated with the OUI.

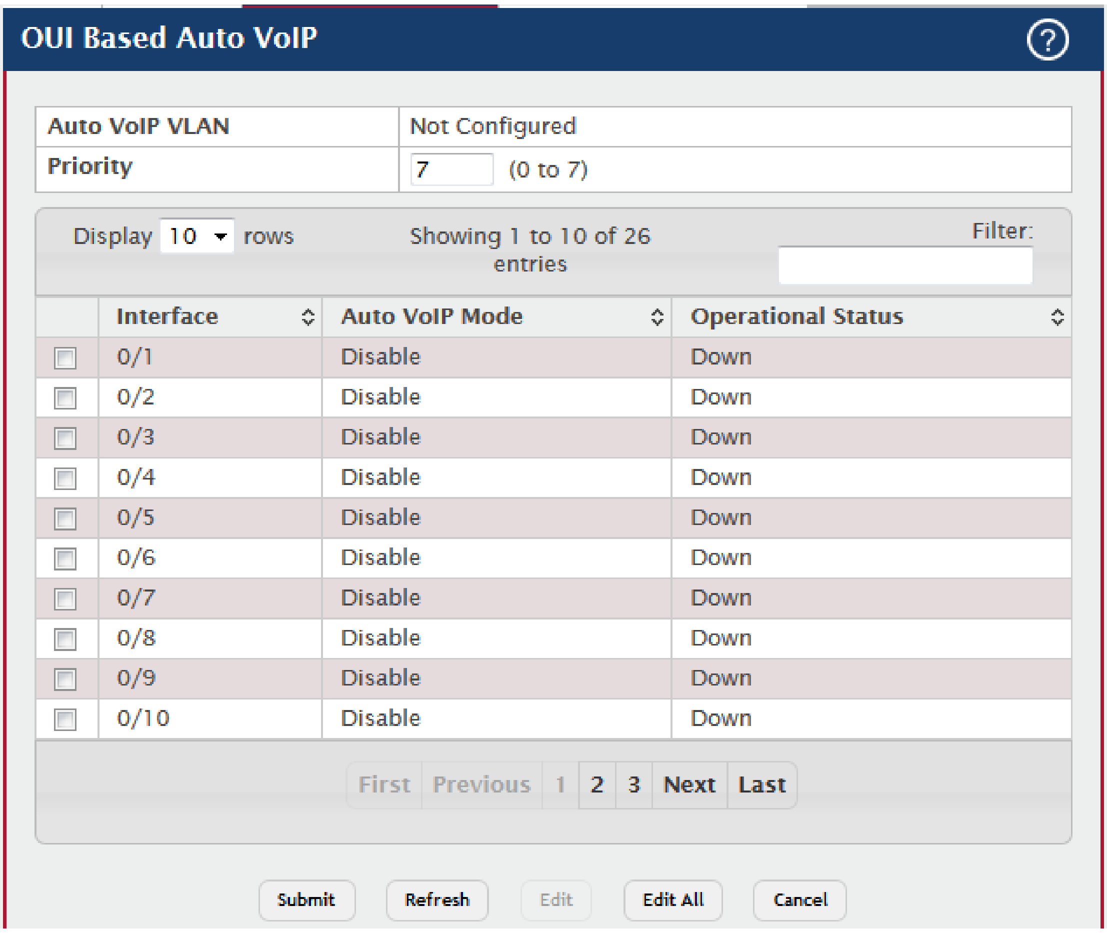
7.1.2.3 OUI Based Auto VoIP

Use this page to configure the Organizationally Unique Identifier (OUI) based Auto VoIP priority and to enable or disable the Auto VoIP mode on the interfaces.

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.**



OUI Based Auto VoIP

Auto VoIP VLAN	Not Configured
Priority	7 (0 to 7)

Display 10 rows   Showing 1 to 10 of 26 entries   Filter:

	Interface	Auto VoIP Mode	Operational Status
□	0/1	Disable	Down
□	0/2	Disable	Down
□	0/3	Disable	Down
□	0/4	Disable	Down
□	0/5	Disable	Down
□	0/6	Disable	Down
□	0/7	Disable	Down
□	0/8	Disable	Down
□	0/9	Disable	Down
□	0/10	Disable	Down

Field	Description
Auto VoIP VLAN	The VLAN used to segregate VoIP traffic from other non-voice traffic. All VoIP traffic that matches a value in the known OUI list gets assigned to this VoIP VLAN.
Priority	The 802.1p priority used for traffic that matches a value in the known OUI list. If the Auto VoIP mode is enabled and the interface detects an OUI match, the device assigns the traffic in that session to the traffic class mapped to this priority value. Traffic classes with a higher value are generally used for time-sensitive 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 OUI-based Auto VoIP on the interface.
Operational	The operational status of an interface. To be up, an interface must be

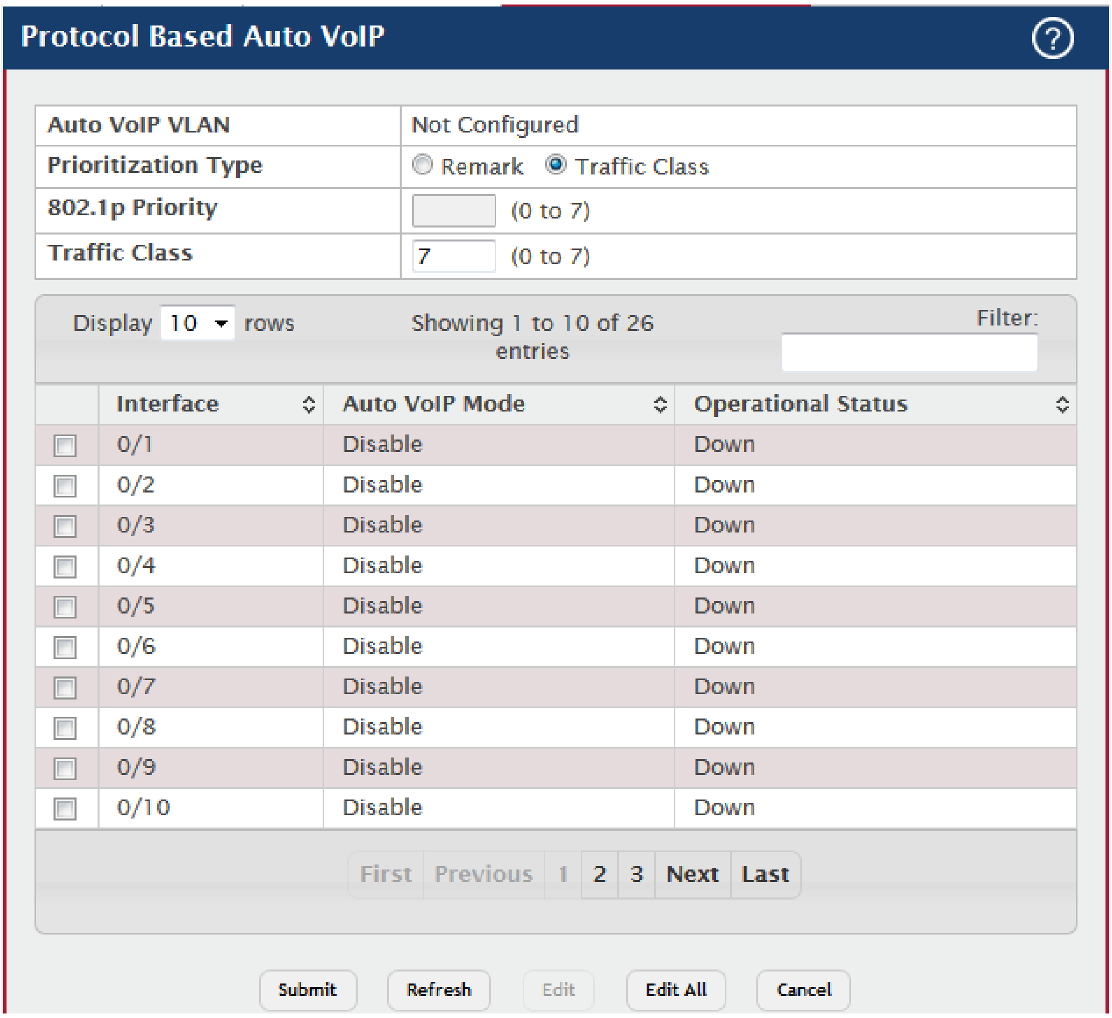
Status	administratively enabled and have a link.

