Fastpath NOS Web guide

Fastpath NOS Web guide

Table of Contents

1. Getting Started 1
    1.1. Management Options 2
    1.2. Using Web-based Management 3
    1.3. Supported Web Browsers 4
    1.4. Connecting to the Switch 5
    1.5. Login Web-based Management 6
2. System 7
    2.1. Summary 8
        2.1.1. System > Summary > Dashboard 8
        2.1.2. System > Summary > Description 10
        2.1.3. System > Summary > Inventory 11
    2.2. System > Advanced Configuration 13
        2.2.1. System > Advanced Configuration > DHCP Server 13
            2.2.1.1. System > Advanced Configuration > DHCP Server > Global 13
            2.2.1.2. System > Advanced Configuration > DHCP Server > Excluded Addresses 14
            2.2.1.3. System > Advanced Configuration > DHCP Server > Pool Summary 15
            2.2.1.4. System > Advanced Configuration > DHCP Server > Pool Configuration 17
            2.2.1.5. System > Advanced Configuration > DHCP Server > Pool Options 19
            2.2.1.6. System > Advanced Configuration > DHCP Server > Bindings 20
            2.2.1.7. System > Advanced Configuration > DHCP Server > Statistics 21
            2.2.1.8. System > Advanced Configuration > DHCP Server > Conflicts 23
        2.2.2. System > Advanced Configuration > DNS 24
            2.2.2.1. System > Advanced Configuration > DNS > Configuration 24
            2.2.2.2. System > Advanced Configuration > DNS > IP Mapping 25
            2.2.2.3. System > Advanced Configuration > DNS > Source Interface Configuration 26
        2.2.3. System > Advanced Configuration > Email Alerts 27
            2.2.3.1. System > Advanced Configuration > Email Alerts > Global 27
            2.2.3.2. System > Advanced Configuration > Email Alerts > Test 28
            2.2.3.3. System > Advanced Configuration > Email Alerts > Server 28
            2.2.3.4. System > Advanced Configuration > Email Alerts > Statistics 29
            2.2.3.5. System > Advanced Configuration > Email Alerts > Subject 30
            2.2.3.6. System > Advanced Configuration > Email Alerts > Address 30
        2.2.4. System > Advanced Configuration > Green Ethernet 31
            2.2.4.1. System > Advanced Configuration > Green Ethernet > Status 31
            2.2.4.2. System > Advanced Configuration > Green Ethernet > Configuration 32
            2.2.4.3. System > Advanced Configuration > Green Ethernet > Interface 33
            2.2.4.4. System > Advanced Configuration > Green Ethernet > Local 34
            2.2.4.5. System > Advanced Configuration > Green Ethernet > Remote Devices 35
            2.2.4.6. System > Advanced Configuration > Green Ethernet > Statistics 36
            2.2.4.7. System > Advanced Configuration > Green Ethernet > EEE History 37
        2.2.5. System > Advanced Configuration > Protection 38
            2.2.5.1. System > Advanced Configuration > Protection > Denial of Service 38
        2.2.6. System > Advanced Configuration > LLDP 40

2.2.6.1. System > Advanced Configuration > LLDP > Global 40
2.2.6.2. System > Advanced Configuration > LLDP > Interface 41
2.2.6.3. System > Advanced Configuration > LLDP > Local Devices 43
2.2.6.4. System > Advanced Configuration > LLDP > Remote Devices 44
2.2.6.5. System > Advanced Configuration > LLDP > Statistics 45
2.2.6.6. System > Advanced Configuration > LLDP > LLDP-MED > Global 47
2.2.6.7. System > Advanced Configuration > LLDP > LLDP-MED > Interface 48
2.2.6.8. System > Advanced Configuration > LLDP > LLDP-MED > Local Devices 49
2.2.6.9. System > Advanced Configuration > LLDP > LLDP-MED > Remote Devices 50
2.2.6.10. System > Advanced Configuration > SNMP > Community 52
2.2.6.11. System > Advanced Configuration > SNMP > Trap Receiver v1/v2 53
2.2.6.12. System > Advanced Configuration > SNMP > Trap Receiver v3 54
2.2.6.13. System > Advanced Configuration > SNMP > Notify Filter 56
2.2.6.14. System > Advanced Configuration > SNMP > Supported MIBs 57
2.2.6.15. System > Advanced Configuration > SNMP > Access Control Group 58
2.2.6.16. System > Advanced Configuration > SNMP > Access Control View 60
2.2.6.17. System > Advanced Configuration > SNMP > User Security Model 61
2.2.7. System > Advanced Configuration > SNTP 62
2.2.7.1. System > Advanced Configuration > SNTP > Global Configuration 62
2.2.7.2. System > Advanced Configuration > SNTP > Global Status 63
2.2.7.3. System > Advanced Configuration > SNTP > Server Configuration 65
2.2.7.4. System > Advanced Configuration > SNTP > Server Status 66
2.2.7.5. System > Advanced Configuration > SNTP > Source Interface Configuration 67
2.2.8. System > Advanced Configuration > Time Ranges 68
2.2.8.1. System > Advanced Configuration > Time Ranges > Configuration 68
2.2.8.2. System > Advanced Configuration > Time Ranges > Entry Configuration 69
2.2.9. System > Advanced Configuration > Time Zone 71
2.2.9.1. System > Advanced Configuration > Time Zone > Summary 71
2.2.9.2. System > Advanced Configuration > Time Zone > Time Zone 73
2.2.9.3. System > Advanced Configuration > Time Zone > Summer Time 74
2.2.10. System > Advanced Configuration > Trap Manager 76
2.2.10.1. System > Advanced Configuration > Trap Manager > Trap Log 76
2.2.10.2. System > Advanced Configuration > Trap Manager > Trap Flags 77
2.2.11. System > Advanced Configuration > PoE System 78
2.2.11.1. System > Advanced Configuration > PoE System > Status 78
2.2.11.2. System > Advanced Configuration > PoE System > Interface 79
2.3. System > Connectivity 80
2.3.1. System > Connectivity > IPv4 80
2.3.2. System > Connectivity > IPv6 81
2.3.3. System > Connectivity > IPv6 Neighbors 83
2.3.4. System > Connectivity > DHCP Client Options 84
2.4. System > Firmware 85

2.4.1. System > Firmware > Status 85
2.4.2. System > Firmware > Configuration and Upgrade 85
2.4.3. System > Firmware > AutoInstall 86
2.5. System > Logs 88
2.5.1. System > Logs > Buffered Log 88
2.5.2. System > Logs > Event Log 89
2.5.3. System > Logs > Persistent Log 90
2.5.4. System > Logs > Hosts 91
2.5.5. System > Logs > Configuration 92
2.5.6. System > Logs > Source Interface Configuration 93
2.5.7. System > Logs > Statistics 94
2.6. System > Statistics 96
2.6.1. System > Statistics > System 96
2.6.1.1. System > Statistics > System > Switch 96
2.6.1.2. System > Statistics > System > Port Summary 98
2.6.1.3. System > Statistics > System > Port Detailed 99
2.6.1.4. System > Statistics > System > Network DHCPv6 103
2.6.2. System > Statistics > Time Based 104
2.6.2.1. System > Statistics > Time Based > Group 104
2.6.2.2. System > Statistics > Time Based > Flow Based 105
2.6.2.3. System > Statistics > Time Based > Statistics 107
2.7. System > Status 108
2.7.1. System > Status > ARP Cache 108
2.7.2. System > Status > Resource Status 108
2.7.3. System > Status > Resource Configuration 109
2.8. System > Configuration Storage 110
2.8.1. System > Configuration Storage > Save 110
2.8.2. System > Configuration Storage > Reset 110
2.8.3. System > Configuration Storage > Erase Startup 110
2.8.4. System > Configuration Storage > Copy 111
2.9. System > Utilities 112
2.9.1. System > Utilities > System Reset 112
2.9.2. System > Utilities > Ping 112
2.9.3. System > Utilities > Ping IPv6 114
2.9.4. System > Utilities > TraceRoute 115
2.9.5. System > Utilities > TraceRoute IPv6 117
2.9.6. System > Utilities > IP Address Conflict 119
2.9.7. System > Utilities > Transfer 120
3. Switching 124
3.1. Switching > MAC Address Table 125
3.1.1. Switching > MAC Address Table > Configuration 125
3.1.2. Switching > MAC Address Table > MAC Address Table 125
3.2. Switching > Port 127
3.2.1. Switching > Port > Summary 127
3.2.2. Switching > Port > Description 129
3.2.3. Switching > Port > Cable Test 130
3.2.4. Switching > Port > Mirroring 131
3.3. Switching > Port Channel 134
3.3.1. Switching > Port Channel > Summary 134
3.3.2. Switching > Port Channel > Statistics 136
3.4. Switching > VLAN 138

3.4.1. Switching > VLAN > Status 138
3.4.2. Switching > VLAN > Port Configuration 139
3.4.3. Switching > VLAN > Port Summary 141
3.4.4. Switching > VLAN > Internal Usage 142
3.4.5. Switching > VLAN > Reset 143
3.4.6. Switching > VLAN > RSPAN 143
3.5. Switching > Private VLAN 144
3.5.1. Switching > Private VLAN > Configuration 144
3.5.2. Switching > Private VLAN > Association 145
3.5.3. Switching > Private VLAN > Interface 146
3.6. Switching > GARP 148
3.6.1. Switching > GARP > Switch 148
3.6.2. Switching > GARP > Port 149
3.7. Switching > Spanning Tree 151
3.7.1. Switching > Spanning Tree > Switch 151
3.7.2. Switching > Spanning Tree > MST 152
3.7.3. Switching > Spanning Tree > MST Port 153
3.7.4. Switching > Spanning Tree > CST 155
3.7.5. Switching > Spanning Tree > CST Port 157
3.7.6. Switching > Spanning Tree > Statistics 160
3.8. Switching > DHCP Snooping 161
3.8.1. Switching > DHCP Snooping > Base 161
3.8.1.1. Switching > DHCP Snooping > Base > Global 161
3.8.1.2. Switching > DHCP Snooping > Base > VLAN Configuration 161
3.8.1.3. Switching > DHCP Snooping > Base > Interface Configuration 162
3.8.1.4. Switching > DHCP Snooping > Base > Static Bindings 164
3.8.1.5. Switching > DHCP Snooping > Base > Dynamic Bindings 164
3.8.1.6. Switching > DHCP Snooping > Base > Persistent 165
3.8.1.7. Switching > DHCP Snooping > Base > Statistics 166
3.8.2. Switching > DHCP Snooping > L2 Relay 167
3.8.2.1. Switching > DHCP Snooping > L2 Relay > Global 167
3.8.2.2. Switching > DHCP Snooping > L2 Relay > Interface Configuration 167
3.8.2.3. Switching > DHCP Snooping > L2 Relay > VLAN Configuration 168
3.8.2.4. Switching > DHCP Snooping > L2 Relay > Statistics 169
3.9. Switching > IPv6 DHCP Snooping 170
3.9.1. Switching > IPv6 DHCP Snooping > Base 170
3.9.1.1. Switching > IPv6 DHCP Snooping > Base > Global 170
3.9.1.2. Switching > IPv6 DHCP Snooping > Base > VLAN Configuration 171
3.9.1.3. Switching > IPv6 DHCP Snooping > Base > Interface Configuration ... 172
3.9.1.4. Switching > IPv6 DHCP Snooping > Base > Static Bindings 173
3.9.1.5. Switching > IPv6 DHCP Snooping > Base > Dynamic Bindings 174
3.9.1.6. Switching > IPv6 DHCP Snooping > Base > Persistent 175
3.9.1.7. Switching > IPv6 DHCP Snooping > Base > Statistics 175
3.10. Switching > IGMP Snooping 177
3.10.1. Switching > IGMP Snooping > Configuration 177
3.10.2. Switching > IGMP Snooping > Interface Configuration 178
3.10.3. Switching > IGMP Snooping > VLAN Status 179
3.10.4. Switching > IGMP Snooping > Multicast Router Configuration 180
3.10.5. Switching > IGMP Snooping > Multicast Router VLAN Status 181
3.11. Switching > IGMP Snooping Querier 183
3.11.1. Switching > IGMP Snooping Querier > Configuration 183

3.11.2. Switching > IGMP Snooping Querier > VLAN Configuration 184
3.11.3. Switching > IGMP Snooping Querier > VLAN Status 185
3.12. Switching > MLD Snooping 187
3.12.1. Switching > MLD Snooping > Configuration 187
3.12.2. Switching > MLD Snooping > Interface Configuration 188
3.12.3. Switching > MLD Snooping > VLAN Status 189
3.12.4. Switching > MLD Snooping > Multicast Router Configuration 190
3.12.5. Switching > MLD Snooping > Multicast Router VLAN Status 191
3.12.6. Switching > MLD Snooping > Multicast Router VLAN Configuration 192
3.13. Switching > MLD Snooping Querier 193
3.13.1. Switching > MLD Snooping Querier > Configuration 193
3.13.2. Switching > MLD Snooping Querier > VLAN Configuration 194
3.13.3. Switching > MLD Snooping Querier > VLAN Status 195
3.14. Switching > Multicast Forwarding Database 196
3.14.1. Switching > Multicast Forwarding Database > Summary 196
3.14.2. Switching > Multicast Forwarding Database > GMRP 197
3.14.3. Switching > Multicast Forwarding Database > IGMP Snooping 198
3.14.4. Switching > Multicast Forwarding Database > MLD Snooping 199
3.14.5. Switching > Multicast Forwarding Database > Statistics 200
3.15. Switching > Voice VLAN 201
3.15.1. Switching > Voice VLAN > Configuration 201
3.15.2. Switching > Voice VLAN > Interface Summary 201
4. Routing 203
4.1. Routing > ARP Table 204
4.1.1. Routing > ARP Table > Summary 204
4.1.2. Routing > ARP Table > Configuration 205
4.1.3. Routing > ARP Table > Statistics 206
4.2. Routing > IP 207
4.2.1. Routing > IP > Configuration 207
4.2.2. Routing > IP > VLAN Interface Configuration 208
4.2.3. Routing > IP > Interface Summary 210
4.2.4. Routing > IP > Interface Configuration 212
4.2.5. Routing > IP > Loopback Configuration 214
4.2.6. Routing > IP > Statistics 215
4.3. Routing > Router 218
4.3.1. Routing > Router > Route Table 218
4.3.2. Routing > Router > Configured Routes 219
4.3.3. Routing > Router > Summary 220
5. Security 222
5.1. Security > AAA 223
5.1.1. Security > AAA > Authentication List 223
5.1.2. Security > AAA > Authentication Selection 225
5.1.3. Security > AAA > Authorization List 226
5.1.4. Security > AAA > Authorization Selection 228
5.1.5. Security > AAA > Accounting List 229
5.1.6. Security > AAA > Accounting Selection 231
5.2. Security > Users 232
5.2.1. Security > Users > Accounts 232
5.2.2. Security > Users > Auth Server Users 233
5.2.3. Security > Users > Sessions 234
5.3. Security > Passwords 235

5.3.1. Security > Passwords > Line Password 235
5.3.2. Security > Passwords > Enable Password 236
5.3.3. Security > Passwords > Password Rules 236
5.3.4. Security > Passwords > Last Password 238
5.3.5. Security > Passwords > Reset Passwords 238
5.4. Security > Management Access 240
5.4.1. Security > Management Access > System 240
5.4.2. Security > Management Access > Telnet 241
5.4.3. Security > Management Access > Outbound Telnet 242
5.4.4. Security > Management Access > Serial 243
5.4.5. Security > Management Access > CLI Banner 243
5.4.6. Security > Management Access > HTTP 244
5.4.7. Security > Management Access > HTTPS 245
5.4.8. Security > Management Access > SSH 247
5.5. Security > Filters 249
5.5.1. Security > Filters > MAC Filters 249
5.6. Security > Protected Ports 251
5.6.1. Security > Protected Ports > Configuration 251
5.7. Security > Port Security 252
5.7.1. Security > Port Security > Global 252
5.7.2. Security > Port Security > Interface 253
5.7.3. Security > Port Security > Static MAC 254
5.7.4. Security > Port Security > Dynamic MAC 255
5.8. Security > Port Access Control 257
5.8.1. Security > Port Access Control > Configuration 257
5.8.2. Security > Port Access Control > Port Summary 258
5.8.3. Security > Port Access Control > Port Configuration 261
5.8.4. Security > Port Access Control > Port Details 264
5.8.5. Security > Port Access Control > Statistics 267
5.8.6. Security > Port Access Control > Client Summary 270
5.8.7. Security > Port Access Control > Privileges Summary 271
5.8.8. Security > Port Access Control > History Log Summary 272
5.9. Security > RADIUS 273
5.9.1. Security > RADIUS > Configuration 273
5.9.2. Security > RADIUS > Named Server 274
5.9.3. Security > RADIUS > Statistics 275
5.9.4. Security > RADIUS > Accounting Server 276
5.9.5. Security > RADIUS > Accounting Statistics 278
5.9.6. Security > RADIUS > Clear Statistics 279
5.9.7. Security > RADIUS > Source Interface Configuration 279
5.10. Security > TACACS+ 281
5.10.1. Security > TACACS+ > Configuration 281
5.10.2. Security > TACACS+ > Server Summary 281
5.10.3. Security > TACACS+ > Server Configuration 282
5.10.4. Security > TACACS+ > Source Interface Configuration 283
5.11. Security > Access Control Lists 284
5.11.1. Security > Access Control Lists > Summary 284
5.11.2. Security > Access Control Lists > Configuration 285
5.11.3. Security > Access Control Lists > Interfaces 292
5.11.4. Security > Access Control Lists > VLANs 293
6. Quality of Service 295

6.1. QoS > Auto VoIP 296
6.1.1. QoS > Auto VoIP > Global 296
6.1.2. QoS > Auto VoIP > OUI Table 296
6.1.3. QoS > Auto VoIP > OUI Based Auto VoIP 297
6.1.4. QoS > Auto VoIP > Protocol Based Auto VoIP 298
6.2. QoS > Class of Service 301
6.2.1. QoS > Class of Service > 802.1p 301
6.2.2. QoS > Class of Service > IP DSCP 302
6.2.3. QoS > Class of Service > Interface 302
6.2.4. QoS > Class of Service > Queue 303
6.3. QoS > Diffserv 305
6.3.1. QoS > Diffserv > Global 305
6.3.2. QoS > Diffserv > Class Summary 306
6.3.3. QoS > Diffserv > Class Configuration 307
6.3.4. QoS > Diffserv > Policy Summary 311
6.3.5. QoS > Diffserv > Policy Configuration 312
6.3.6. QoS > Diffserv > Service Summary 316
6.3.7. QoS > Diffserv > Policy Statistics 317
7. Stacking commands 318
7.1. Stacking > Base 319
7.1.1. Stacking > Base > Summary 319
7.1.2. Stacking > Base > Unit Configuration 321
7.1.3. Stacking > Base > Supported Switches 323
7.1.4. Stacking > Base > Firmware Update 324
7.1.5. Stacking > Base > Firmware Synchronization 325
7.1.6. Stacking > Base > Port Configuration 326
7.1.7. Stacking > Base > Statistics 327
7.1.8. Stacking > Base > Diagnostics 328

List of Figures

1.1. System login window 6
2.1. System Dashboard 8
2.2. System Description 10
2.3. System Inventory 11

List of Tables

2.1. System information 8
2.2. Device information 8
2.3. System Resource Usage 9
2.4. Logged In Users 9
2.5. Temperature Sensors 9
2.6. Fan 9
2.7. Messages Received 22
2.8. Messages Sent 22
2.9. Auto DOS 38
2.10. TCP Settings 39
2.11. ICMP Settings 39
2.12. Buffered Log Configuration 92
2.13. Command Logger Configuration 92
2.14. Console Log Configuration 92
2.15. Persistent Log Configuration 93
2.16. Syslog Configuration 93
2.17. Buffered Log 94
2.18. Persistent Log 95
2.19. Syslog 95
5.1. HTTP 240
5.2. Telnet 240
5.3. Outbound Telnet 240
5.4. Secure HTTP 241
5.5. Secure Shell 241

Chapter 1. Getting Started

This chapter introduces the management interface of Netberg Aurora 100 Switch Series.

1.1. Management Options

The Netberg Aurora 100 Switch Series can be managed through any port on the device by using the Web-based Management. Each switch must be assigned its own IP Address, which is used for communication with Web-Based Management. The PC's IP address should be in the same range as the switch. Each switch can allow only one user to access the Web-Based Management at a time. The PC should have an IP address in the same range as the switch. Each switch can allow one user to access to the Web-Based Management at a time.

1.2. Using Web-based Management

After a successful physical installation, you can configure the Switch, monitor the network status, and display statistics using a web browser.

1.3. Supported Web Browsers

The embedded Web-based Management currently supports all modern web browsers.

1.4. Connecting to the Switch

You will need the following equipment to begin the web configuration of your device:

1. A PC with a RJ-45 Ethernet connection
2. A standard Ethernet cable

Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.

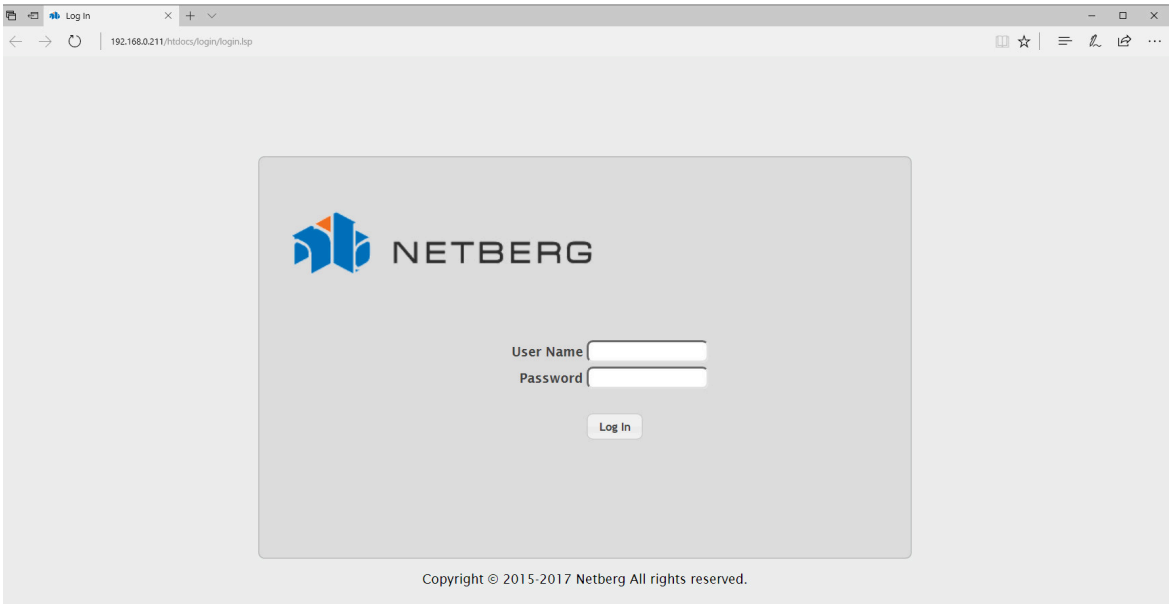
1.5. Login Web-based Management

In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of 192.168.1.1, the PC should have an IP address of 192.168.1.z (where z is a number between 2 ~ 254), and a subnet mask of 255.255.255.0. You can open the web browser and enter 192.168.1.1 (the factory-default IP address) in the address bar. Then press <Enter>.

The default IP address is 192.168.0.1.

The default user name is "admin", and the password is empty.

Figure 1.1. System login window



Chapter 2. System

2.1. Summary

2.1.1. System > Summary > Dashboard

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

Figure 2.1. System Dashboard

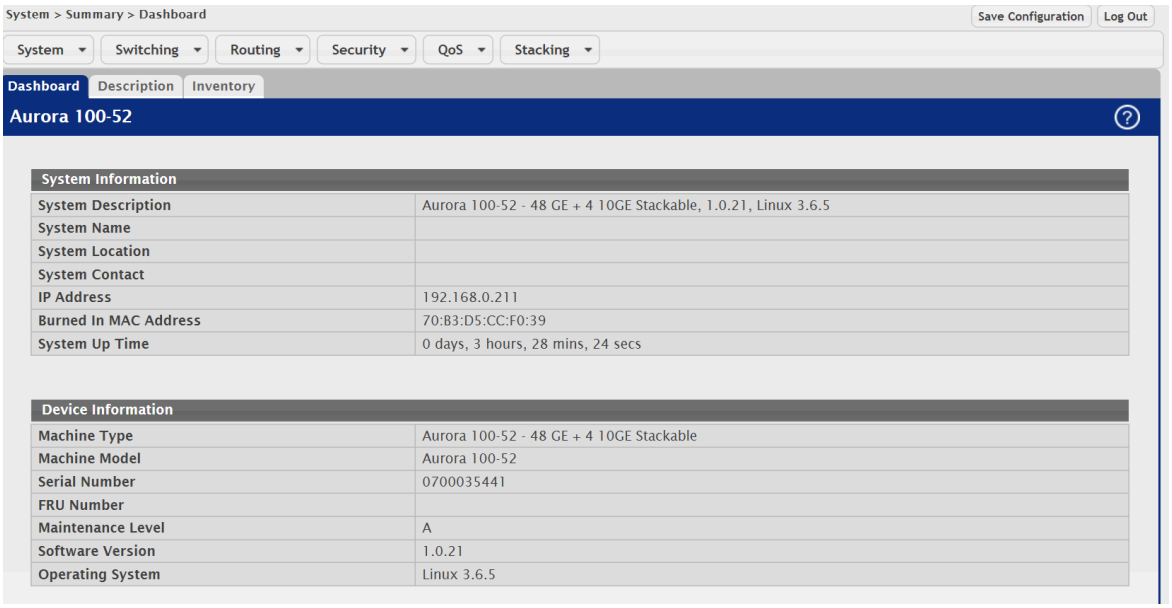


Table 2.1. System information

System Description	The product name of this device.
System Name	The configured name used to identify this device.
System Location	The configured location of this device.
System Contact	The configured contact person for this device.
IP Address	The IP address assigned to the network interface. The network interface is the logical interface that allows remote management of the device via any of the front-panel switch ports.
Burned In MAC Address	The device burned-in universally-administered media access control (MAC) address of the base system.
System Up Time	The time in days, hours, minutes and seconds since the system was last reset.

Table 2.2. Device information

Machine Type	The device hardware type or product family.
Machine Model	The model identifier, which is usually related to the Machine Type.
Serial Number	The unique device serial number.
FRU Number	The field replaceable unit number.

Maintenance Level	The device hardware change level identifier.
Software Version	The release.version.maintenance number of the software currently running on the device. For example, if the release is 1, the version is 2, and the maintenance number is 4, this version number is displayed as 1.2.4.
Operating System	The device operating system type and version identification information.

Table 2.3. System Resource Usage

CPU Utilization (60 Second Average)	The percentage of CPU utilization for the entire system averaged over the past 60 seconds.
Memory Usage	The percentage of total available system memory (RAM) that is currently in use.

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.

Table 2.4. Logged In Users

User Name	The names of connected users.
Connection From	Connection address and source.
Idle Time	Time since the last action.

A brief list of different system temperature sensors.

Table 2.5. Temperature Sensors

Unit	The unit number in the stack.
Sensor	The temperature sensor for the given unit.
Description	The description of the temperature sensor.
Temp©	The temperature of the specified unit.
State	The unit temperature state.
Max. Temp	The maximum temperature of CPU and MACs.

A brief list of the fans status in all units. These fans remove the heat generated by the power, CPU and other chipsets, make chipsets work normally.

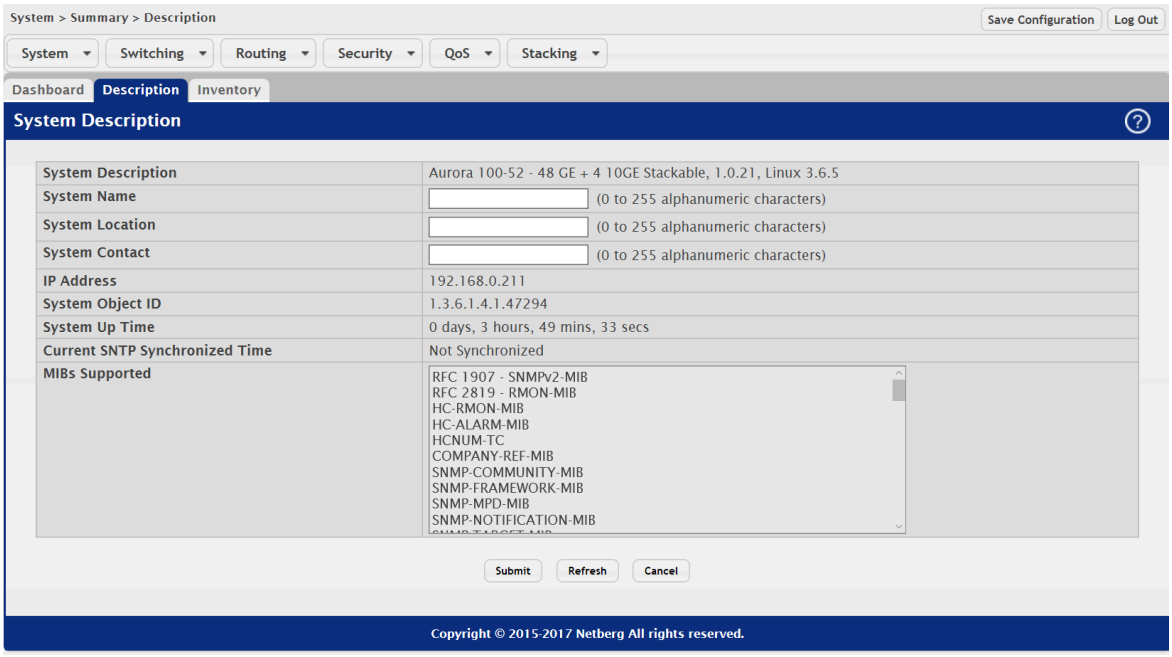
Table 2.6. Fan

Unit	The unit number in the stack.
Fan	The fan index used to identify fan for the given stack member.
Description	The description of the fans.
Type	Specifies whether the fan module is fixed or removable.
Speed	The fan speed.
Duty level	The duty level of the fan.
State	Specifies whether the fan is running or stopped.

2.1.2. System > Summary > 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.

Figure 2.2. System Description



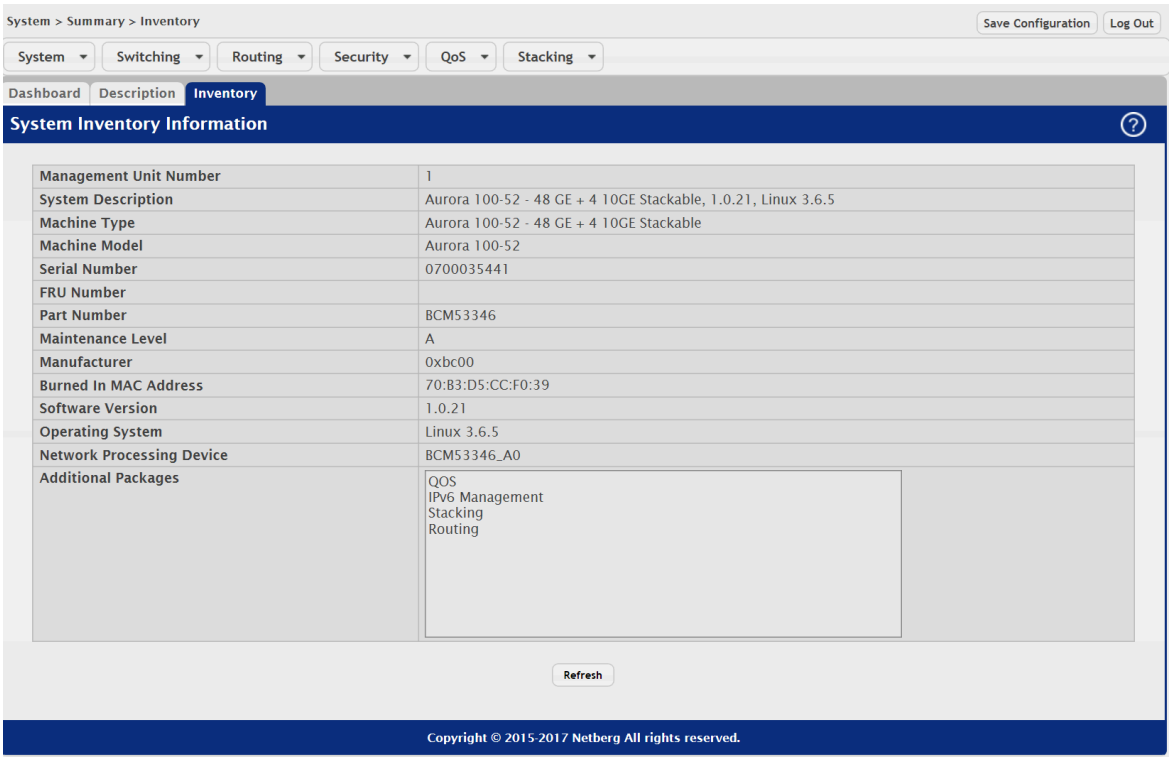
System Description	The product name of this device.
System Name	The name used to identify this device. The factory default is blank.
System Location	The location of this device. The factory default is blank.
System Contact	The contact person for this device. The factory default is blank.
IP Address	The 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.
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 Time	Displays the currently synchronized SNTP time in UTC. If the time is not synchronized with an SNTP server, it displays "Not Synchronized."
MIBs Supported	The list of MIBs supported by the SNMP agent running on this device.

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

2.1.3. System > Summary > Inventory

This page displays information about the system hardware and software.

Figure 2.3. System Inventory



Management Unit Number	The number assigned to the stack management unit.
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.

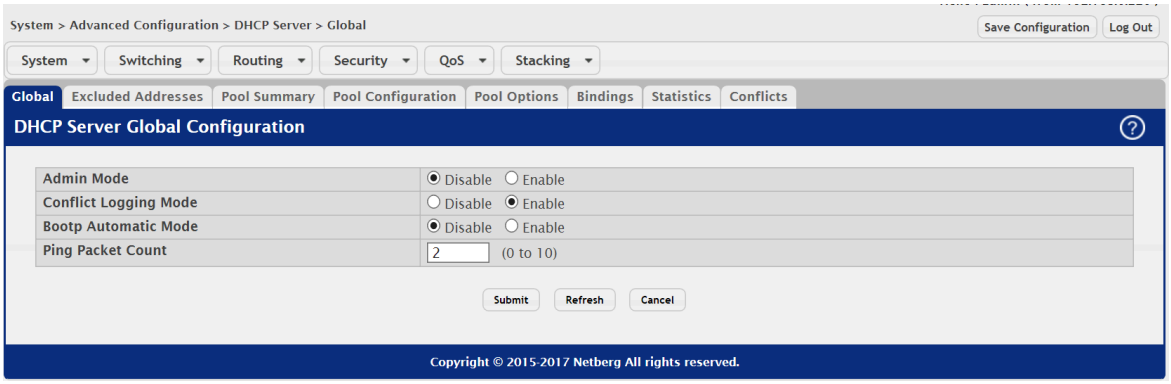
Network Processing Device	Identifies the network processor hardware.
Additional Packages	A list of the optional software packages installed on the device, if any. For example, QoS.

2.2. System > Advanced Configuration

2.2.1. System > Advanced Configuration > DHCP Server

2.2.1.1. System > Advanced Configuration > DHCP Server > Global

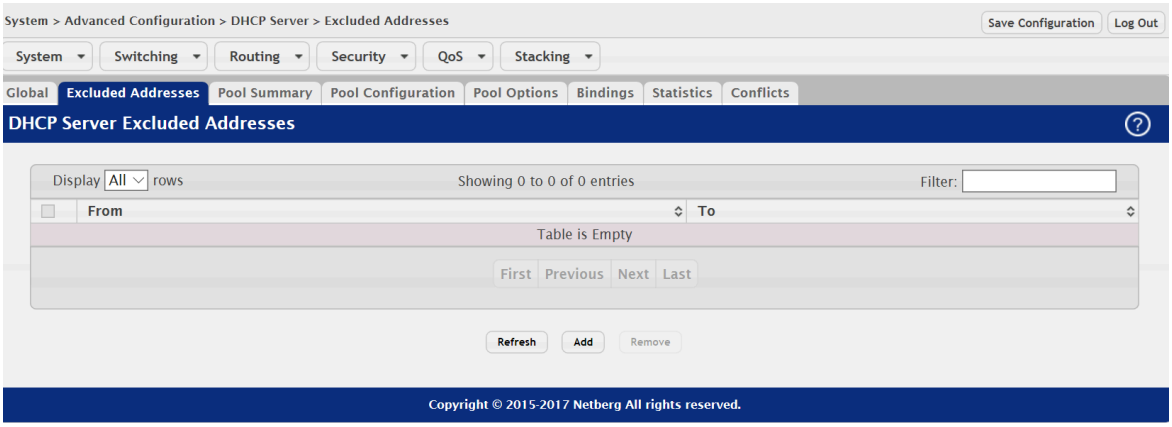
Use this page to configure the global Dynamic Host Configuration Protocol (DHCP) server settings for the device. The device includes a DHCP server that can be configured to communicate with DHCP clients on the network and provide network information such as IP addresses, default gateways, and other network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



Admin Mode	Enables or disables the DHCP server administrative mode. When enabled, the device can be configured to automatically allocate TCP/IP configurations for clients.
Conflict Logging Mode	Enables or disables the logging mode for IP address conflicts. When enabled, the system stores information IP address conflicts that are detected by the DHCP server.
Bootp Automatic Mode	Enables or disables the BOOTP automatic mode. When enabled, the DHCP server supports the allocation of automatic addresses for BOOTP clients. When disabled the DHCP server supports only static addresses for BOOTP clients.
Ping Packet Count	The number of packets the server sends to a pool address to check for duplication as part of a ping operation. If the server receives a response to the ping, the address is considered to be in conflict and is removed from the pool.