7.1.2.4 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.

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.**



Protocol Based Auto VoIP

Auto VoIP VLAN	Not Configured
Prioritization Type	○ Remark ● Traffic Class
802.1p Priority	(0 to 7)
Traffic Class	7 (0 to 7)

Display 10 rows Showing 1 to 10 of 26 entries Filter:

	Interface	Auto VoIP Mode	Operational Status
□	0/1	Disable	Down
□	0/2	Disable	Down
□	0/3	Disable	Down
□	0/4	Disable	Down
□	0/5	Disable	Down
□	0/6	Disable	Down
□	0/7	Disable	Down
□	0/8	Disable	Down
□	0/9	Disable	Down
□	0/10	Disable	Down

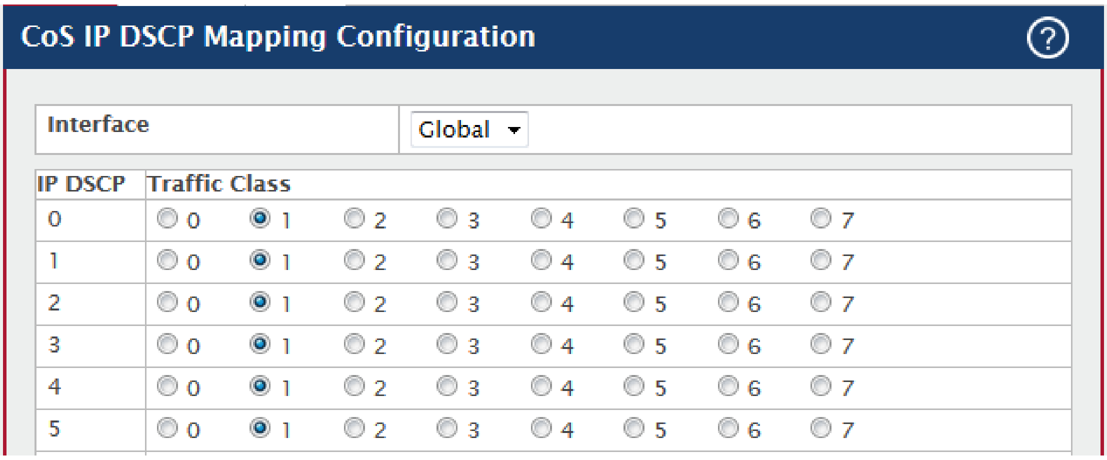
Field	Description
Auto VoIP VLAN	The VLAN used to segregate VoIP traffic from other non-voice traffic. All VoIP traffic in a session identified by the call-control protocol gets

	assigned to this VoIP VLAN.
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.

7.1.3 Class of Service

7.1.3.1 IP DSCP

Use this page to configure the per-interface mapping between the IP DiffServ Code Point (DSCP) value and the traffic class. A DSCP value can be included in the Service Type field of an IP header. When traffic is queued for transmission on the interface, the DSCP value in the IP header is mapped to the traffic class specified on this page. A traffic class with a higher value has priority over a traffic class with a lower value.



CoS IP DSCP Mapping Configuration

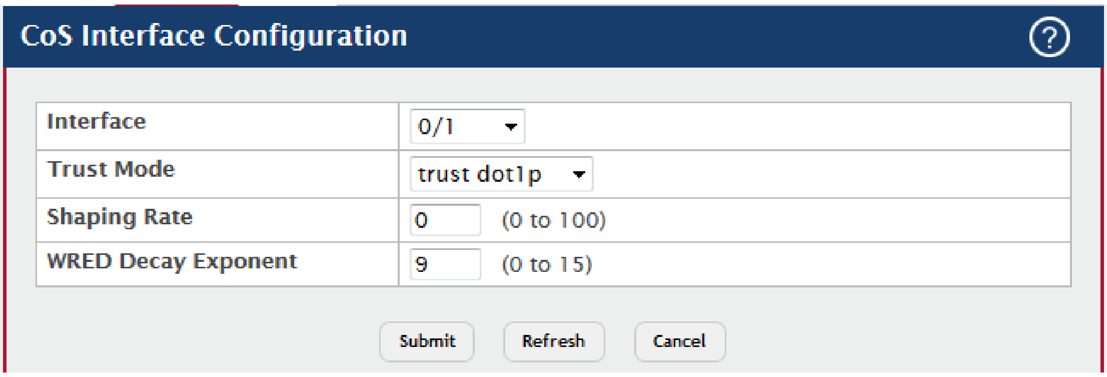
Interface	Global

IP DSCP	Traffic Class							
0	○ 0	● 1	○ 2	○ 3	○ 4	○ 5	○ 6	○ 7
1	○ 0	● 1	○ 2	○ 3	○ 4	○ 5	○ 6	○ 7
2	○ 0	● 1	○ 2	○ 3	○ 4	○ 5	○ 6	○ 7
3	○ 0	● 1	○ 2	○ 3	○ 4	○ 5	○ 6	○ 7
4	○ 0	● 1	○ 2	○ 3	○ 4	○ 5	○ 6	○ 7
5	○ 0	● 1	○ 2	○ 3	○ 4	○ 5	○ 6	○ 7

Field	Description
Interface	The interface to configure. To configure the same IP DSCP-to-Traffic Class mappings on all interfaces, select the Global menu option.
IP DSCP	The list of possible IP DSCP values the IP header can include.
Traffic Class	The internal traffic class to which the corresponding IP DSCP priority value is mapped. The higher the traffic class value, the higher its priority is for sending traffic.

7.1.3.2 Interface

Use this page to configure the per-interface Class of Service (CoS) settings. The CoS feature allows preferential treatment for certain types of traffic over others. To set up this preferential treatment, you can configure the CoS interface settings and individual queues on the egress ports to provide customization that suits the network environment. The level of service is determined by the egress port queue to which the traffic is assigned. When traffic is queued for transmission, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in other queues for that port.