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

2.2.1.2. System > Advanced Configuration > DHCP Server > Excluded Addresses



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

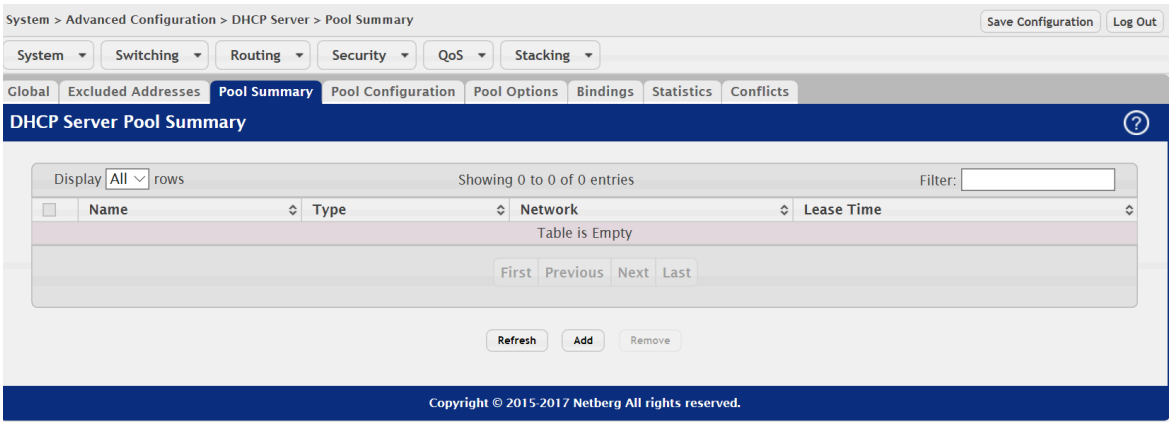
Use the buttons to perform the following tasks:

- 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.

From	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.

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

2.2.1.3. System > Advanced Configuration > DHCP Server > Pool Summary



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.

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.

When you click Add, the Add DHCP Server Pool modal page opens and allows you to configure the following DHCP pool settings:

Name	The name that identifies the DHCP server pool.
Type of Binding	The type of binding for the pool. The options are: • Manual • Dynamic

	The binding type you select determines the fields that are available to configure.
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 (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 Expiration Mode	Indicates whether the information the server provides to the client should expire. • Enable – Allows the lease to expire. If you select this option, you can specify the amount of time the lease is valid in the Lease Duration field. • Disable – Sets an infinite lease time. For Dynamic bindings, an infinite lease time implies a lease period of 60 days. For a Manual binding, an infinite lease period never expires.
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.
Default 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.

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

2.2.1.4. System > Advanced Configuration > DHCP Server > Pool 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.

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.

When you click Add, the Add DHCP Server Pool modal page opens and allows you to configure the following DHCP pool settings:

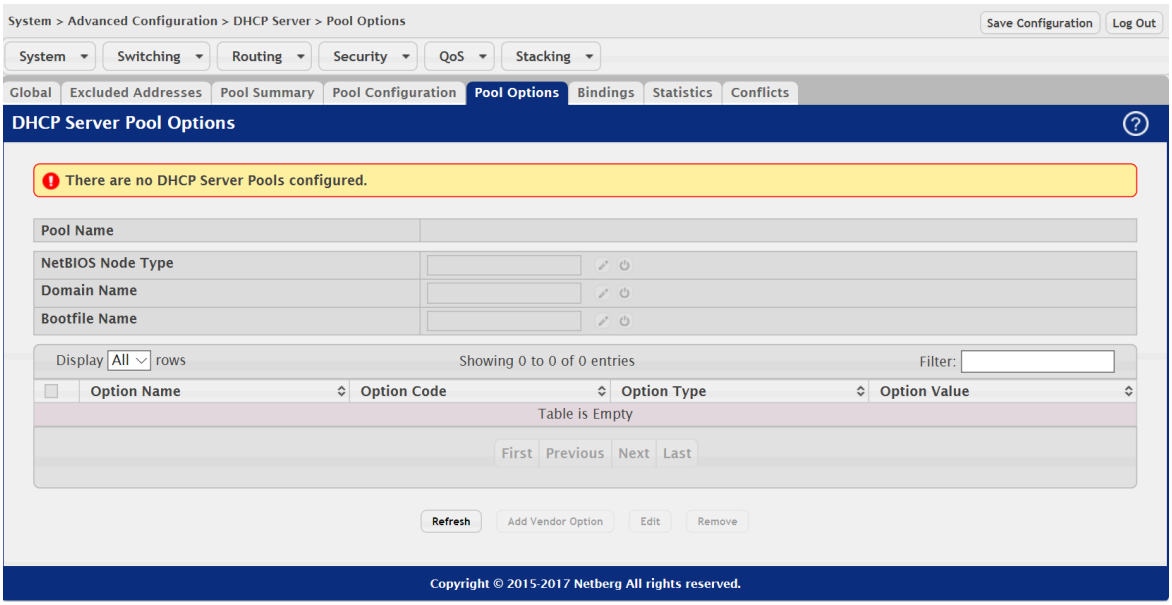
Name	The name that identifies the DHCP server pool.
Type of Binding	The type of binding for the pool. The options are: • Manual

	• Dynamic The binding type you select determines the fields that are available to configure.
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 (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 Expiration Mode	Indicates whether the information the server provides to the client should expire. • Enable – Allows the lease to expire. If you select this option, you can specify the amount of time the lease is valid in the Lease Duration field. • Disable – Sets an infinite lease time. For Dynamic bindings, an infinite lease time implies a lease period of 60 days. For a Manual binding, an infinite lease period never expires.
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.
Default 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.

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

2.2.1.5. System > Advanced Configuration > DHCP Server > Pool 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.

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.

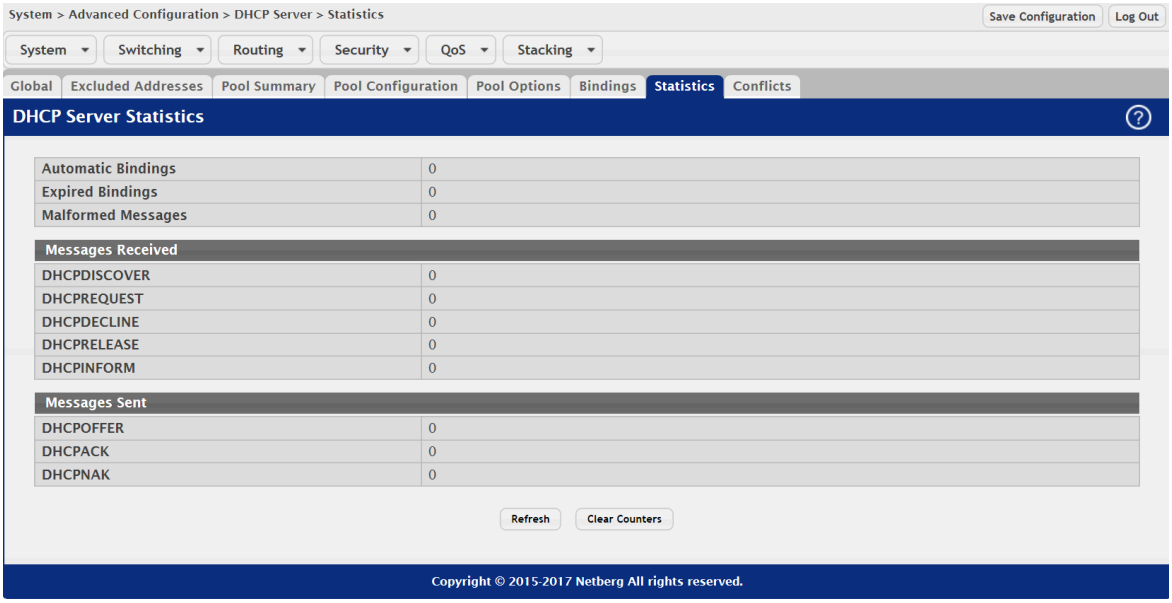
Applied changes update the device running configuration. If you want the device to retain these changes across a reset, you must first save the configuration.

2.2.1.6. System > Advanced Configuration > DHCP Server > 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.

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.

2.2.1.7. System > Advanced Configuration > DHCP Server > 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.

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.

This table shows statistical information about the messages received from DHCP clients on the network.

Table 2.7. Messages Received

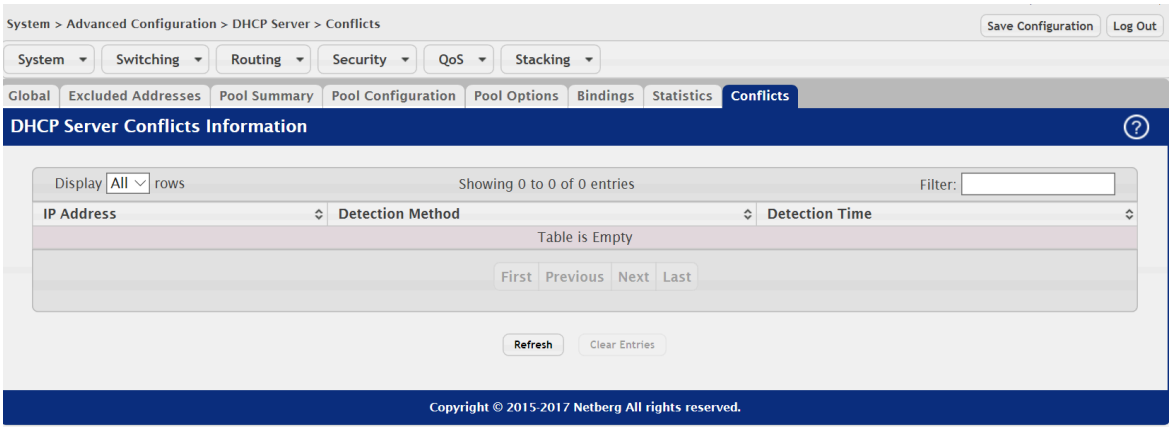
DHCPDISCOVER	The number of DHCP discovery messages the DHCP server has received. A DHCP client broadcasts this type of message to discover available DHCP servers.
DHCPREQUEST	The number of DHCP request messages the DHCP server has received. A DHCP client broadcasts this type of message in response to 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.

This table shows statistical information about messages the DHCP server has sent to DHCP clients on the network.

Table 2.8. 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.

2.2.1.8. System > Advanced Configuration > DHCP Server > Conflicts



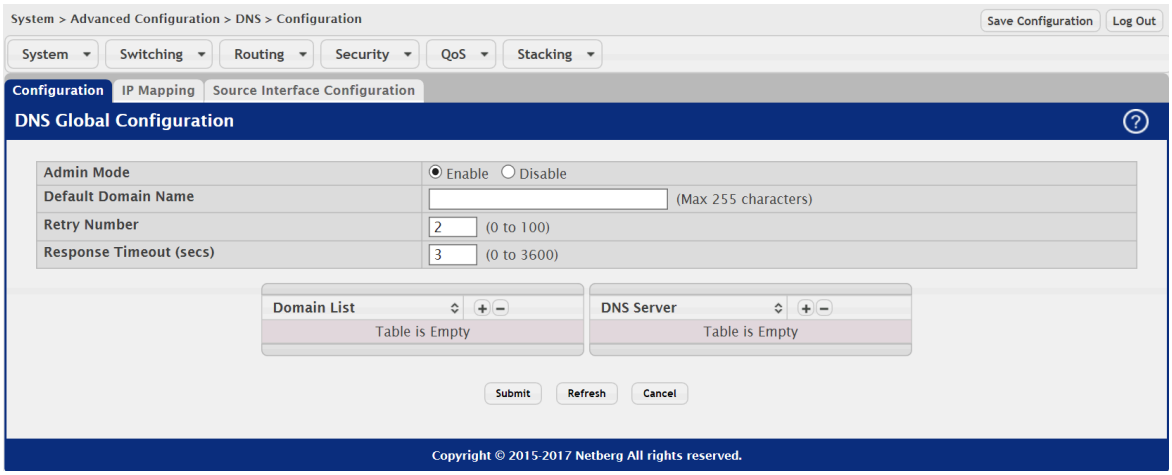
This page displays information about IP address conflicts detected during the DHCP message exchange process between the server and client. An address conflict occurs when two hosts on the same network use the same IP address. Any address detected as a duplicate is removed from the pool and will not be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

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.

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

2.2.2. System > Advanced Configuration > DNS

2.2.2.1. System > Advanced Configuration > DNS > 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:

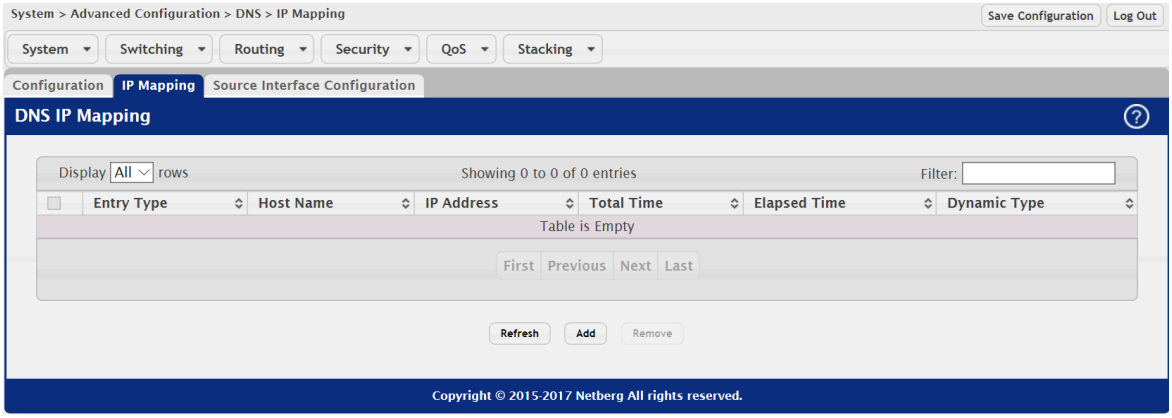
- To add an entry to the Domain List or list of DNS servers, click the + (plus) button and enter the desired information.
- To edit the IPv4 or IPv6 address of a configured DNS server, click the Edit icon associated with the entry to edit and update the desired information.
- To delete an entry from 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.

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.

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

2.2.2.2. System > Advanced Configuration > DNS > 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:

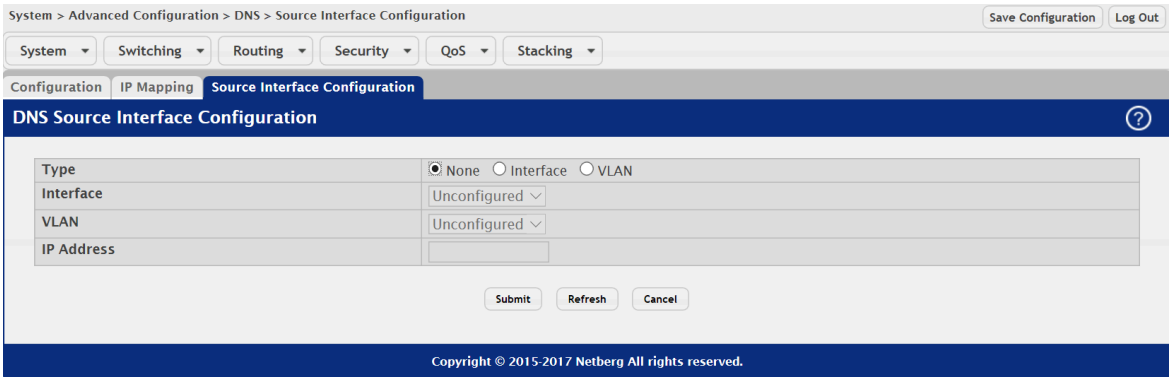
- To statically map an IP address to a hostname, click Add and configure the fields available in the Add DNS Entry dialog box.
- To delete one or more entries, select each entry to delete and click Remove.

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, th	

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.

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

2.2.2.3. System > Advanced Configuration > DNS > Source Interface Configuration



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

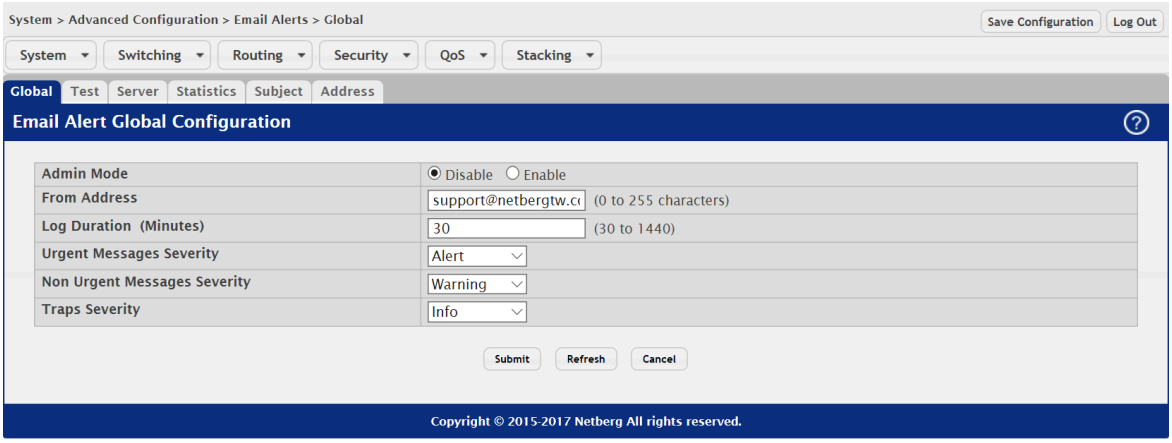
Type	The type of interface to use as the source interface: • None – The primary IP address of the originating (outbound) interface is used as the source address. • Interface – The primary IP address of a physical port is used as the source address. • VLAN – The primary IP address of a VLAN routing interface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

IP Address	The IP address associated with the configured Source Interface.

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

2.2.3. System > Advanced Configuration > Email Alerts

2.2.3.1. System > Advanced Configuration > Email Alerts > Global



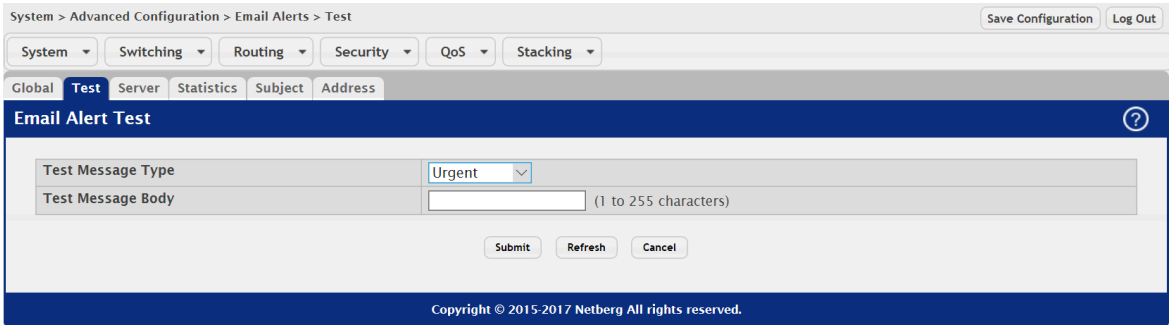
Use this page to configure system-wide settings for the Email Alert feature, which allows the device to send log messages to one or more email addresses. You must configure information about the network Simple Mail Transport Protocol (SMTP) server for email to be successfully sent from the device.

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.
Email Alert	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.

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

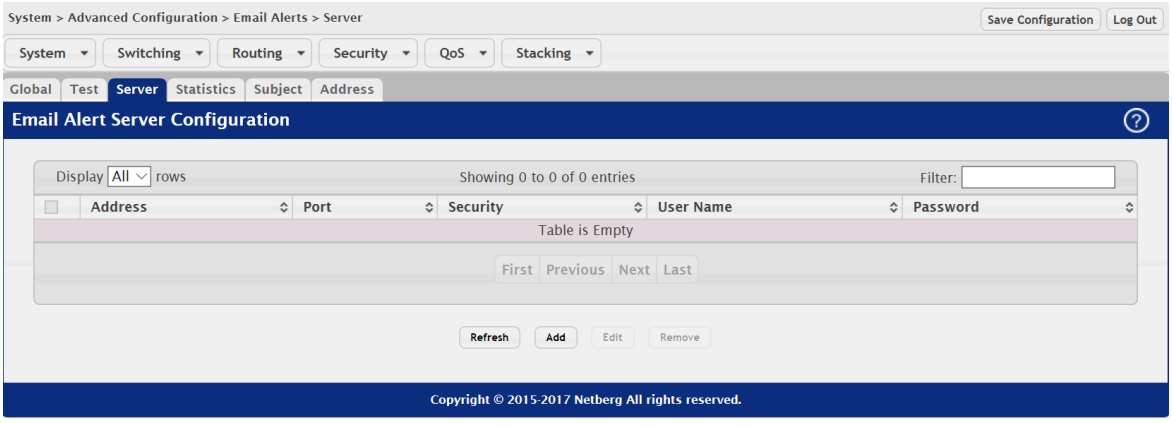
2.2.3.2. System > Advanced Configuration > Email Alerts > Test



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.

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.

2.2.3.3. System > Advanced Configuration > Email Alerts > Server



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

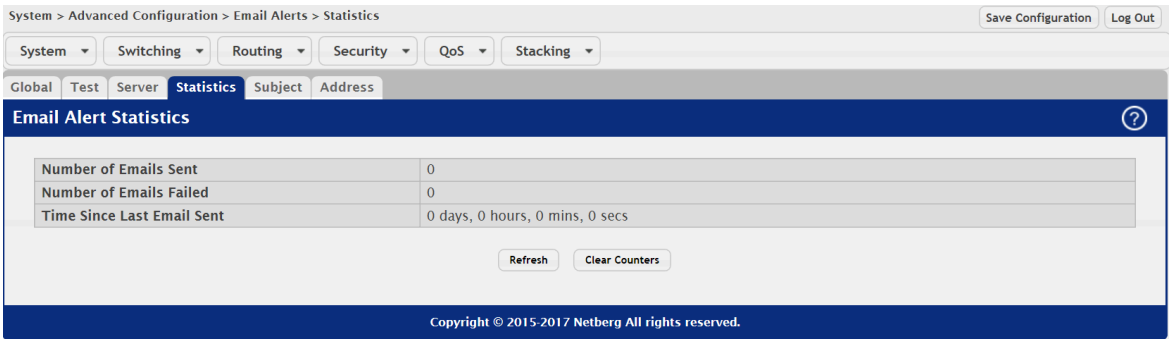
Use the buttons to perform the following tasks:

- 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.

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.

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

2.2.3.4. System > Advanced Configuration > Email Alerts > Statistics

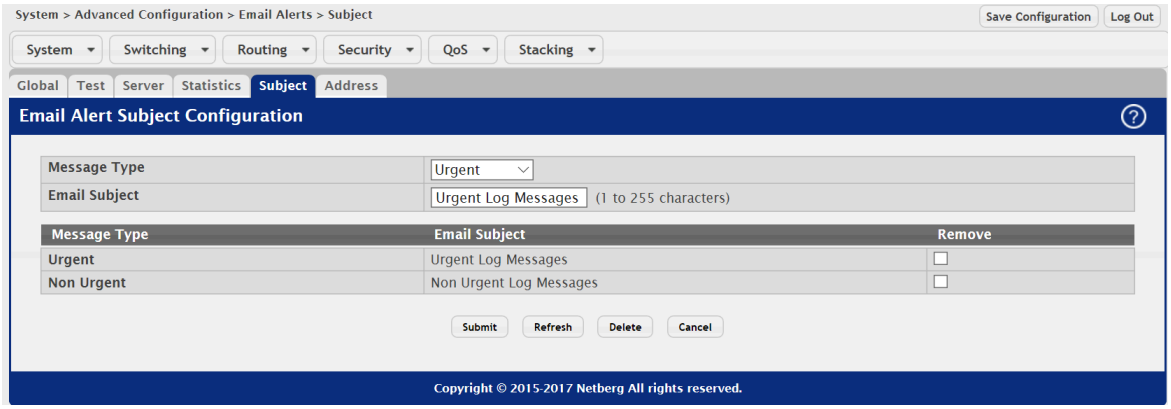


Use this page to view information about the email alerts the device has sent or attempted to send. The statistics are cleared when the system is reset.

Number of Emails Sent	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.

2.2.3.5. System > Advanced Configuration > Email Alerts > Subject

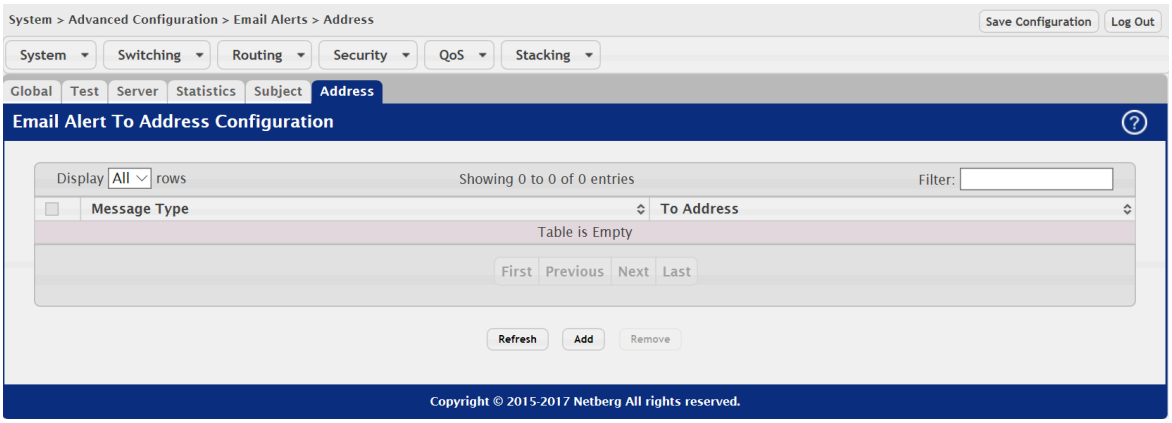


Use this page to view and edit the subject line of the urgent and non urgent email alert messages sent from the device.

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.

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

2.2.3.6. System > Advanced Configuration > Email Alerts > Address



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

Use the buttons to perform the following tasks:

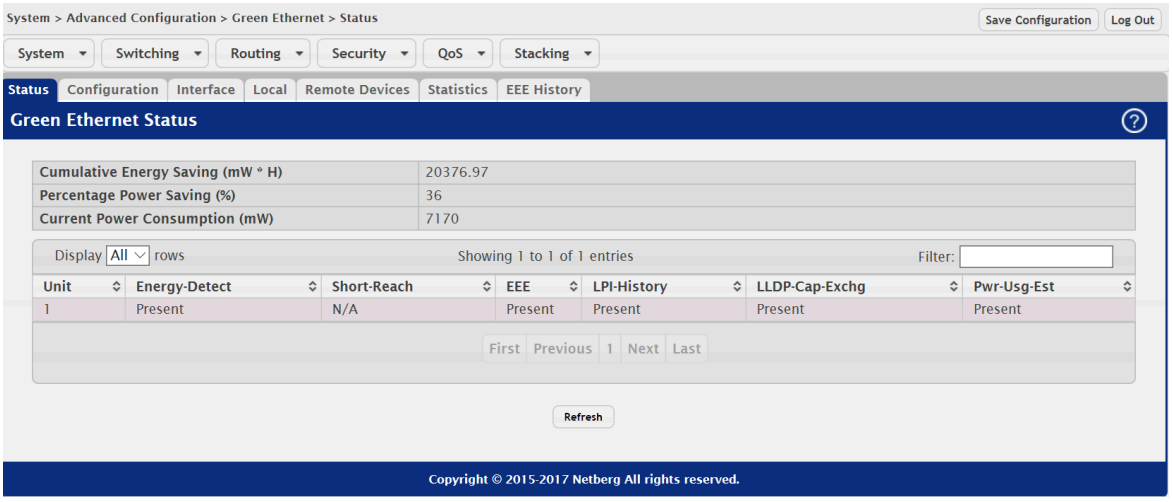
- To add an email address to the list of email alert message recipients, click Add and configure the desired settings.
- To delete an entry from the list, select the check box associated with each entry to delete and click Remove.

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.

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

2.2.4. System > Advanced Configuration > Green Ethernet

2.2.4.1. System > Advanced Configuration > Green Ethernet > Status



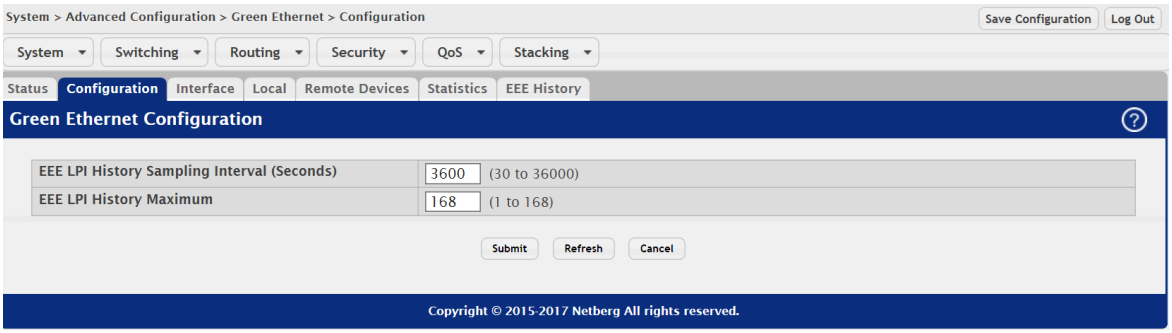
Use this page to view status information about the Green Ethernet feature on the device. The Green Ethernet feature is designed to reduce per-port power usage.

Cumulative Energy Saving (mW * H)	The estimated cumulative energy saved on the device in (milliWatts x Hours) due to the Green Ethernet feature.
Percentage Power Saving (%)	The estimated percentage of power saved on all ports due to the Green Ethernet feature. For example, 10% means that the device required 10%

	less power than it would have required if the Green Ethernet feature were not present.
Current Power Consumption (mW)	The estimated power consumption by all ports.

Unit	The device Unit ID.
Energy-Detect	Indicates whether Energy Detect mode is present on the device. When the Energy Detect mode is enabled and a port link is down, the PHY automatically goes down for a short period of time and then wakes up to check link pulses. This mode reduces power consumption on the port when no link partner is present.
Short-Reach	Indicates whether the Short-Reach cable mode is present on the device. When present and enabled, short-reach cable mode performs a cable test when the port link is up. If the cable that connects the port to its link partner has a length less than 10m, PHYs are placed in low-power mode (nominal power).
EEE	Indicates whether Energy Efficient Ethernet (EEE) is present on the device. EEE enables ports to enter a low-power mode to reduce power consumption during periods of low link utilization. EEE is defined by IEEE 802.3az. EEE enables both the send and receive sides of the link to disable some functionality for power savings when the link is lightly loaded.
LPI-History	Indicates whether the device is able to provide historical data about the amount of time the device has spent in low-power idle (LPI) mode.
LLDP-Cap-Exchg	Indicates whether the device is able to exchange information about its power capabilities with link partners by transmitting information in Link Layer Discovery Protocol (LLDP) data units.
Pwr-Usg-Est	Indicates whether the device is able to provide estimates of the device's power consumption.

2.2.4.2. System > Advanced Configuration > Green Ethernet > Configuration

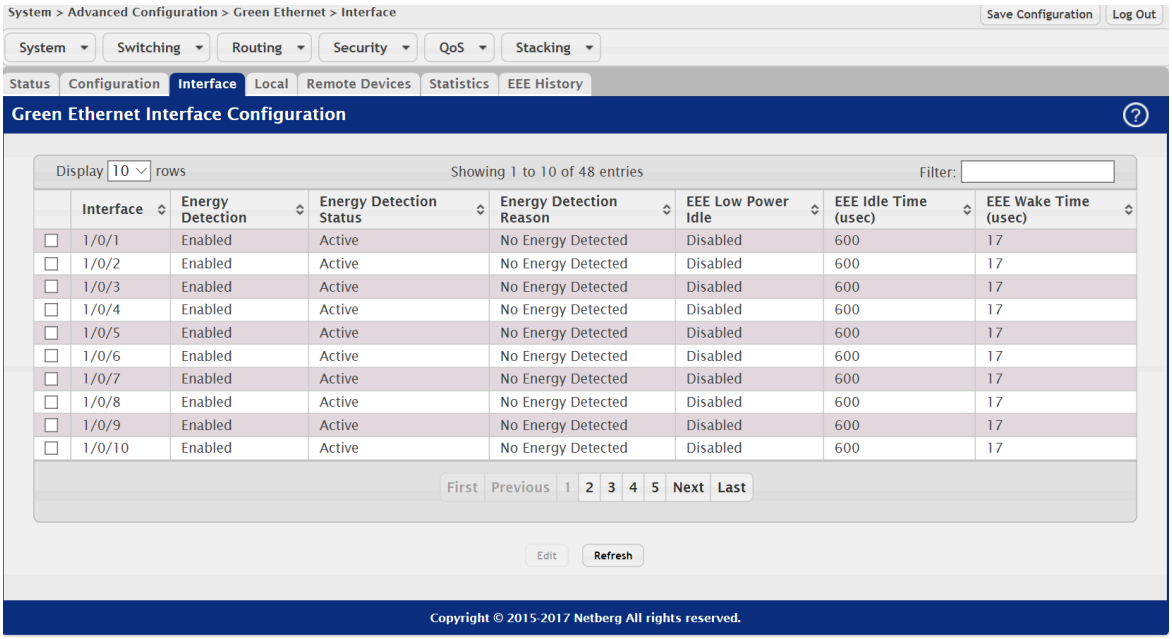


Use this page to configure the global settings for the Energy Efficient Ethernet (EEE) settings on the device.

EEE LPI History Sampling Interval	The amount of time to wait between collecting Low-Power Idle (LPI) samples on the device.
EEE LPI History Maximum	The number of LPI samples to store in the buffer.

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

2.2.4.3. System > Advanced Configuration > Green Ethernet > Interface



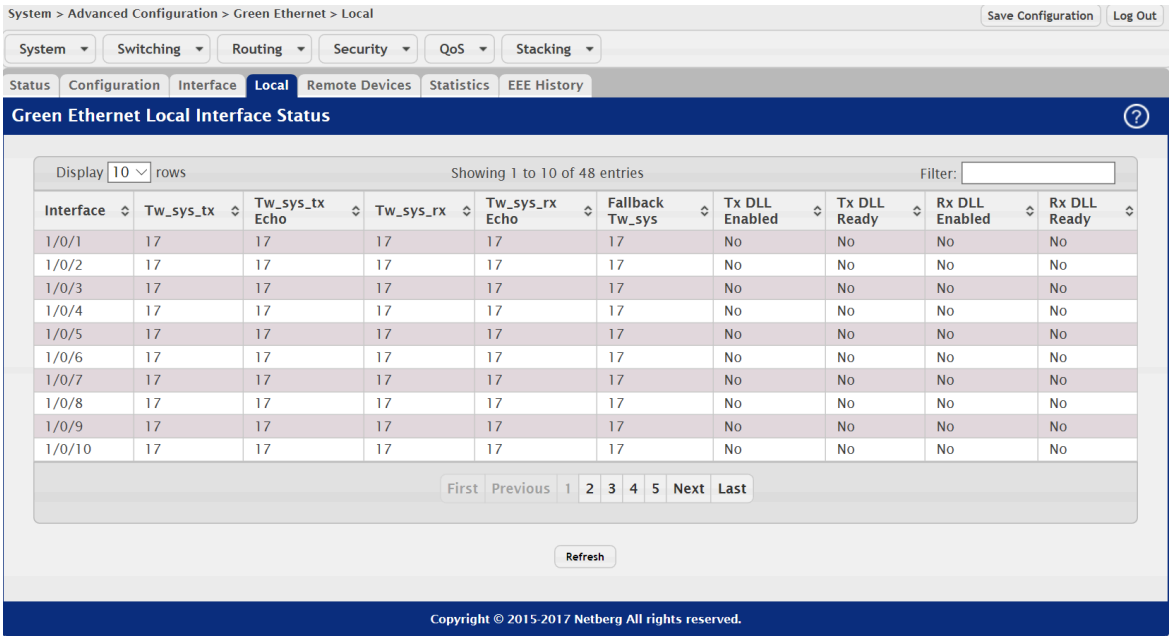
Use this page to configure per-port Green Ethernet settings. Only interfaces that are capable of supporting Green Ethernet modes appear in the table. To configure the settings for one or more interfaces, select each interface to configure and click **Edit**. The same settings are applied to all selected interfaces.

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 the interface(s) being configured.
Energy Detection	The administrative status of Energy Detect mode on the interface. When the Energy Detect mode is enabled and a port link is down, the PHY automatically goes down for short period of time and then wakes up to check link pulses. This mode reduces power consumption on the port when no link partner is present.
Energy Detection Status	The current operational state of Energy Detect mode, which is either Active or Inactive.

Energy Detection Reason	The current reason of Energy Detect mode, which is "Admin Down", "Link Up" or "No Energy Detected".
EEE Low Power Idle	The administrative mode of Low-Power Idle (LPI) on the interface. LPI can reduce power consumption on the interface during periods where no traffic is present on the interface. Enabling this mode does not affect link status and should not cause traffic loss. Note that LPI mode is available only if the interface Physical Mode is Auto Negotiate.
EEE Idle Time (usec)	The amount of time in micro seconds allowed for the interface to move to an LPI state.
EEE Wake Time (usec)	The system wake time in micro seconds that the interface transmits when it is enabled for EEE. The wake time is the amount of time allowed to wake up from the low-power state that occurs when no data is transmitted .

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

2.2.4.4. System > Advanced Configuration > Green Ethernet > Local

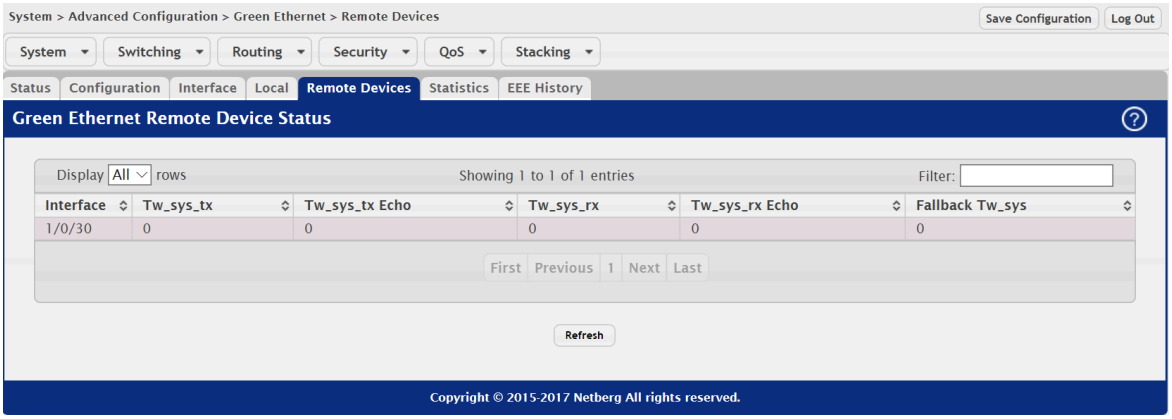


Use this page to view the information that each Energy Efficient Ethernet (EEE)-enabled interface transmits in the Link Layer Discovery Protocol (LLDP) Type-Length-Values (TVLs) to its link partner (the remote system). The TVLs are defined in the IEEE 802.1AB standard and provide information about the capabilities of the local device.