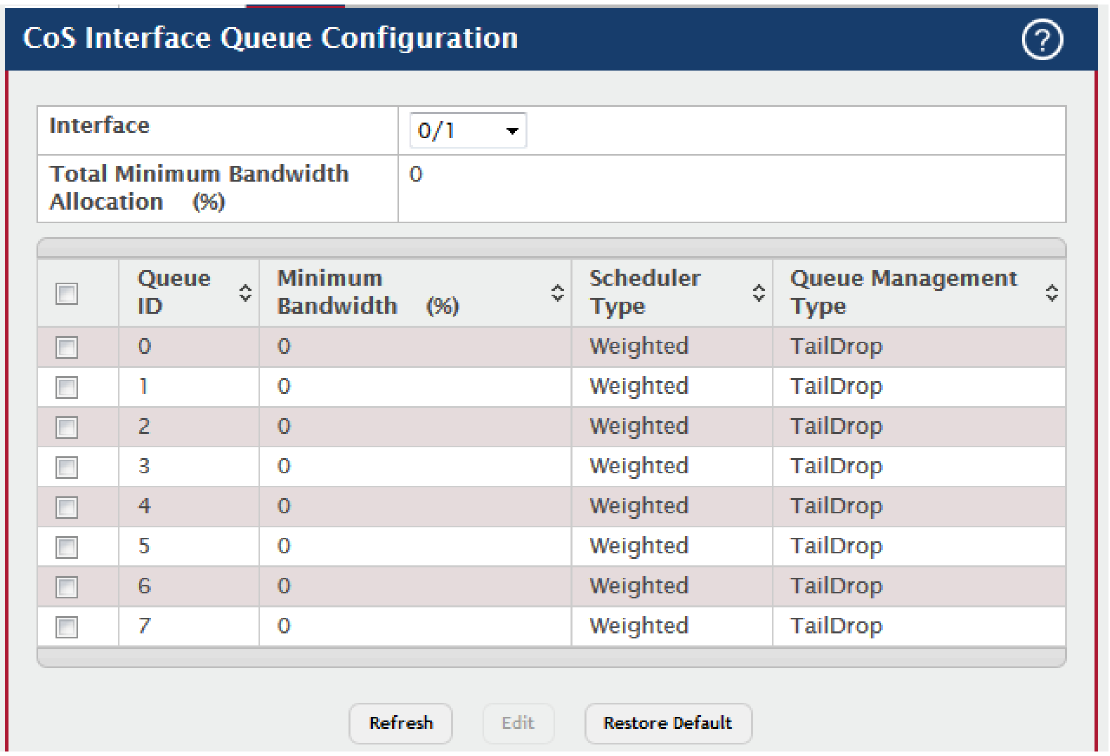
CoS Interface Configuration

Interface	0/1
Trust Mode	trust dot1p
Shaping Rate	0 (0 to 100)
WRED Decay Exponent	9 (0 to 15)

Field	Description
Interface	The interface to configure. To configure the same settings on all interfaces, select the Global menu option.
Trust Mode	The trust mode for ingress traffic on the interface, which is one of the following: untrusted – The interface ignores any priority designations encoded in incoming packets, and instead sends the packets to a traffic queue based on the ingress port's default priority. trust dot1p – The port accepts at face value the 802.1p priority designation encoded within packets arriving on the port. trust ip dscp – The port accepts at face value the IP DSCP priority designation encoded within packets arriving on the port.
Shaping Rate	The upper 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.
WRED Decay Exponent	The decay exponent value used with the Weighted Random Early Detection (WRED) average queue length calculation algorithm.

7.1.3.3 Queue

Use this page to define the behavior of the egress CoS queues on each interface. 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 an interface. Each interface has its own CoS queue-related configuration. To configure the CoS queue settings on an interface, select the interface to configure and click Edit. Or, to configure the same CoS queue settings on all interfaces, select the Global option from the Interface menu and click Edit.



CoS Interface Queue Configuration

Interface	0/1
Total Minimum Bandwidth Allocation (%)	0

□	Queue ID	Minimum Bandwidth (%)	Scheduler Type	Queue Management Type
□	0	0	Weighted	TailDrop
□	1	0	Weighted	TailDrop
□	2	0	Weighted	TailDrop
□	3	0	Weighted	TailDrop
□	4	0	Weighted	TailDrop
□	5	0	Weighted	TailDrop
□	6	0	Weighted	TailDrop
□	7	0	Weighted	TailDrop

Field	Description
Interface	The interface to configure. To configure the same settings on all interfaces, select the Global menu option.
Total Minimum Bandwidth Allocation	Shows the total minimum bandwidth allocation to the selected interface for all the queues.
Queue ID	The CoS queue. The higher the queue value, the higher its priority is for sending traffic.
Minimum Bandwidth	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. A zero value (0) means no guaranteed minimum. The sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum 100.
Scheduler Type	The type of queue processing. Defining this value on a per-queue basis allows you to create the desired service characteristics for different types of traffic. The options are as follows: Weighted – Weighted round robin associates a weight to each queue. Strict – Strict priority services traffic with the highest priority on a queue first.

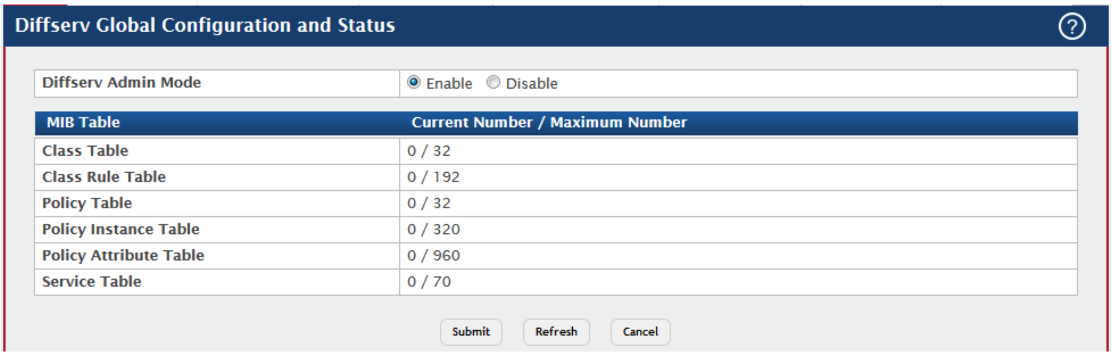
Queue Management Type	The type of queue depth management techniques used for all queues on this interface. The options are as follows: Taildrop – All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped. WRED – Weighted Random Early Detection (WRED) drops packets selectively based their drop precedence level.
Restore Default (Button)	Restores all CoS queue settings on the select interface to the default values. If Global is selected from the Interface menu, all default settings for all interfaces are restored.

7.1.4 Diffserv

7.1.4.1 Global

Use this page to configure the administrative mode of Differentiated Services (DiffServ) support on the device and to view the current and maximum number of entries in each of the main DiffServ private MIB tables. DiffServ allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Packets are classified and processed based on defined criteria. The classification criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.