Interface	The interface associated with the rest of the data in the row. The table displays all interfaces that are enabled for EEE.

Tw_sys_tx	The system wake time (Tw_sys) that the interface transmits. The wake time is the amount of time allowed to wake up from the low-power state that occurs when no data is transmitted.
Tw_sys_tx Echo	The system wake time the interface sends to the link partner when it receives a Tw_sys_tx request from the link partner.
Tw_sys_rx	The system wake time that the local interface requests from the remote link partner.
Tw_sys_rx Echo	The remote system's receive Tw_sys that was used by the local system to compute the Tw_sys that it can support.
Fallback Tw_sys	The value of fallback Tw_sys that the local system requests from the remote system. The fallback is the second preference of the receiving system when requesting the Tw_sys from its transmitting partner.
Tx DLL Enabled	The initialization status of the EEE transmit Data Link Layer (DLL) management function on the local system.
Tx DLL Ready	The DLL ready transmission status of the interface. This field indicates whether the transmission system initialization is complete and is ready to update/transmit LLDP Data Units (LLDPDUs) containing the EEE TLVs.
Rx DLL Enabled	The status of the EEE capability negotiation on the local interface.
Rx DLL Ready	The DLL ready receive status of the interface. This field indicates whether the local interface initialization is complete and is ready to update/receive LLDPDUs containing EEE TLVs.

2.2.4.5. System > Advanced Configuration > Green Ethernet > Remote Devices

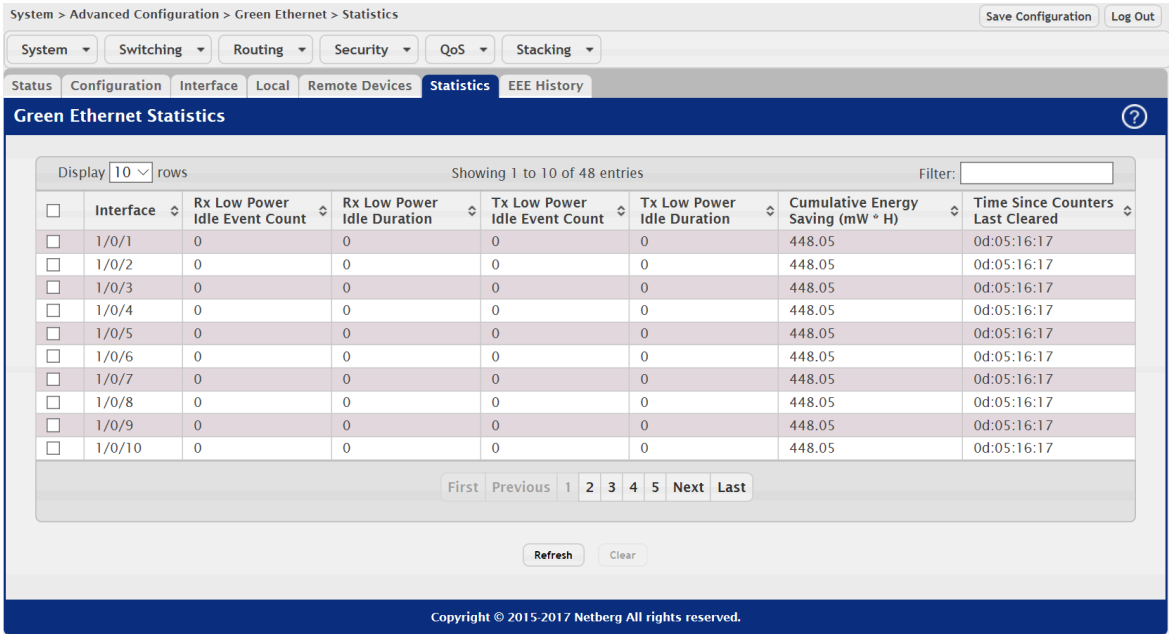


Use this page to view the information that an Energy Efficient Ethernet (EEE)-enabled interface receives in the Link Layer Discovery Protocol (LLDP) Type-Length-Values (TVLs) from its link partner (the remote system). The TVLs are defined in the IEEE 802.1AB standard and provide information about the capabilities of the remote device.

Interface	The interface associated with the rest of the data in the row. The table displays all interfaces that are enabled for EEE and have received EEE TVLs from a link partner.

Tw_sys_tx	The system wake time (Tw_sys) the interface received from its link partner.
Tw_sys_tx Echo	The system wake time the remote system sends to the local interface when it receives a Tw_sys_tx request from the local interface.
Tw_sys_rx	The of system wake time that the remote link partner requests from the local interface.
Tw_sys_rx Echo	The local system's receive Tw_sys used by the remote system to compute the Tw_sys that it can support.
Fallback Tw_sys	The value of fallback Tw_sys that the remote system requests from the local system. The fallback is the second preference of the receiving system when requesting the Tw_Sys from its transmitting partner.

2.2.4.6. System > Advanced Configuration > Green Ethernet > Statistics



This page displays per-port statistics about the number of times and the amount of time the local and remote interfaces have spent in a low-power idle mode.

Interface	The interface associated with the rest of the data in the row. The table includes all interfaces that are enabled for EEE.
Rx Low Power Idle Event Count	The number of times the local interface has entered a low-power idle state.
Rx Low Power Idle Duration	The amount of time (in 10 microsecond increments) the local interface has spent in a low-power idle state.
Tx Low Power Idle Event Count	The number of times the link partner has entered a low-power idle state.

Tx Low Power Idle Duration	The amount of time (in 10 microsecond increments) the link partner has spent in a low-power idle state.
Cumulative Energy Saving (mW * H)	The estimated cumulative energy saved of the interface in (milliWatts x Hours) due to the Green Ethernet feature.
Time Since Counters Last Cleared	The amount of time since the statistics on this page were reset to zero.
Clear (Button)	Resets all Green Ethernet statistics counters on this page to 0.

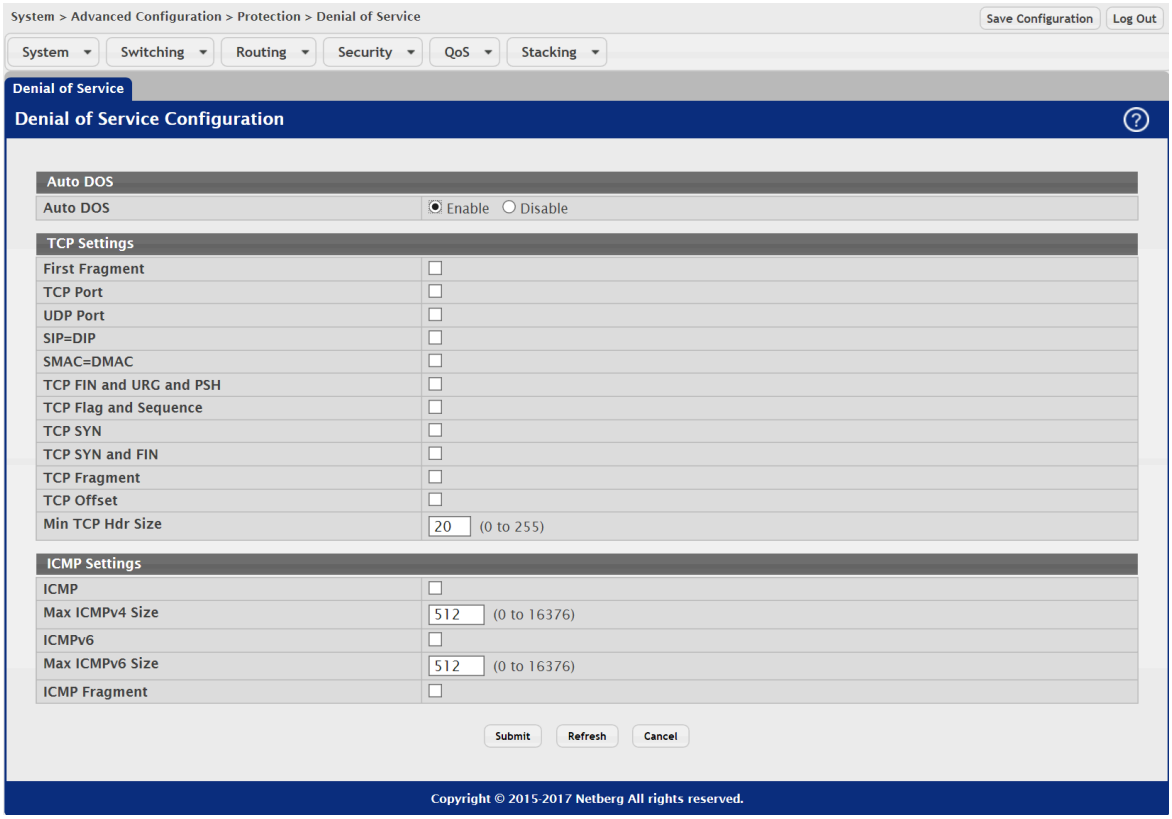
2.2.4.7. System > Advanced Configuration > Green Ethernet > EEE History

This page displays information about the Energy Efficient Ethernet (EEE) Low-Power Idle (LPI) history on the device.

Interface	The interfaces enabled for EEE.
EEE LPI History Sampling Interval	The amount of time to wait between collecting LPI samples on the device.
EEE LPI History Maximum	The maximum number of samples maintained in the LPI history table.
Sample No.	A unique number that identifies the sample.
Age	The amount of time that has passed since the sample was recorded.
% Time in LPI since last sample	The percentage of time the interface has spent in LPI mode since the last sample was taken.
% Time in LPI since last reset	The percentage of time the interface has spent in LPI mode since the last time the EEE statistics were cleared.

2.2.5. System > Advanced Configuration > Protection

2.2.5.1. System > Advanced Configuration > 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.

Table 2.9. Auto DOS

Auto DOS	Enable this option to allow the device to perform DOS automatically. The following options will be enabled: SIP=DIP First Fragment TCP Fragment ICMP SMAC=DMAC ICMP Fragment ICMPv6

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.

Table 2.10. TCP Settings

First Fragment	Enable this option to allow the device to drop packets that have a TCP header smaller than the value configured in the Min TCP Hdr Size field.
TCP Port	Enable this option to allow the device to drop packets that have the TCP source port equal to the TCP destination port.
UDP Port	Enable this option to allow the device to drop packets that have the UDP source port equal to the UDP destination port.
SIP=DIP	Enable this option to allow the device to drop packets that have a source IP address equal to the destination IP address.
SMAC=DMAC	Enable this option to allow the device to drop packets that have a source MAC address equal to the destination MAC address.
TCP FIN and URG and PSH	Enable this option to allow the device to drop packets that have TCP Flags FIN, URG, and PSH set and a TCP Sequence Number equal to 0.
TCP Flag and Sequence	Enable this option to allow the device to drop packets that have TCP control flags set to 0 and the TCP sequence number set to 0.
TCP SYN	Enable this option to allow the device to drop packets that have TCP Flags SYN set.
TCP SYN and FIN	Enable this option to allow the device to drop packets that have TCP Flags SYN and FIN set.
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.
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.

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.

Table 2.11. ICMP Settings

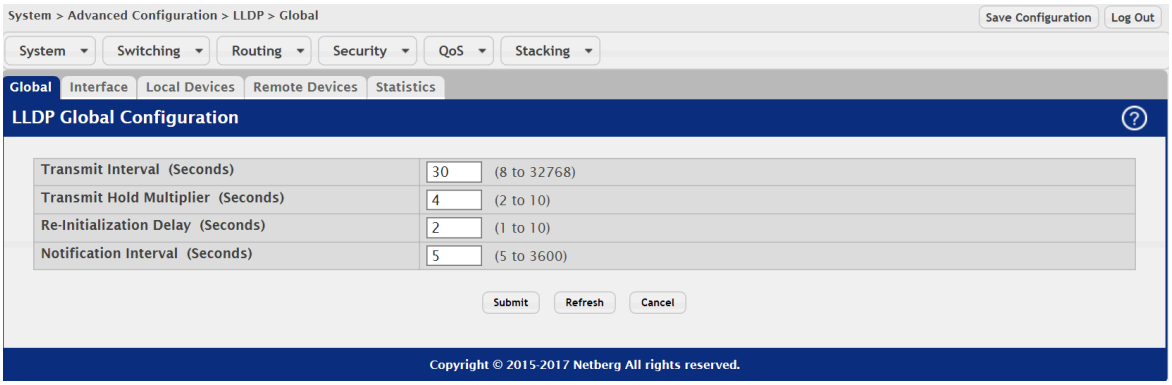
ICMP	Enable this option to allow the device to drop ICMP packets that have a type set to ECHO_REQ (ping) and a payload size greater than the ICMP payload size configured in the Max ICMPv4 Size field.
Max ICMPv4 Size	The maximum allowed ICMPv4 packet size. If ICMP DoS prevention is enabled, the device 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.

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

2.2.6. System > Advanced Configuration > LLDP

2.2.6.1. System > Advanced Configuration > LLDP > Global

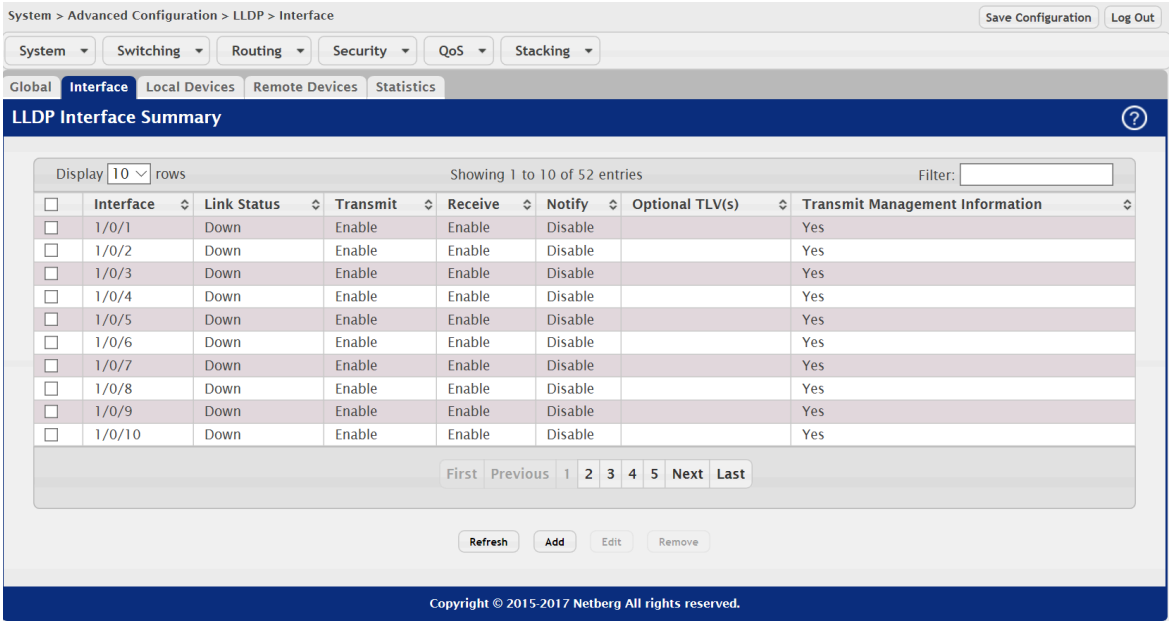


Use this page to set the global Link Layer Discovery Protocol (LLDP) timers. LLDP is defined by the IEEE 802.1AB standard and allows the device to advertise major capabilities and physical descriptions. This information can help you identify system topology and detect bad configurations on the LAN. All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

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.

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

2.2.6.2. System > Advanced Configuration > LLDP > 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.

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.

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.
Link Status	The link status of the interface, which is either Up or Down. An interface that is down does not forward traffic.

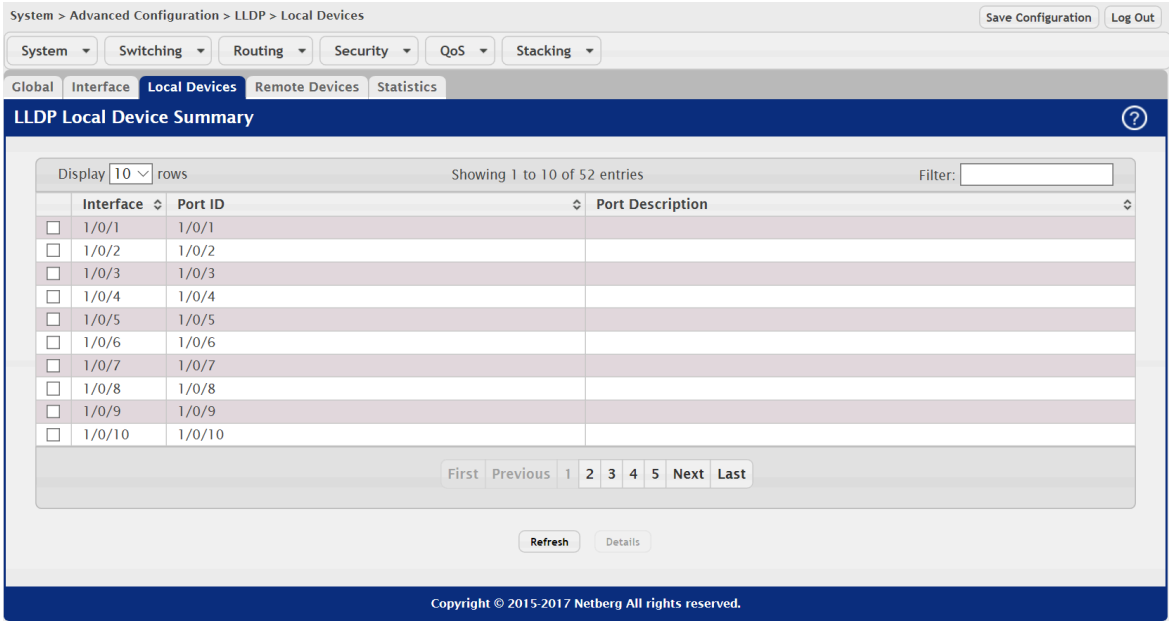
Transmit	The LLDP advertise (transmit) mode on the interface. If the transmit mode is enabled, the interface sends LLDP Data Units (LLDPDUs) that advertise the mandatory TLVs and any optional TLVs that are enabled.
Receive	The LLDP receive mode on the interface. If the receive mode is enabled, the device 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.

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.

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

2.2.6.3. System > Advanced Configuration > LLDP > 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	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.

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

System Capabilities Supported	The primary function(s) the device supports.
System Capabilities Enabled	The primary function(s) the device supports that are enabled.
Management Address	The physical address associated with the management interface of the device.
Management Address Type	The protocol type or standard associated with the management address.