Diffserv Global Configuration and Status

Diffserv Admin Mode ● Enable ○ Disable

MIB Table	Current Number / Maximum Number
Class Table	0 / 32
Class Rule Table	0 / 192
Policy Table	0 / 32
Policy Instance Table	0 / 320
Policy Attribute Table	0 / 960
Service Table	0 / 70

Field	Description
Diffserv Admin Mode	The administrative mode of DiffServ on the device. While disabled, the DiffServ configuration is retained and can be changed, but it is not active. While enabled, Differentiated Services are active.
MIB Table	

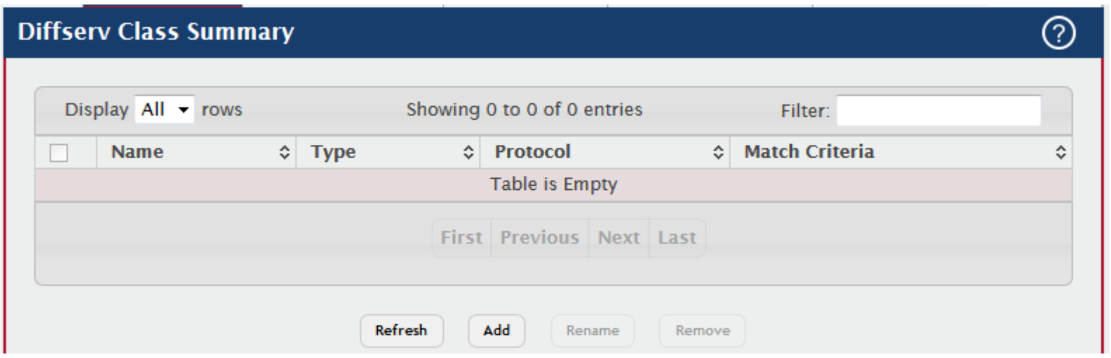
The information in this table displays the number of entries (rows) that are currently in each of the main DiffServ private MIB tables and the maximum number of rows that can exist in each table.	
Class Table	The current and maximum number of classifier entries in the table. DiffServ classifiers differentiate among traffic types.
Class Rule Table	The current and maximum number of class rule entries in the table. Class rules specify the match criteria that belong to a class definition.
Policy Table	The current and maximum number of policy entries in the table. The policy determines the traffic conditioning or service provisioning actions applied to a traffic class.
Policy Instance Table	The current and maximum number of policy-class instance entries in the table. A policy-class instance is a policy that is associated with an existing DiffServ class.
Policy Attribute Table	The current and maximum number of policy attribute entries in the table. A policy attribute entry attaches various policy attributes to a policy-class instance.
Service Table	The current and maximum number of service entries in the table. A service entry associates a DiffServ policy with an interface and inbound or outbound direction.

7.1.4.2 Class Summary

Use this page to create or remove DiffServ classes and to view summary information about the classes that exist on the device. Creating a class is the first step in using DiffServ to provide Quality of Service. After a class is created, you can define the match criteria for the class.

Use the buttons to perform the following tasks:

- To add a DiffServ class, click **Add**.
- To change the name of an existing class, select the entry to modify and click **Rename**.
- To remove one or more configured classes, select each entry to delete and click **Remove.**You must confirm the action before the entry is deleted.



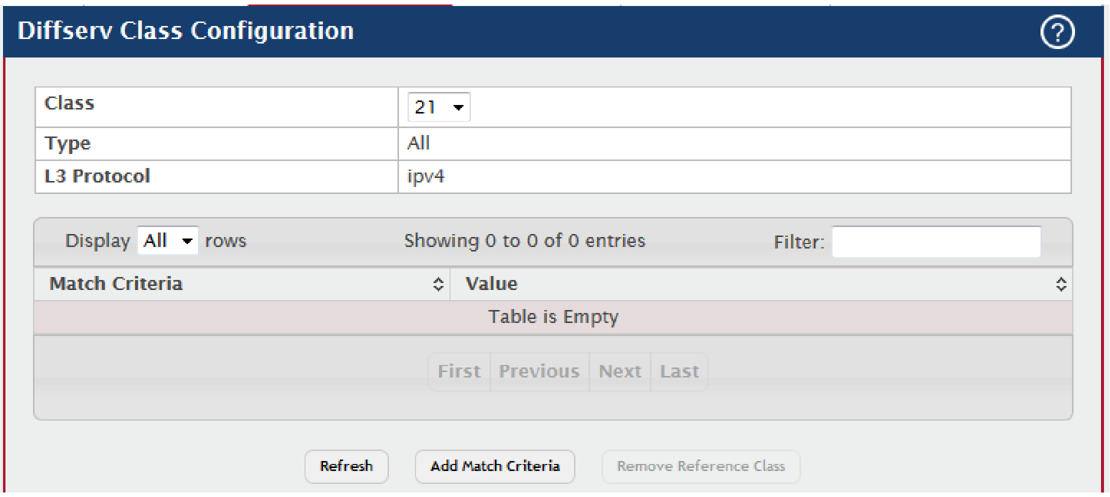
Field	Description
Name	The name of the DiffServ class. When adding a new class or renaming an existing class, the name of the class is specified in the Class field of the dialog window.
Type	The class type, which is one of the following: All – All the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria.
Protocol	The Layer 3 protocol to use for filtering class types, which is either IPv4 or IPv6.
Match Criteria	The criteria used to match packets.

7.1.4.3 Class Configuration

Use this page to define the criteria to associate with a DiffServ class. As packets are received or transmitted, these DiffServ classes are used to classify and prioritize packets. Each class can contain multiple match criteria.

After you select the class to configure from the **Class** menu, use the buttons to perform the following tasks:

- To define criteria for matching packets within a class, click **Add Match Criteria**. Once you add a match criteria entry to a class, you cannot edit or remove the entry. However, you can add more match criteria entries to a class until the maximum number of entries has been reached for the class.
- To remove the associated reference class from the selected class, click **Remove Reference Class.** You must confirm the action before the reference class is removed. Note that unless the reference class is the last entry in the list of match criteria, the Reference Class match type remains in the list as a placeholder, but the associated value is N/A, and the previously referenced class is removed.



Diffserv Class Configuration

Class	21
Type	All
L3 Protocol	ipv4

Display All rows Showing 0 to 0 of 0 entries Filter:

Match Criteria	Value
Table is Empty	

Field	Description
Class	The name of the class. To configure match criteria for a class, select its name from the menu.
Type	The class type, which is one of the following: All – All the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria.
Protocol	The Layer 3 protocol to use for filtering class types, which is either IPv4 or IPv6.
Match Criteria	The type of match criteria defined for the selected class.
Value	The configured value of the match criteria that corresponds to the match type. After you click Add Match Criteria, the Add Match Criteria window opens and allows you to define the match criteria for the selected class. The window lists the match criteria that are available for the class. To add match criteria, select the check box associated with the criteria type. The fields to configure the match values appear after you select the match type. Each match criteria type can be used only once within a class. If a reference class includes the match criteria type, it cannot be used as an additional match type within the class, and the match criteria type cannot be selected or configured.
Any	Select this option to specify that all packets are considered to match the specified class. There is no need to configure additional match criteria if Any is selected because a match will occur on all packets.
Reference Class	Select this option to reference another class for criteria. The match

	criteria defined in the referenced class is as match criteria in addition to the match criteria you define for the selected class. After selecting this option, the classes that can be referenced are displayed. Select the class to reference. A class can reference at most one other class of the same type.
Class of Service	Select this option to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value.
Secondary Class of Service	Select this option to require the secondary CoS value in an Ethernet frame header to match the specified secondary CoS value.
Ethertype	Select this option to require the EtherType value in the Ethernet frame header to match the specified EtherType value. After you select this option, specify the EtherType value in one of the following two fields: Ethertype Keyword – The menu includes several common protocols that are mapped to their EtherType values. Ethertype Value – This field accepts custom EtherType values.
VLAN	Select this option to require a packet's VLAN ID to match a VLAN ID or a VLAN ID within a continuous range. If you configure a range, a match occurs if a packet's VLAN ID is the same as any VLAN ID within the range. After you select this option, use the following fields to configure the VLAN match criteria: VLAN ID – The VLAN ID to match.
Secondary VLAN	Select this option to require a packet's VLAN ID to match a secondary VLAN ID or a secondary VLAN ID within a continuous range. If you configure a range, a match occurs if a packet's secondary VLAN ID is the same as any secondary VLAN ID within the range. After you select this option, use the following fields to configure the secondary VLAN match criteria: Secondary VLAN ID – The secondary VLAN ID to match.
Source MAC Address	Select this option to require a packet's source MAC address to match the specified MAC address. After you select this option, use the following fields to configure the source MAC address match criteria: MAC Address – The source MAC address to match. MAC Mask – The MAC mask, which specifies the bits in the source MAC address to compare against an Ethernet frame. Use F's and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is

	ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
Destination MAC Address	Select this option to require a packet's destination MAC address to match the specified MAC address. After you select this option, use the following fields to configure the destination MAC address match criteria: MAC Address – The destination MAC address to match. MAC Mask – The MAC mask, which specifies the bits in the destination MAC address to compare against an Ethernet frame. Use F's and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
Source IP Address	Select this option to require the source IP address in a packet header to match the specified values. After you select this option, use the following fields to configure the source IP address match criteria: IP Address – The source IP address to match. IP Mask – A valid subnet mask, which determines the bits in the IP address that are significant. Note that this is not a wildcard mask.
Destination IP Address	Select this option to require the destination IP address in a packet header to match the specified values. After you select this option, use the following fields to configure the destination IP address match criteria: IP Address – The destination IP address to match. IP Mask – A valid subnet mask, which determines the bits in the IP address that are significant. Note that this is not a wildcard mask.
Source IPv6 Address	Select this option to require the source IPv6 address in a packet header to match the specified values. After you select this option, use the following fields to configure the source IPv6 address match criteria: Source Prefix – The source IPv6 prefix to match. Source Prefix Length – The IPv6 prefix length.
Destination IPv6 Address	Select this option to require the destination IPv6 address in a packet header to match the specified values. After you select this option, use

	the following fields to configure the destination IPv6 address match criteria: Destination Prefix – The destination IPv6 prefix to match. Destination Prefix Length – The IPv6 prefix length.
Source L4 Port	Select this option to require a packet's TCP/UDP source port to match the specified port or the port number within a range of port numbers. If you configure a range, a match occurs if a packet's source port number is the same as any source port number within the range. After you select this option, use the following fields to configure a source port keyword, source port number, or source port range for the match criteria: Protocol – Select the desired L4 keyword from the list on which the match is based. If you select a keyword, the other source port configuration fields are not configurable. Port – The source port number to match.
Destination L4 Port	Select this option to require a packet's TCP/UDP destination port to match the specified port or the port number within a range of port numbers. If you configure a range, a match occurs if a packet's destination port number is the same as any destination port number within the range. After you select this option, use the following fields to configure a destination port keyword, destination port number, or destination port range for the match criteria: Protocol – Select the desired L4 keyword from the list on which the match is based. If you select a keyword, the other destination port configuration fields are not configurable. Port – The destination port number to match.
IP DSCP	Select this option to require the packet's IP DiffServ Code Point (DSCP) value to match the specified value. The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header. After you select this option, use one of the following fields to configure the IP DSCP match criteria: IP DSCP Keyword – The IP DSCP keyword code that corresponds to the IP DSCP value to match. If you select a keyword, you cannot configure an IP DSCP Value. IP DSCP Value – The IP DSCP value to match.
IP Precedence	Select this option to require the packet's IP Precedence value to match the number configured in the IP Precedence Value field. The IP

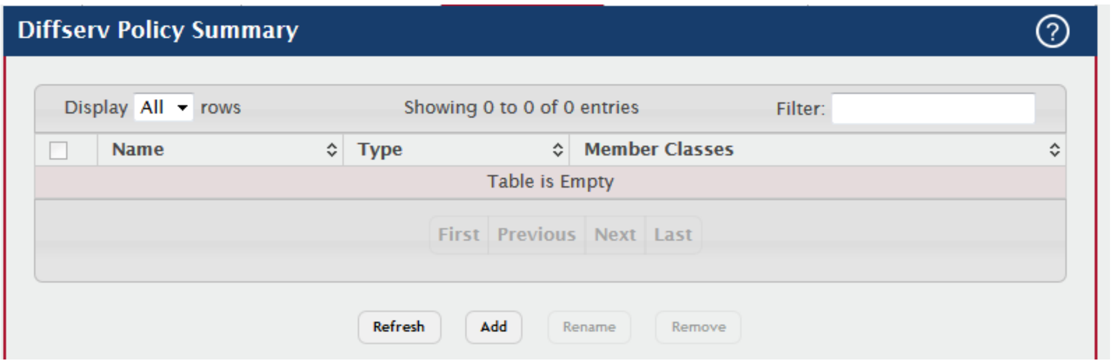
	Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header.
IP TOS	Select this option to require the packet's Type of Service (ToS) bits in the IP header to match the specified value. The IP ToS field in a packet is defined as all eight bits of the Service Type octet in the IP header. After you select this option, use the following fields to configure the ToS match criteria: IP TOS Bits – Enter a two-digit hexadecimal number to match the bits in a packet's ToS field. IP TOS Mask – Specify the bit positions that are used for comparison against the IP ToS field in a packet.
Protocol	Select this option to require a packet header's Layer 4 protocol to match the specified value. After you select this option, use one of the following fields to configure the protocol match criteria: Protocol – The L4 keyword that corresponds to value of the IANA protocol number to match. If you select a keyword, you cannot configure a Protocol Value. Protocol Value – The IANA L4 protocol number value to match.
Flow Label	Select this option to require an IPv6 packet's flow label to match the configured value. The flow label is a 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers.

7.1.4.4 Policy Summary

Use this page to create or remove DiffServ policies and to view summary information about the policies that exist on the device. A policy defines the QoS attributes for one or more traffic classes. A policy attribute identifies the action taken when a packet matches a class rule. A policy is applied to a packet when a class match within that policy is found.