2.2.6.4. System > Advanced Configuration > LLDP > Remote Devices

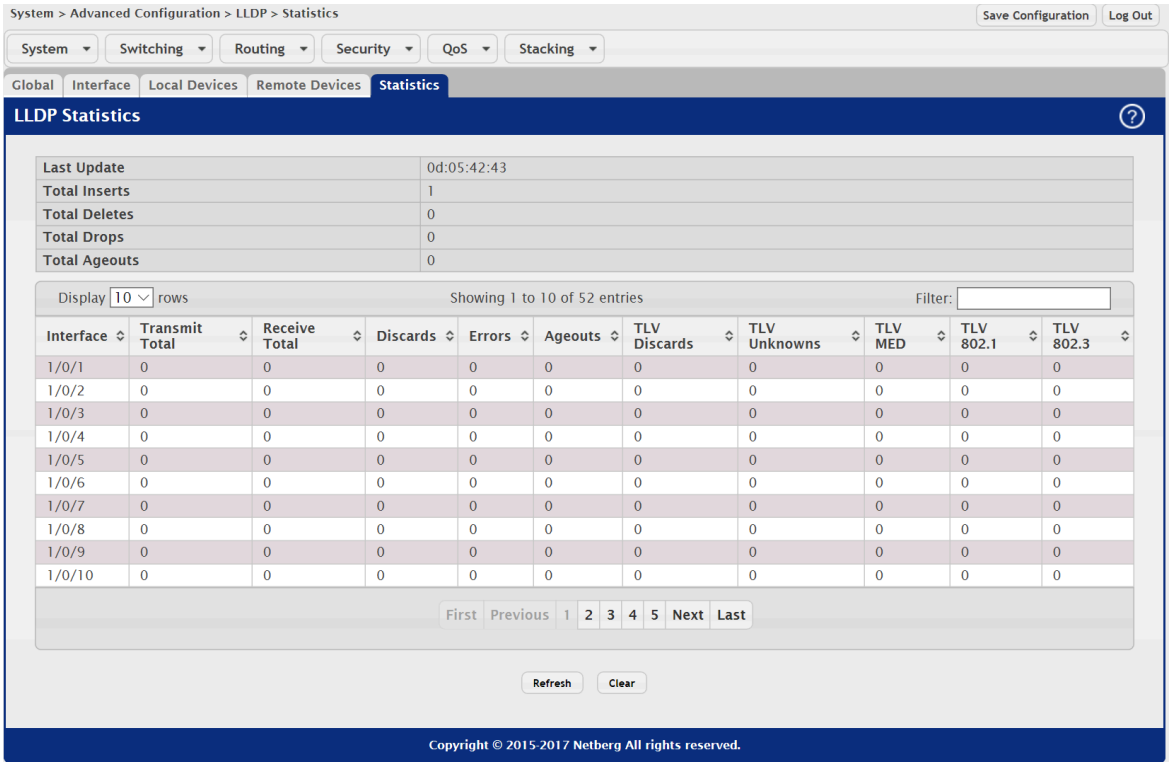
This page displays information about the remote devices the local system has learned about through the Link Layer Discovery Protocol (LLDP) data units received on its interfaces. The table lists all interfaces that are enabled to receive LLDP data from remote devices. However, information is available 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.

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.

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.

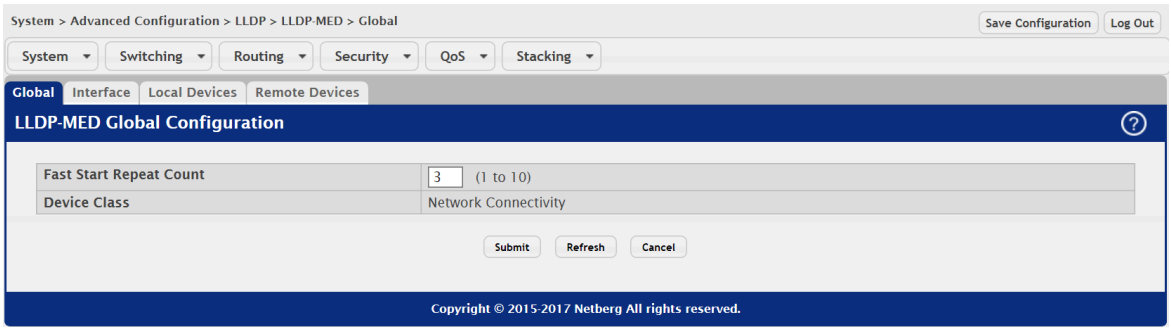
2.2.6.5. System > Advanced Configuration > LLDP > Statistics



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.

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.

2.2.6.6. System > Advanced Configuration > LLDP > LLDP-MED > 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:

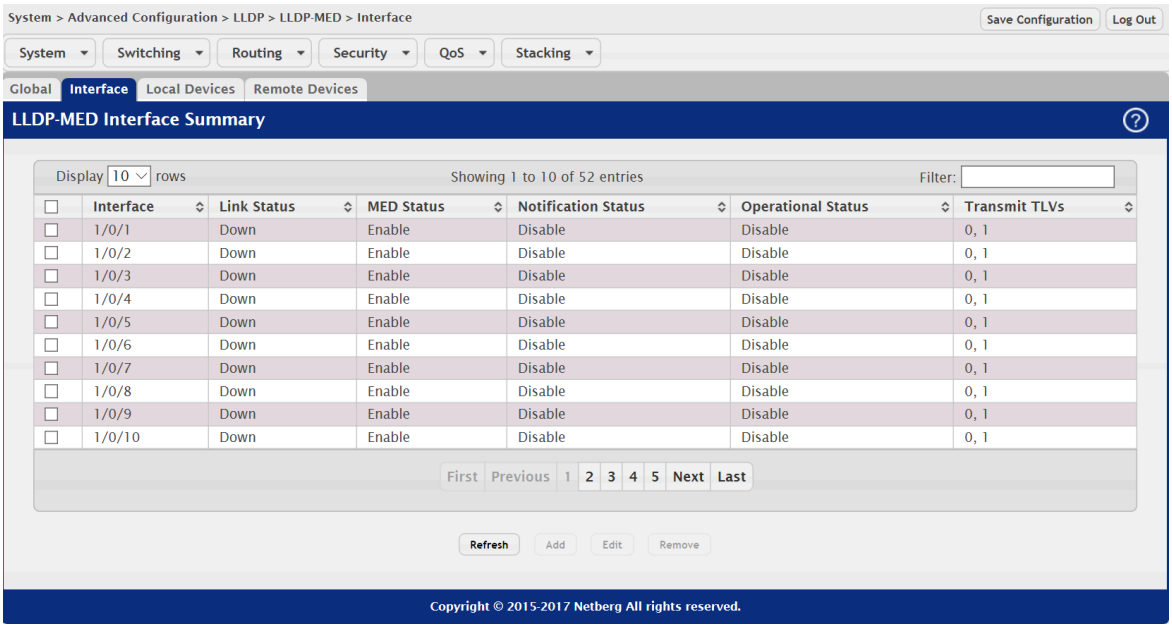
- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and DiffServ settings), enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet (PoE) endpoints.
- Inventory management, enabling 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.

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.

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

2.2.6.7. System > Advanced Configuration > LLDP > LLDP-MED > Interface



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).

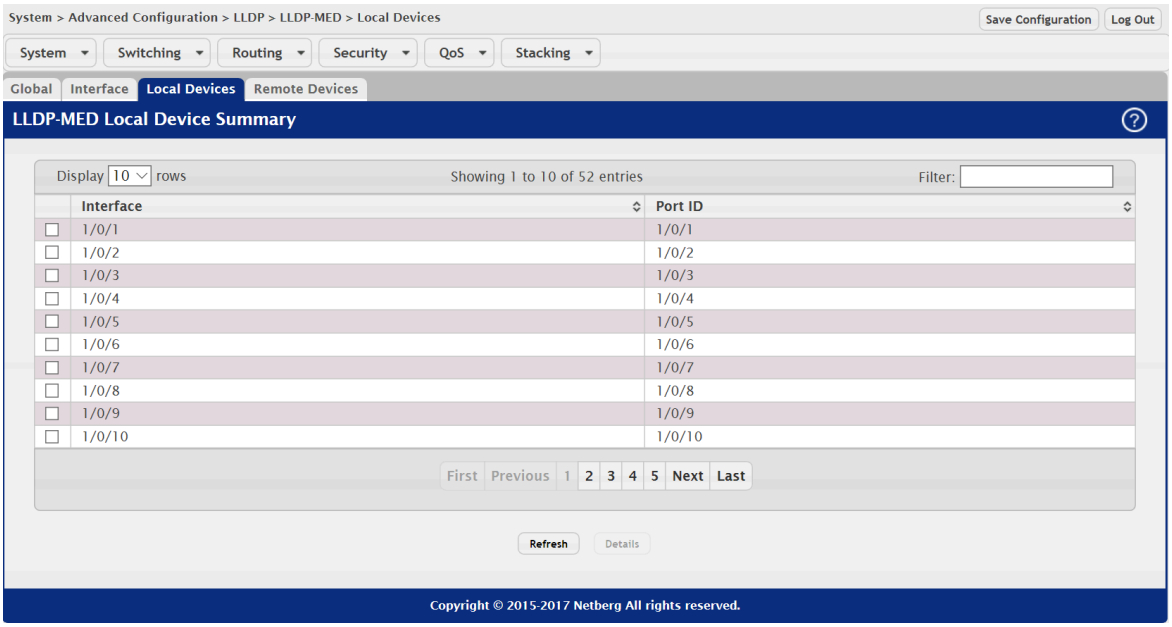
LLDP-MED uses LLDP's organizationally-specific Type-Length-Value (TLV) extensions and defines new TLVs that make it easier for a VoIP deployment in a wired or wireless LAN/MAN environment. It also makes mandatory a few optional TLVs from LLDP and recommends not transmitting some TLVs.

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.

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

2.2.6.8. System > Advanced Configuration > LLDP > LLDP-MED > 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**.

Interface	The interface associated with the rest of the data in the row. When viewing LLDP-MED details for an interface, this field identifies the interface that is being viewed.
Port ID	The MAC address of the interface. This is the MAC address that is advertised in LLDP-MED PDUs.

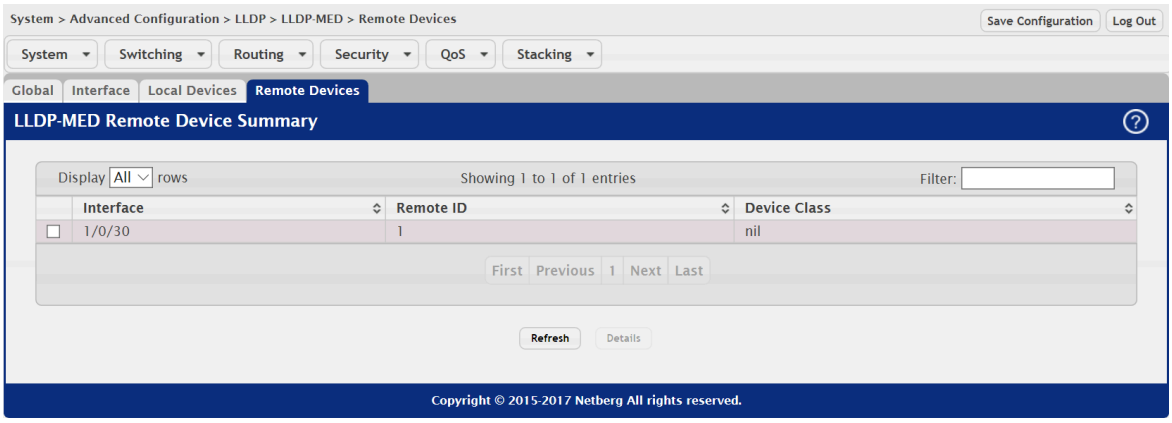
After you click **Details**, a window opens and shows detailed information about the LLDP-MED information the selected interface transmits. The following information describes the additional fields that appear in the **LLDP-MED Local Device Information** window.

Network Policy Information	The information in this table identifies the data transmitted in the Network Policy TLVs.

Media Application Type	The media application type transmitted in the TLV. The application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Each application type that is transmitted has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port may transmit one or many such application types. This information is displayed only when a network policy TLV has been transmitted.
VLAN ID	The VLAN ID associated with a particular policy type.
Priority	The user priority associated with a particular policy type.
DSCP	The DSCP value associated with a particular policy type.
Unknown Bit Status	The unknown bit associated with a particular policy type.
Tagged Bit Status	Identifies whether the network policy is defined for tagged or untagged VLANs.

Location Information	The information in this table identifies the data transmitted in the location TLVs.
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.

2.2.6.9. System > Advanced Configuration > LLDP > LLDP-MED > 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.

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	This section describes the supported and enabled capabilities that were received in the LLDP-MED TLVs on this interface.
Supported Capabilities	The supported capabilities that were received in the MED TLV on this interface.
Enabled Capabilities	The supported capabilities on the remote device that are also enabled.
Device Class	The MED Classification advertised by the TLV from the remote device. The following three classifications represent the actual endpoints: • Class I Generic (for example, IP Communication Controller) • Class II Media (for example, Conference Bridge) • Class III Communication (for example, IP Telephone) The fourth device is Network Connectivity Device, which is typically a device such as a LAN switch or router, IEEE 802.1 bridge, or IEEE 802.11 wireless access point.

Network Policy Information	This section describes the information in the network policy TLVs received in the LLDP-MED frames on this interface.
Media Application Type	The media application type received in the TLV from the remote device. The application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Each application type that is transmitted has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. The port on the remote device may transmit one or many such application types. This information is displayed only when a network policy TLV has been received.
VLAN ID	The VLAN ID associated with a particular policy type.
Priority	The user priority associated with a particular policy type.
DSCP	The DSCP value associated with a particular policy type.
Unknown Bit Status	The unknown bit associated with a particular policy type.
Tagged Bit Status	Identifies whether the network policy is defined for tagged or untagged VLANs.

Inventory Information	This section describes the information in the inventory TLVs received in the LLDP-MED frames on this interface.
Hardware Revision	The hardware version advertised by the remote device.

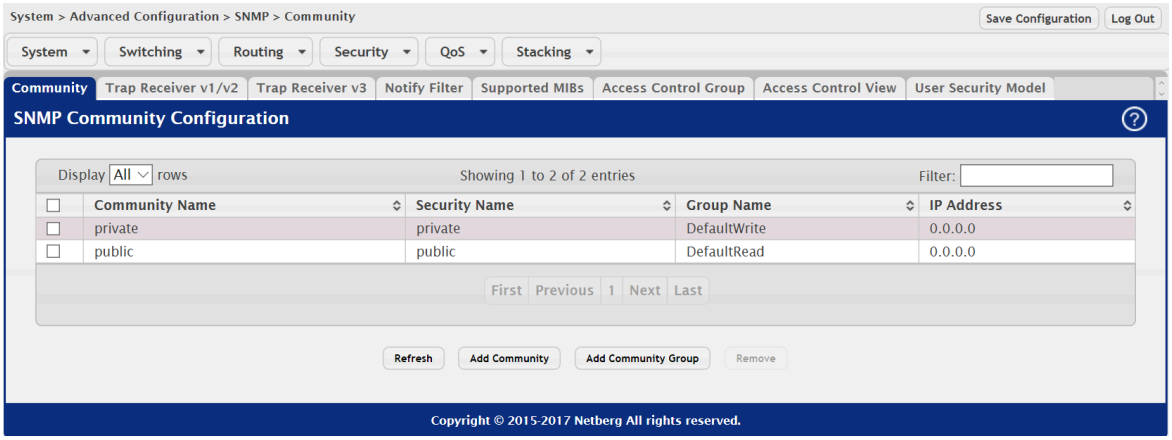
Firmware Revision	The firmware version advertised by the remote device.
Software Revision	The software version advertised by the remote device.
Serial Number	The serial number advertised by the remote device.
Manufacturer Name	The name of the system manufacturer advertised by the remote device.
Model Name	The name of the system model advertised by the remote device.
Asset ID	The system asset ID advertised by the remote device.

Location Information	This section describes the information in the location TLVs received in the LLDP-MED frames on this interface.
Sub Type	The type of location information advertised by the remote device.
Information	The text description of the location information included in the subtype.

Extended PoE	Indicates whether the remote device is advertised as a PoE device.
Device Type	If the remote device is a PoE device, this field identifies the PoE device type of the remote device connected to this port.

Extended PoE PD	The information about PoE powered device.

2.2.6.10. System > Advanced Configuration > SNMP > 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:

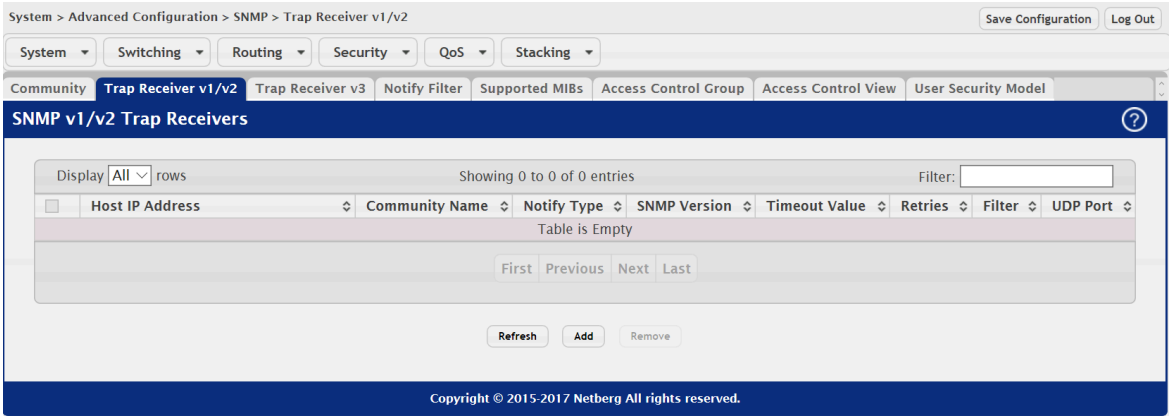
- To add a community, click Add and configure the desired settings.
- To delete a configured community from the list, select the check box associated with each entry to delete and click Remove.

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 (Button)	Add a new SNMP Community
Add Community Group (Button)	Add a new SNMP Community Group

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

2.2.6.11. System > Advanced Configuration > SNMP > 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:

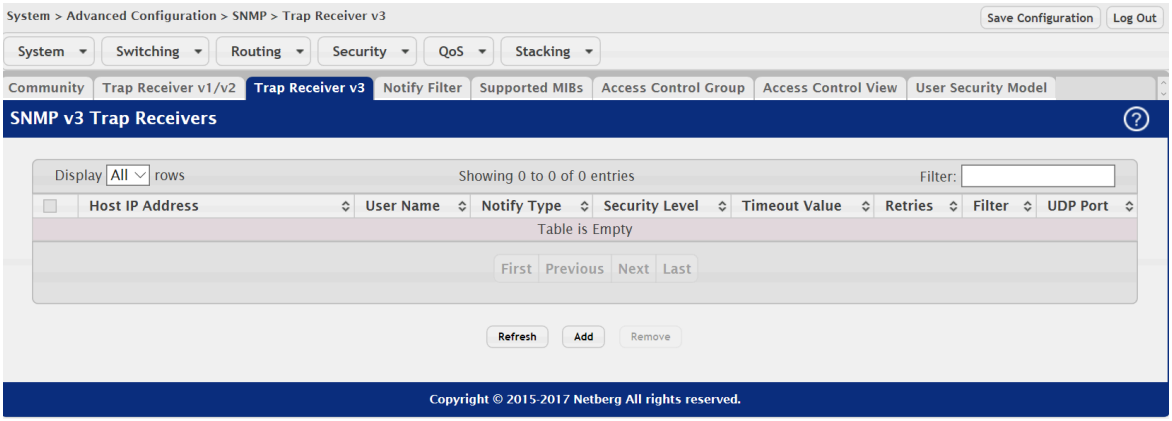
- To add an SNMP trap receiver and configure its settings, click Add and complete the required information.
- To delete one or more SNMP trap receivers from the list, select each entry to delete and click Remove.

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.