Use the buttons to perform the following tasks:

- To add a DiffServ policy, click **Add**.
- To change the name of an existing policy, select the entry to modify and click **Rename**.
- To remove one or more configured policies, select each entry to delete and click **Remove.**You must confirm the action before the entry is deleted.



Diffserv Policy Summary

Display All rows Showing 0 to 0 of 0 entries Filter:

□	Name	Type	Member Classes
Table is Empty			

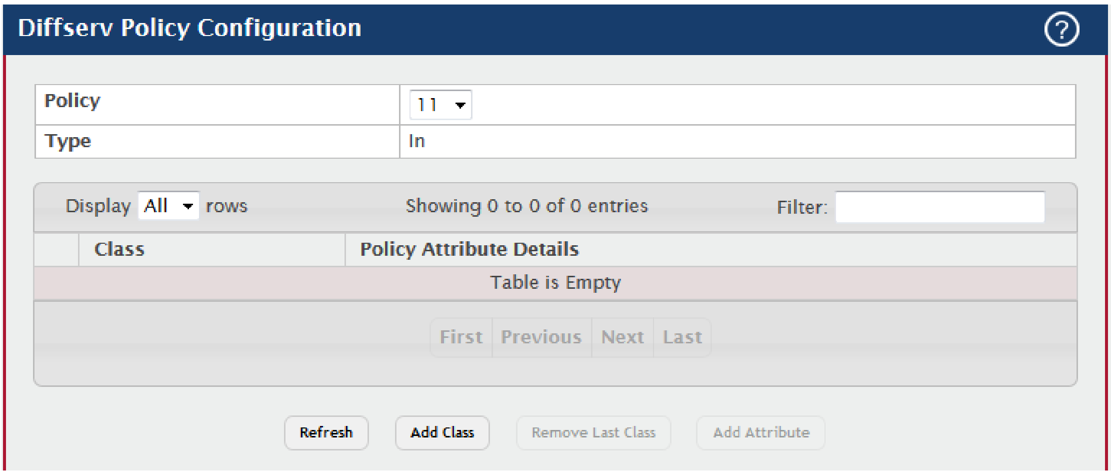
Field	Description
Name	The name of the DiffServ policy. When adding a new policy or renaming an existing policy, the name of the policy is specified in the Policy field of the dialog window.
Type	The traffic flow direction to which the policy is applied: In – The policy is specific to inbound traffic. Out – The policy is specific to outbound traffic direction.
Member Classes	The DiffServ class or classes that have been added to the policy.

7.1.4.5 Policy Configuration

Use this page to add or remove a DiffServ policy-class association and to configure the policy attributes. The policy attributes identify the action or actions taken when a packet matches a class rule.

After you select the policy to configure from the **Policy** menu, use the buttons to perform the following tasks:

- To add a class to the policy, click **Add Class**.
- To add attributes to a policy or to change the policy attributes, select the policy with the attributes to configure and click **Add Attribute**.
- To remove the most recently associated class from the selected policy, click **Remove Last Class.**



Diffserv Policy Configuration

Policy	11
Type	In

Display All rows Showing 0 to 0 of 0 entries Filter:

Class	Policy Attribute Details
Table is Empty	

Field	Description
Policy	The name of the policy. To add a class to the policy, remove a class from the policy, or configure the policy attributes, you must first select its name from the menu.
Type	The traffic flow direction to which the policy is applied.
Class	The DiffServ class or classes associated with the policy. The policy is applied to a packet when a class match within that policy-class is found.
Policy Attribute Details	The policy attribute types and their associated values that are configured for the policy. After you click Add Attribute, a window opens and allows you to define the policy attributes for the selected policy. To add and configure the policy attributes, select the check box associated with the attribute type. The fields to configure the attribute values appear after you select the attribute type.
Assign Queue	Select this option to assign matching packets to a traffic queue. Use the Queue ID Value field to select the queue to which the packets of this policy-class are assigned.
Drop	Select this option to drop packets that match the policy-class.
Mark CoS	Select this option to mark all packets in a traffic stream with the specified Class of Service (CoS) queue value. Use the Class of Service field to select the CoS value to mark in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted.
Mark CoS as	Select this option to mark the priority field of the 802.1p header in the

Secondary CoS	outer tag of a double-VLAN tagged packet with the same CoS value that is included in the inner tag.
Mark IP DSCP	Select this option to mark all packets in the associated traffic stream with the specified IP DSCP value. After you select this option, use one of the following fields to configure the IP DSCP value to mark in packets that match the policy-class: IP DSCP Keyword – The IP DSCP keyword code that corresponds to the IP DSCP value. If you select a keyword, you cannot configure an IP DSCP Value. IP DSCP Value – The IP DSCP value.
Mark IP Precedence	Select this option to mark all packets in the associated traffic stream with the specified IP Precedence value. After you select this option, use the IP Precedence Value field to select the IP Precedence value to mark in packets that match the policy-class.
Mirror Interface	Select this option to copy the traffic stream to a specified egress port (physical or LAG) without bypassing normal packet forwarding. This action can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. Use the Interface menu to select the interface to which traffic is mirrored.
Police Simple	Select this option to enable the simple traffic policing style for the policy-class. The simple form of the police attribute uses a single data rate and burst size, resulting in two outcomes (conform and violate). After you select this option, configure the following policing criteria: Color Mode – The type of color policing used in DiffServ traffic conditioning. Color Conform Class – For color-aware policing, packets in this class are metered against both the committed information rate (CIR) and the peak information rate (PIR). The class definition used for policing color awareness is only allowed to contain a single, non-excluded class match condition identifying one of the supported comparison fields: CoS, IP DSCP, IP Precedence, or Secondary COS. Committed Rate (Kbps) – The maximum allowed arrival rate of incoming packets for this class. Committed Burst Size (Kbytes) – The amount of conforming traffic allowed in a burst. Conform Action – The action taken on packets that are considered conforming (below the police rate).

	Violate Action – The action taken on packets that are considered non-conforming (above the police rate).
Police Single Rate	Select this option to enable the single-rate traffic policing style for the policy-class. The single-rate form of the police attribute uses a single data rate and two burst sizes, resulting in three outcomes (conform, exceed, and violate). After you select this option, configure the following policing criteria: Color Mode – The type of color policing used in DiffServ traffic conditioning. Color Conform Class – For color-aware policing, packets are metered against the committed information rate (CIR) and the peak information rate (PIR). The class definition used for policing color awareness is only allowed to contain a single, non-excluded class match condition identifying one of the supported comparison fields: CoS, IP DSCP, IP Precedence, or Secondary COS. This field is available only if one or more classes that meets the color-awareness criteria exist. Color Exceed Class – For color-aware policing, packets are metered against the PIR only. Committed Rate (Kbps) – The maximum allowed arrival rate of incoming packets for this class. Committed Burst Size (Kbytes) – The amount of conforming traffic allowed in a burst. Excess Burst Size (Kbytes) – The amount of conforming traffic allowed to accumulate beyond the Committed Burst Size (Kbytes) value during longer-than-normal idle times. This value allows for occasional bursting. Conform Action – The action taken on packets that are considered conforming (below the police rate). Exceed Action – The action taken on packets that are considered to exceed the committed burst size but are within the excessive burst size. Violate Action – The action taken on packets that are considered non-conforming (above the police rate).
Police Two Rate	Select this option to enable the two-rate traffic policing style for the policy-class. The two-rate form of the police attribute uses two data rates and two burst sizes. Only the smaller of the two data rates is intended to be guaranteed. After you select this option, configure the

	following policing criteria: Color Mode – The type of color policing used in DiffServ traffic conditioning. Color Conform Class – For color-aware policing, packets are metered against the committed information rate (CIR) and the peak information rate (PIR). The class definition used for policing color awareness is only allowed to contain a single, non-excluded class match condition identifying one of the supported comparison fields: CoS, IP DSCP, IP Precedence, or Secondary COS. This field is available only if one or more classes that meets the color-awareness criteria exist. Color Exceed Class – For color-aware policing, packets are metered against the PIR. Committed Rate (Kbps) – The maximum allowed arrival rate of incoming packets for this class. Committed Burst Size (Kbytes) – The amount of conforming traffic allowed in a burst. Peak Rate (Kbps) – The maximum peak information rate for the arrival of incoming packets for this class. Excess Burst Size (Kbytes) – The maximum size of the packet burst that can be accepted to maintain the Peak Rate (Kbps). Conform Action – The action taken on packets that are considered conforming (below the police rate). Exceed Action – The action taken on packets that are considered to exceed the committed burst size but are within the excessive burst size. Violate Action – The action taken on packets that are considered non-conforming (above the police rate).
Redirect Interface	Select this option to force a classified traffic stream to the specified egress port (physical port or LAG). Use the Interface field to select the interface to which traffic is redirected.

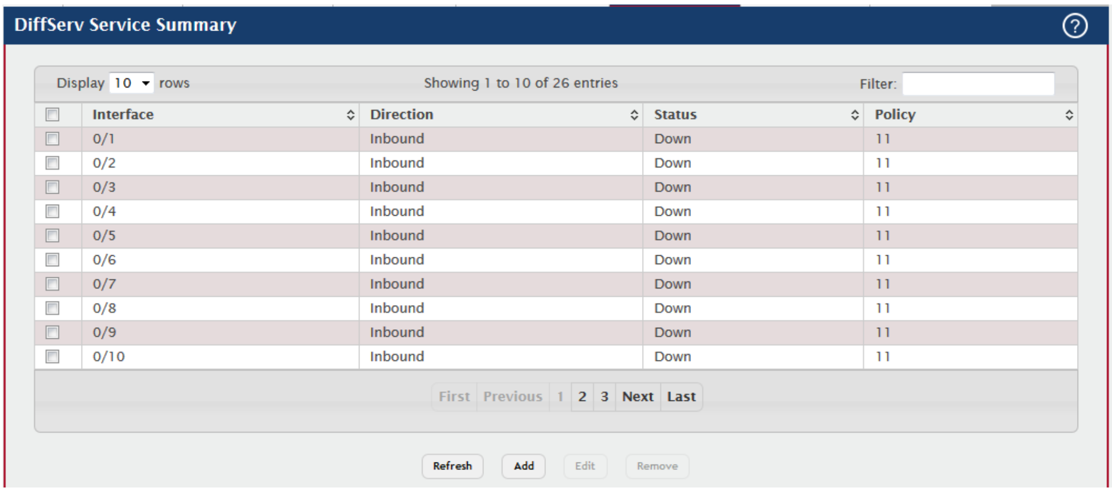
7.1.4.6 Service Summary

Use this page to add DiffServ policies to interfaces, remove policies from interfaces, and edit policy-interface mappings.

Use the buttons to perform the following tasks:

- To add a policy to an interface, click **Add**.

- To edit a configured interface-policy association, select the entry to modify and click **Edit**.
- To remove one or more configured interface-policy associations, select each entry to delete and click **Remove.** You must confirm the action before the entry is deleted.



DiffServ Service Summary

Display 10 rows   Showing 1 to 10 of 26 entries   Filter:

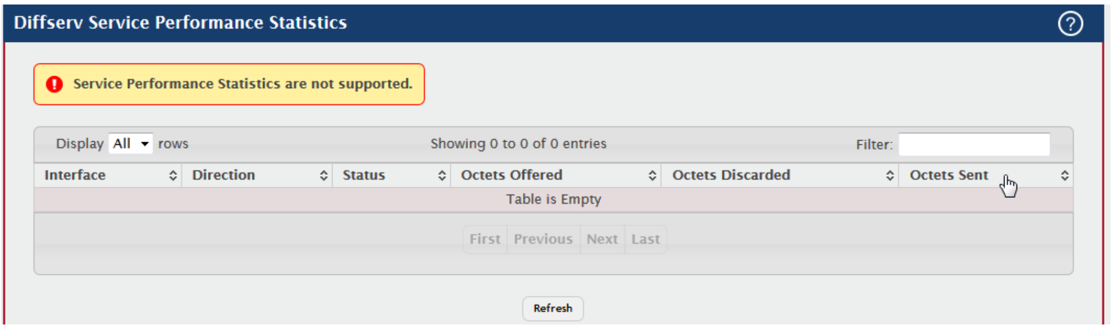
□	Interface	Direction	Status	Policy
□	0/1	Inbound	Down	11
□	0/2	Inbound	Down	11
□	0/3	Inbound	Down	11
□	0/4	Inbound	Down	11
□	0/5	Inbound	Down	11
□	0/6	Inbound	Down	11
□	0/7	Inbound	Down	11
□	0/8	Inbound	Down	11
□	0/9	Inbound	Down	11
□	0/10	Inbound	Down	11

Field	Description
Interface	The interface associated with the rest of the data in the row. Only interfaces that have an associated policy are listed in the table. To configure the same settings on all interfaces, select the Global menu option.
Direction	The traffic flow direction to which the policy is applied: Inbound – The policy is applied to traffic as it enters the interface. Outbound – The policy is applied to traffic as it exits the interface
Status	The status of the policy on the interface. A policy is Up if DiffServ is globally enabled, and if the interface is administratively enabled and has a link. Otherwise, the status is Down.
Policy	The DiffServ policy associated with the interface. When you click Add or Edit, the Configure Service window opens and allows you to configure DiffServ interface policies. Specifying None for a policy has no effect when adding or editing interface policies. To remove an interface-policy mapping, use the Remove button on the parent page. The following information describes the fields in this window.
Interface	Select an interface to associate with a policy.
Policy In	The menu lists all policies configured with a type of In. Select the

	policy to apply to traffic as it enters the interface.
Policy Out	The menu lists all policies configured with a type of Out. Select the policy to apply to traffic as it exits the interface.

7.1.4.7 Service Statistics

This page displays service-level statistical information for all interfaces in the system to which a DiffServ policy has been attached.



Diffserv Service Performance Statistics

Service Performance Statistics are not supported.