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

2.2.6.12. System > Advanced Configuration > SNMP > 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.

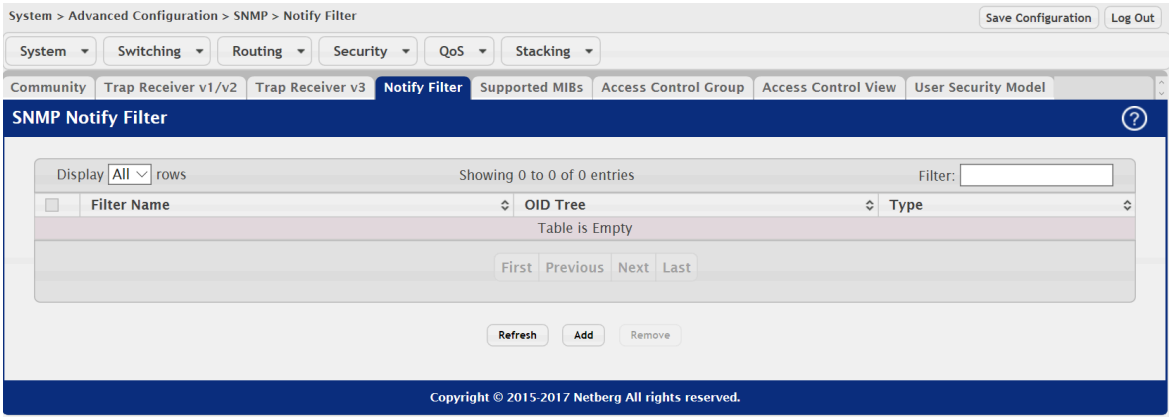
Use the buttons to perform the following tasks:

- 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.

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.

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

2.2.6.13. System > Advanced Configuration > SNMP > Notify Filter



A MIB filter is combination of a set of filter subtrees or a family of filter subtrees where each filter subtree is a subtree within the managed object naming tree. You can create MIB filters to control the OID range.

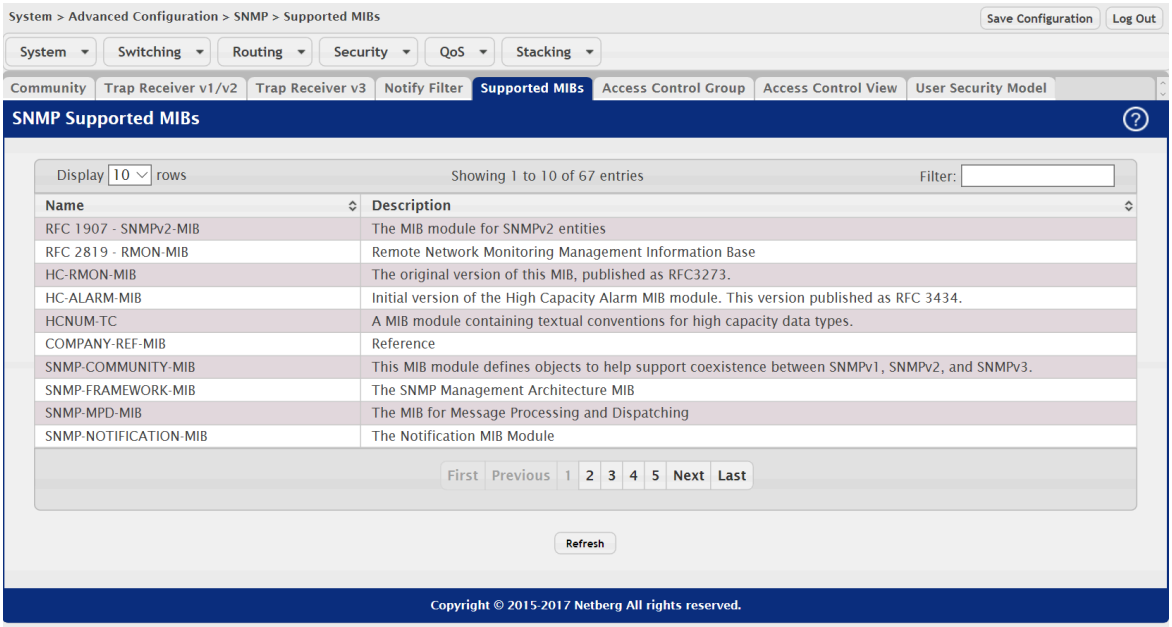
Use the buttons to perform the following tasks:

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

Filter Name	The name of the filter for the SNMP management host. The filter defines which MIB objects to include or exclude from the view. Filter names can contain up to 30 alphanumeric characters.
OID Tree	Specifies the SNMP OID Tree for the subtree to include or exclude from the view. OID string is 128 characters in length.
Type	Specifies whether to include or exclude the filter subtree or family of subtrees from the MIB view.

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

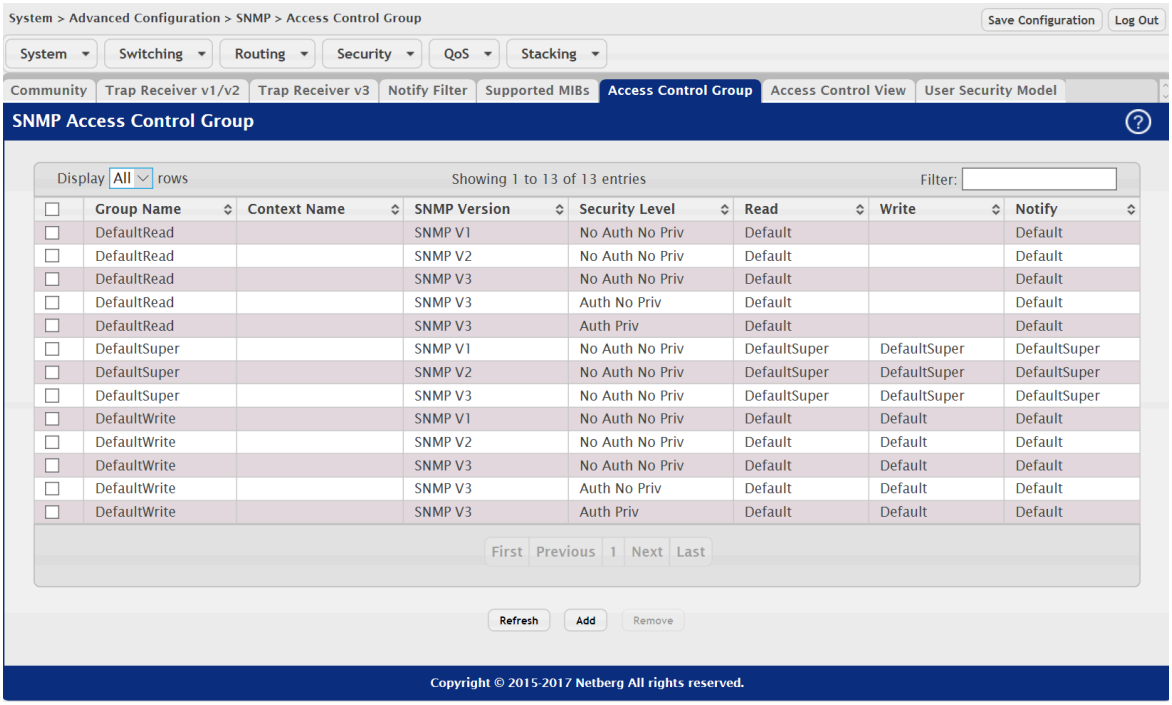
2.2.6.14. System > Advanced Configuration > SNMP > Supported MIBs



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

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.

2.2.6.15. System > Advanced Configuration > SNMP > 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.

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.

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

2.2.6.16. System > Advanced Configuration > SNMP > Access Control View

A MIB view is combination of a set of view subtrees or a family of view subtrees where each view subtree is a subtree within the managed object naming tree. You can create MIB views to control the OID range that SNMP users can access. A MIB view called all is created by default in the system, which contains all management objects supported by the system.

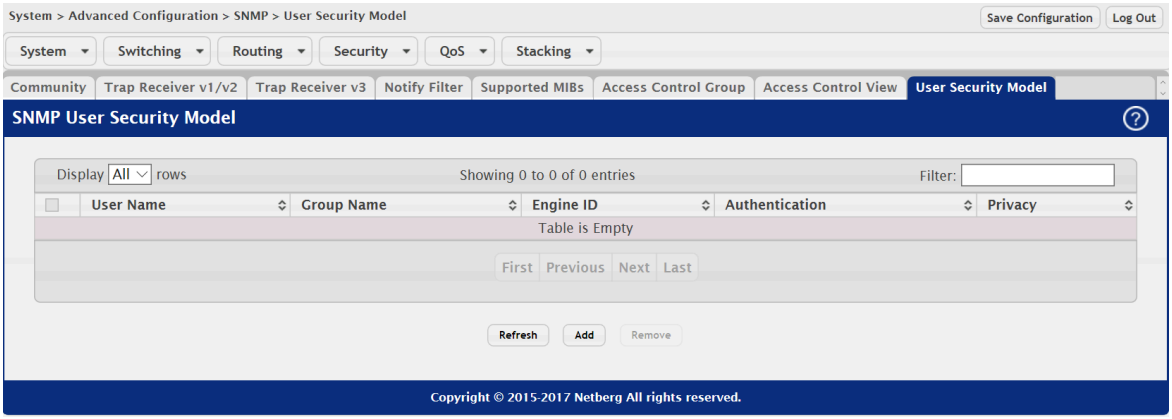
Use the buttons to perform the following tasks:

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

View Name	The name that identifies the SNMP view. View names can contain up to 30 alphanumeric characters.
OID Tree	Specifies the SNMP OID Tree for the subtree to include or exclude from the view. OID string is 128 characters in length.
Type	Specifies whether to include or exclude the view subtree or family of subtrees from the MIB view.

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

2.2.6.17. System > Advanced Configuration > SNMP > User Security Model



This page provides the capability to configure the SNMP V3 user accounts.

- 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.

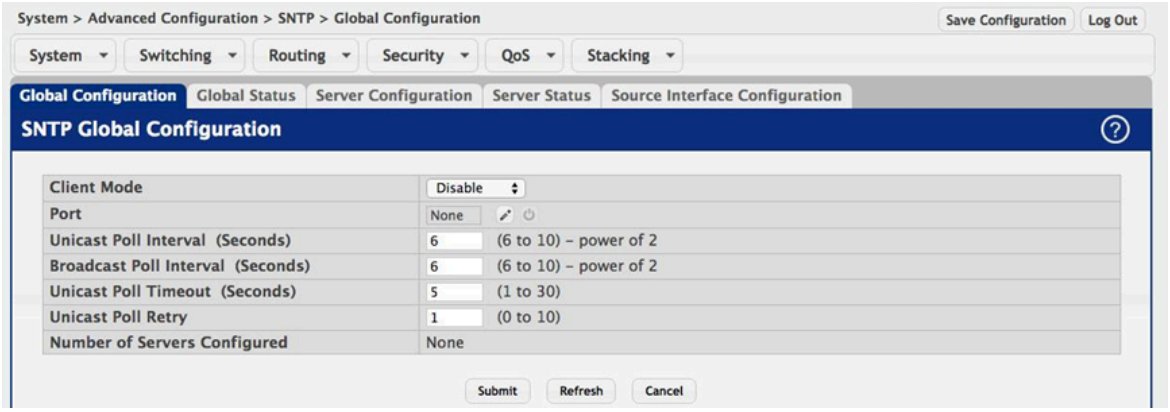
Engine ID	Each SNMPv3 agent has an engine ID that uniquely identifies the agent in the device. If given this entry will be used only for packets whose engine id is this. This field takes an hexadecimal string in the form 0102030405.
User Name	Specifies the name of the SNMP user being added for the User-based 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. • SHA - SHA protocol will be used. • MD5 - MD5 protocol will be used. • None - No authentication will be used for this user.

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. • DES - DES protocol will be used. • None - No privacy 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.

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

2.2.7. System > Advanced Configuration > SNTP

2.2.7.1. System > Advanced Configuration > SNTP > Global Configuration



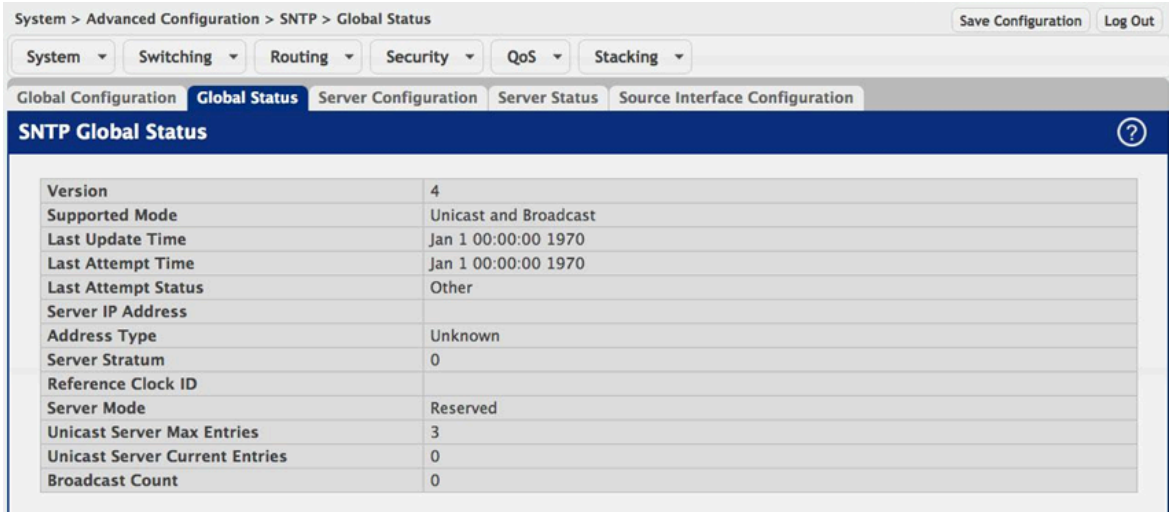
Use this page to enable the Simple Network Time Protocol (SNTP) client on the device and to configure the SNTP client settings. Enabling and configuring the SNTP client allows the device to synchronization the system time with a valid SNTP server on the network.

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.

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

2.2.7.2. System > Advanced Configuration > SNTP > Global Status



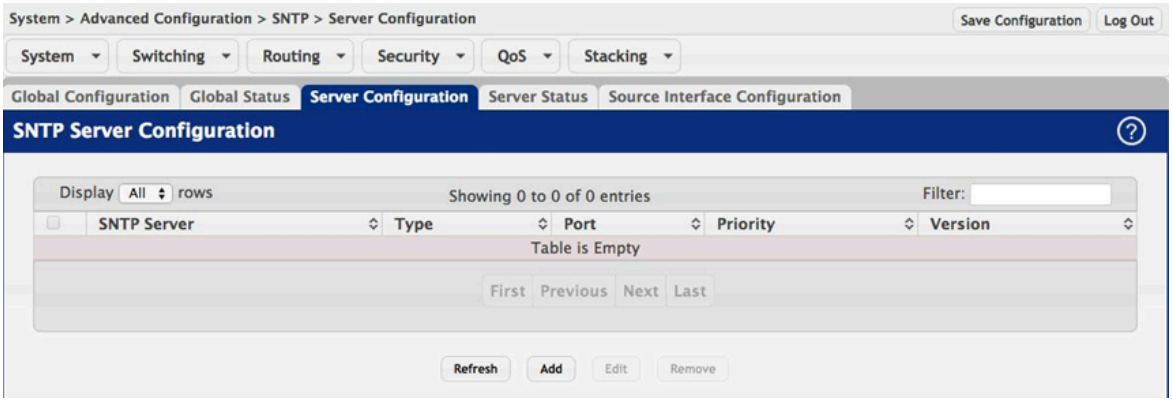
This page displays global status information related to SNTP operation in the device.

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.
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.

2.2.7.3. System > Advanced Configuration > SNTP > 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	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.

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

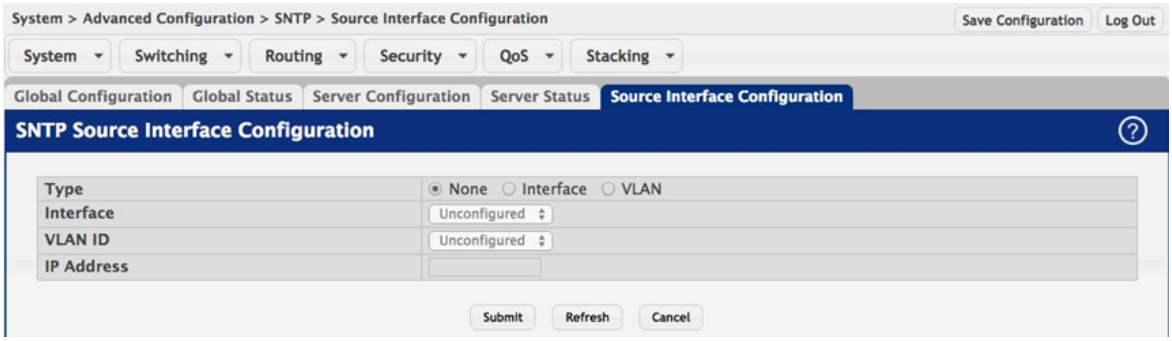
2.2.7.4. System > Advanced Configuration > SNTP > Server Status

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

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.
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.

2.2.7.5. System > Advanced Configuration > SNTP > Source Interface Configuration



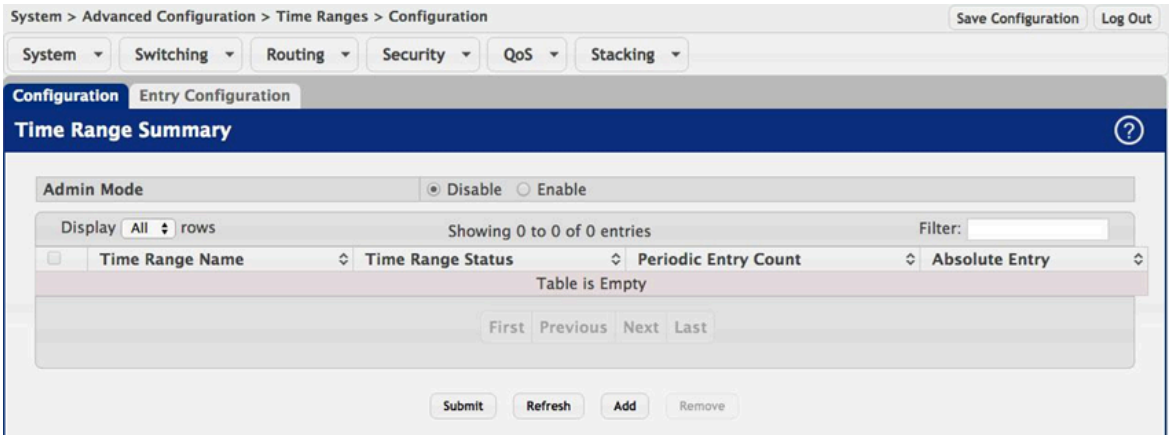
Use this page to specify the physical or logical interface to use as the SNTP client source interface. When an IP address is configured on the source interface, this address is used for all SNTP communications between the local SNTP client and the remote SNTP server. The IP address of the designated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

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.
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.
IP Address	The IP address associated with the configured Source Interface.