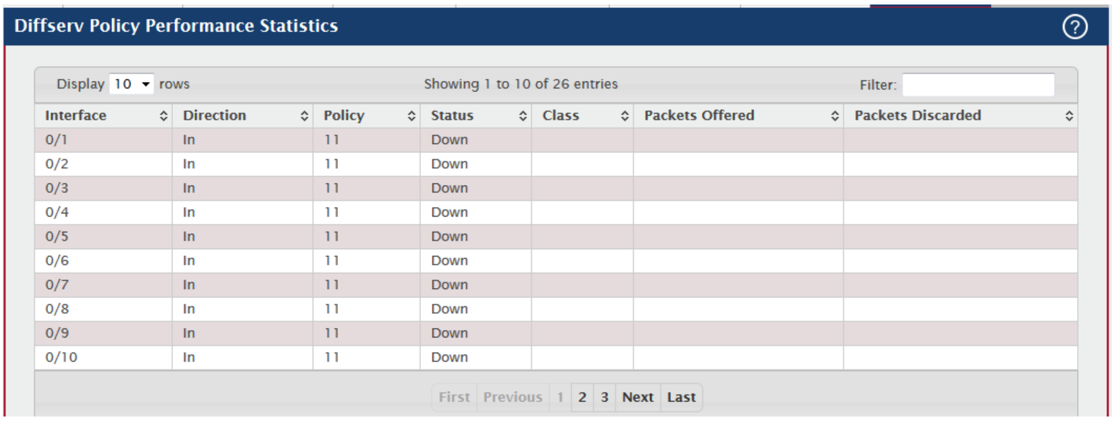
Display All rows   Showing 0 to 0 of 0 entries   Filter:

Interface	Direction	Status	Octets Offered	Octets Discarded	Octets Sent
Table is Empty					

Field	Description
Interface	The interface associated with the rest of the data in the row. The table displays all interfaces that have a DiffServ policy currently attached in a traffic flow direction.
Direction	The traffic flow direction to which the policy is applied: In – The policy is applied to traffic as it enters the interface. Out – The policy is applied to traffic as it exits the interface.
Status	The operational status of this service interface, either Up or Down.

7.1.4.8 Policy Statistics

This page displays class-oriented statistical information for the policy, which is specified by the interface and direction.



Diffserv Policy Performance Statistics

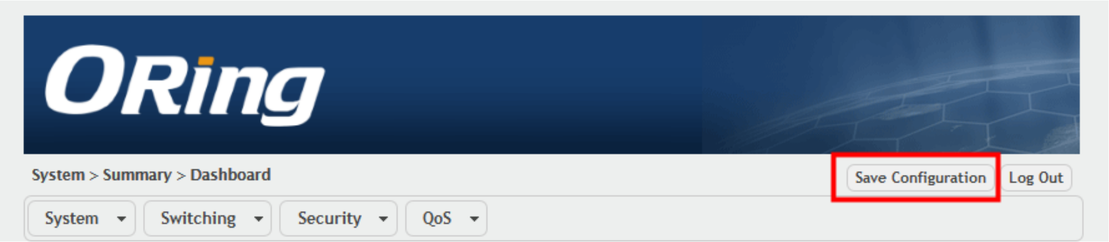
Display 10 rows   Showing 1 to 10 of 26 entries   Filter:

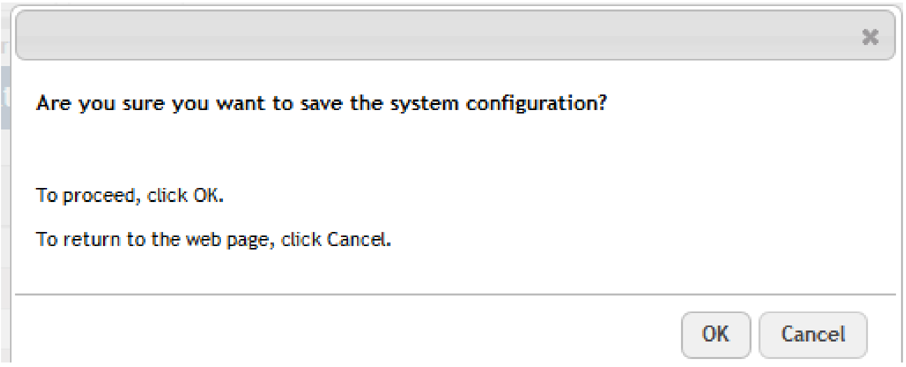
Interface	Direction	Policy	Status	Class	Packets Offered	Packets Discarded
0/1	In	11	Down			
0/2	In	11	Down			
0/3	In	11	Down			
0/4	In	11	Down			
0/5	In	11	Down			
0/6	In	11	Down			
0/7	In	11	Down			
0/8	In	11	Down			
0/9	In	11	Down			
0/10	In	11	Down			

Field	Description
Interface	The interface associated with the rest of the data in the row. The table displays all interfaces that have a DiffServ policy currently attached in a traffic flow direction.
Direction	The traffic flow direction to which the policy is applied: In – The policy is applied to traffic as it enters the interface. Out – The policy is applied to traffic as it exits the interface.
Policy	The name of the policy currently attached to the interface.
Status	The operational status of the policy currently attached to the interface.
Class	The DiffServ class currently defined for the attached policy.
Packets Offered	The total number of packets offered to all class instances in this service policy before their defined DiffServ treatment is applied. This is the overall count per-interface, per-direction.
Packets Discarded	The total number of packets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.

8.1 Save Config

All config save button , if the device configuration has changed,user can user this button , save the configuration to ensure that it is preserved , (if loss save , reboot device config will loss)



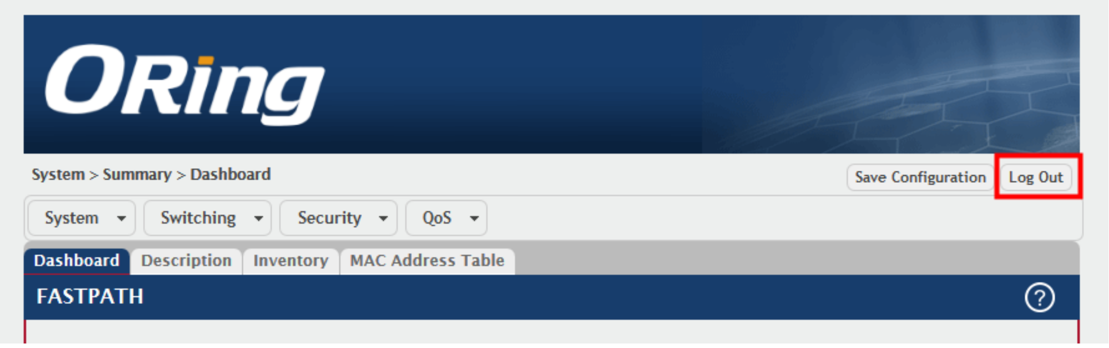

Are you sure you want to save the system configuration?

To proceed, click OK.

To return to the web page, click Cancel.

9.1 Logout

This button can help user log out WEB GUI


ORing
System > Summary > Dashboard
Save Configuration
Log Out
System
Switching
Security
QoS
Dashboard
Description
Inventory
MAC Address Table
FASTPATH