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

2.2.8. System > Advanced Configuration > Time Ranges

2.2.8.1. System > Advanced Configuration > Time Ranges > Configuration



Use this page to add and remove time range configurations. 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:

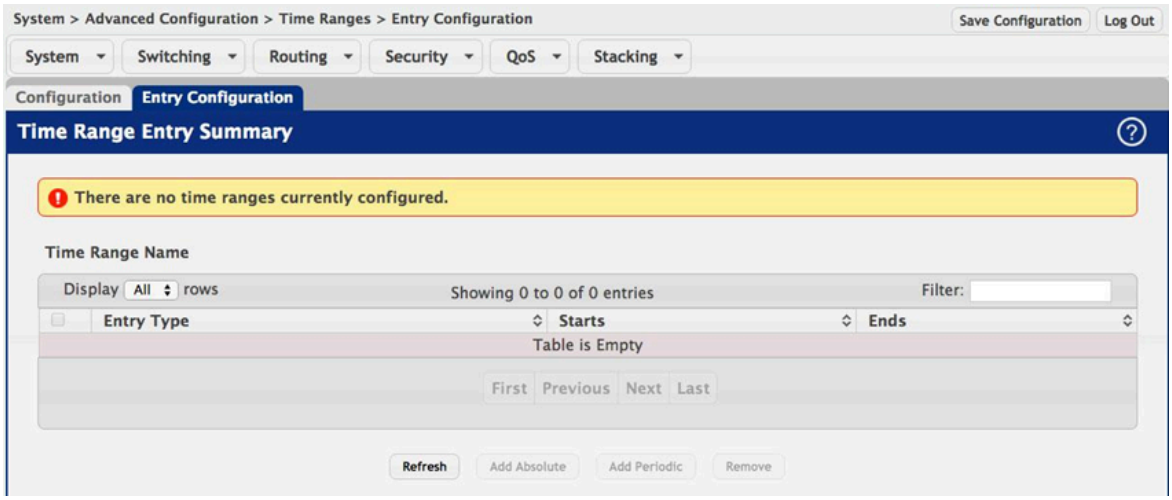
- To add a time range, click Add and configure a name for the time range configuration.
- To delete a configured time range, select each entry to delete, click Remove, and confirm the action.

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.

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

2.2.8.2. System > Advanced Configuration > Time Ranges > 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.

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.

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.

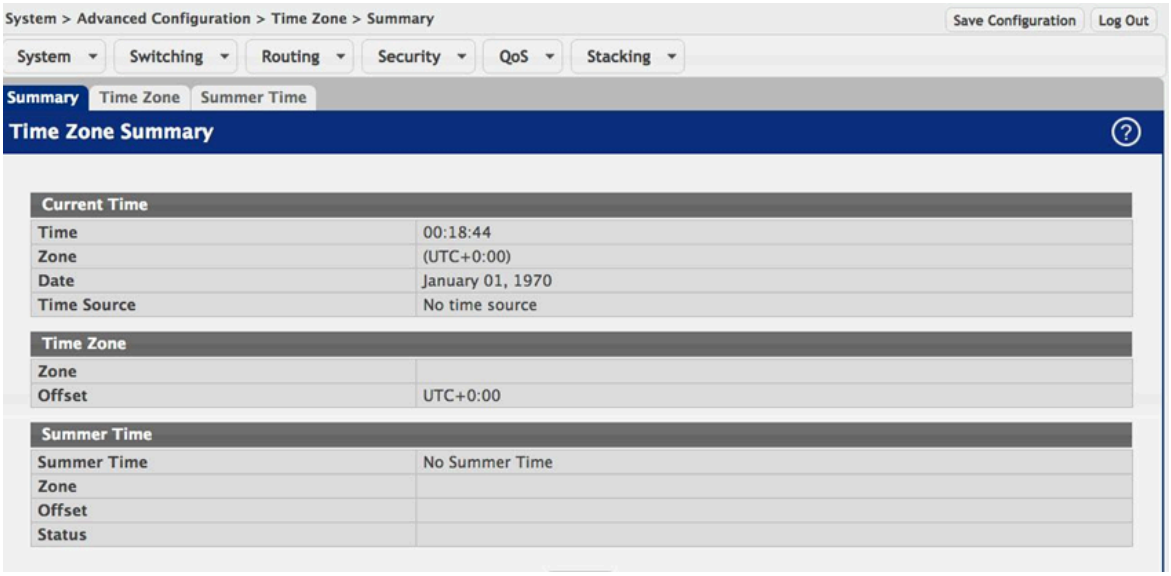
Time Range Name	The time range configuration that will include the Periodic time range entry.
Applicable Days	Select the days on which the Periodic time range entry is active: • Daily – Every day of the week

	• 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.

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

2.2.9. System > Advanced Configuration > Time Zone

2.2.9.1. System > Advanced Configuration > Time Zone > Summary



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.

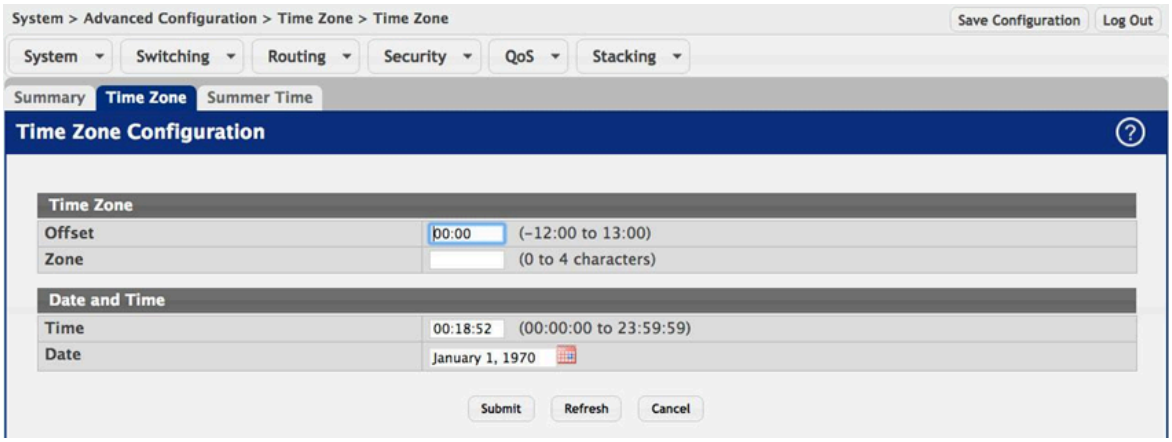
Current Time	This section contains information about the system time and date on the device. If the current time has not been acquired by the SNTP client on the device or configured manually, this section shows the default time and date plus the amount of time since the system was reset.
Time	The current time on the system clock. This time is used to provide time stamps on log messages. 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	This section contains information about the time zone and offset.
Zone	The acronym that represents the time zone.
Offset	The number of hours offset from Coordinated Universal Time (UTC), which is also known as Greenwich Mean Time (GMT).

Summer Time	The administrative status of summer time (daylight saving time). In some regions, the time shifts by one hour in the fall and spring.
Summer Time	The summer time mode on the system: • Disable – Summer time is not active, and the time does not shift based on the time of year. • Recurring – Summer time occurs at the same time every year. The start and end times and dates for the time shift must be manually configured. • EU – The system clock uses the standard recurring summer time settings used in countries in the European Union. When this field is selected, the rest of the applicable fields on the page except Offset and Zone are automatically populated and cannot be edited. • USA – The system clock uses the standard recurring daylight saving time settings used in the United States. When this field is selected, the rest of the applicable fields on the page except Offset and Zone are automatically populated and cannot be edited. • Non-Recurring – Summer time settings are in effect only between the start date and end date of the specified year. When this mode is selected, the summer time settings do not repeat on an annual basis.

Zone	The acronym that represents the time zone of the summer time.
Offset	The number of hours offset from Coordinated Universal Time (UTC), which is also known as Greenwich Mean Time (GMT).
Status	Indicates if summer time is currently active.

2.2.9.2. System > Advanced Configuration > Time Zone > Time Zone



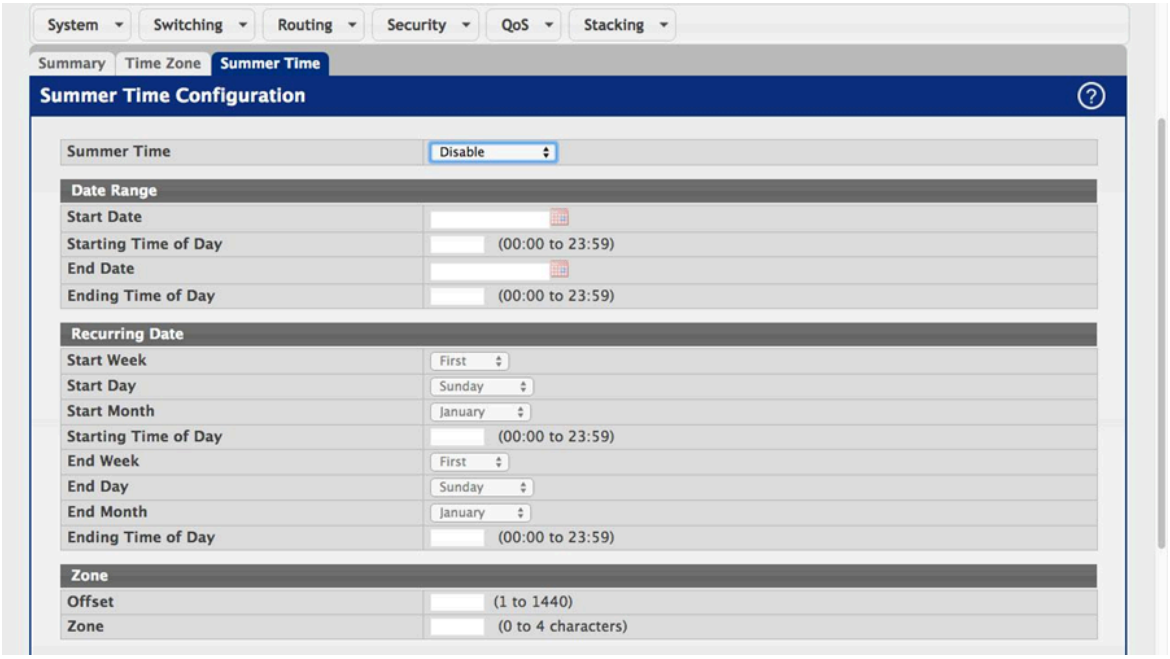
Use this page to manually configure the system clock settings. The SNTP client must be disabled to allow manual configuration of the system time and date.

Time Zone	The time zone settings include the amount of time the system clock is offset from Coordinated Universal Time (UTC) and the time zone acronym.
Offset	The 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	Use the fields in this section to manually configure the system time and date. If the SNTP client is enabled (Unicast mode or Broadcast mode), these fields cannot be configured.
Time	The current time in hours, minutes, and seconds on the system clock.
Date	The current date in month, day, and year on the system clock. To change the date, click the calendar icon to the right of the field, select the year from the menu, browse to the desired month, and click the date.

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

2.2.9.3. System > Advanced Configuration > Time Zone > 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	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	The fields in this section are available only if the Non-Recurring mode is selected from the Summer Time menu.
Start Date	The day, month, and year that summer time begins. To change the date, click the calendar icon to the right of the field, select the year from the menu, browse to the desired month, and click the date.
Starting Time of Day	The time, in hours and minutes, to start summer time on the specified day.
End Date	The day, month, and year that summer time ends. To change the date, click the calendar icon to the right of the field, select the year from the menu, browse to the desired month, and click the date.
Ending Time of Day	The time, in hours and minutes to end summer time on the specified day.

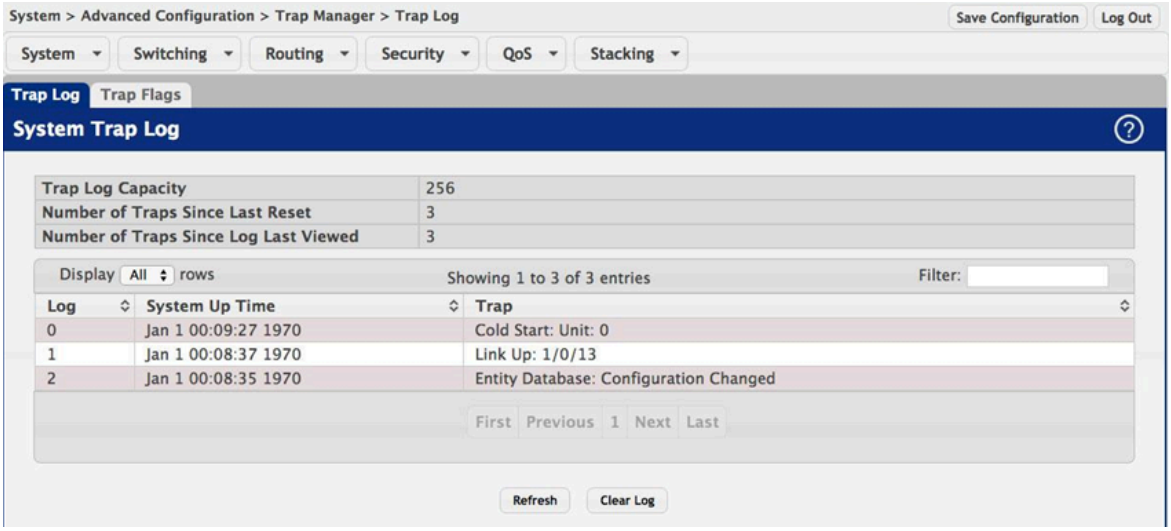
Recurring Date	The fields in this section are available only if the Recurring mode is selected from the Summer Time menu.
Start Week	The week of the month within which summer time begins.
Start Day	The day of the week on which summer time begins.
Start Month	The month of the year within which summer time begins.
Starting Time of Day	The time, in hours and minutes, to start summer time.
End Week	The week of the month within which summer time ends.
End Day	The day of the week on which summer time ends.
End Month	The month of the year within which summer time ends.
Ending Time of Day	The time, in hours and minutes, to end summer time.

Zone	The fields in this section are available for all modes selected from the Summer Time menu except Disable.
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.

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

2.2.10. System > Advanced Configuration > Trap Manager

2.2.10.1. System > Advanced Configuration > Trap Manager > Trap Log

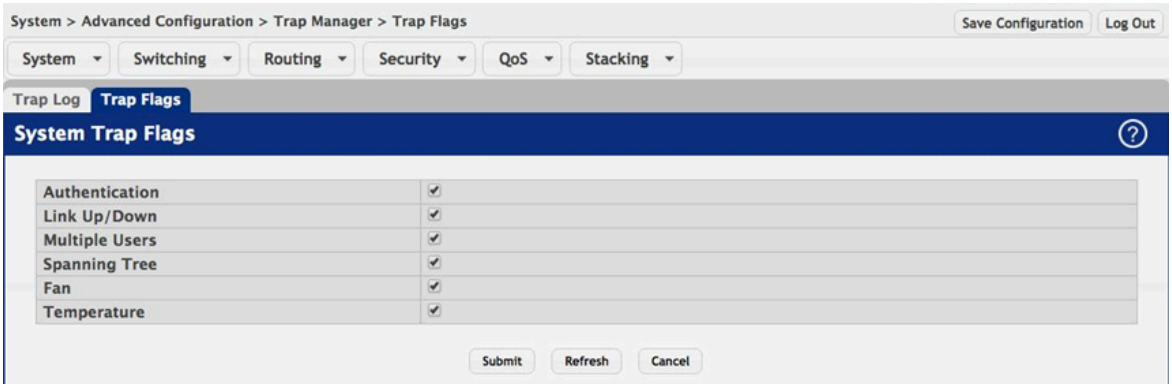


This page displays information about the SNMP traps that have been logged to the device. You can save the trap log to a file on a remote system by using the Upload page.

Trap Log Capacity	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.

2.2.10.2. System > Advanced Configuration > Trap Manager > Trap Flags



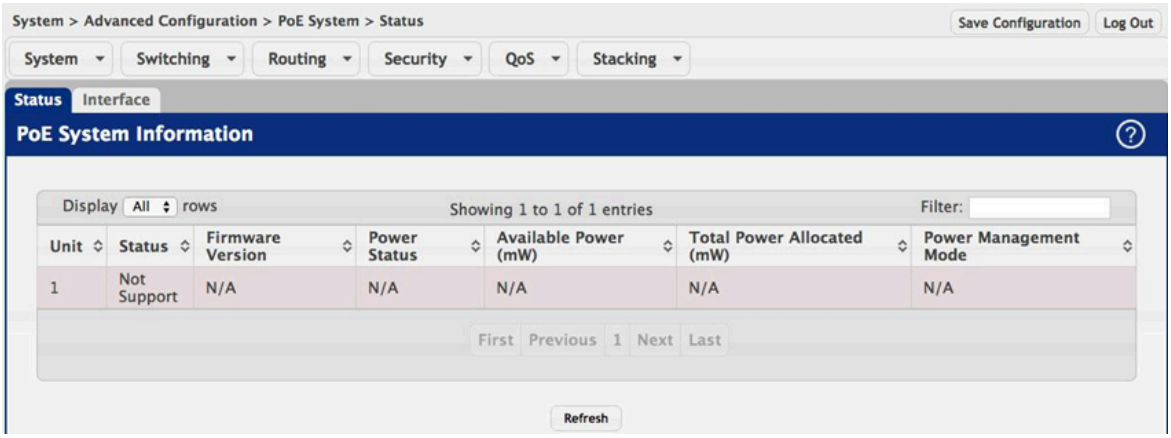
Use this page to specify which software features should generate SNMP traps. If the trap flag is enabled for a feature and a significant event occurs, the SNMP agent on the device sends a trap message to any enabled SNMP trap receivers and writes a message to the trap log.

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.
Fan	Specify whether to enable SNMP notifications when fan events occur.
Temperature	Specify whether to enable SNMP notifications when temperature events occur.

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

2.2.11. System > Advanced Configuration > PoE System

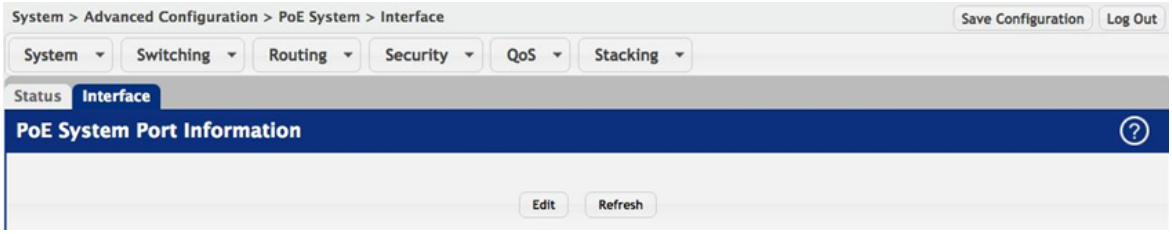
2.2.11.1. System > Advanced Configuration > PoE System > Status



Use this page to view status information about the PoE System feature on the device.

Unit	The device Unit ID.
Status	The status of this device. • Ready – It means that PoE system of this device is ready. • Not Ready – It means that this device is failed to initialize the PoE system. • Not Support – It means that this device does not support the PoE system.
Firmware Version	Version of the PoE controller's FW image.
Power Status	Indicates the power status.
Available Power (mW)	Maximum amount of available power the system can deliver to all ports in milliWatts.
Total Power Allocated (mW)	Total amount of a power which is currently allocated for all ports in milliWatts.
Power Management Mode	Describes or controls the power management algorithm used by the PSE to deliver power to the requesting PDs. • Static – It means power allocated for each port depends on the type of power threshold configured on the port. • Dynamic – It means that power consumption of each port is measured and calculated in real-time.

2.2.11.2. System > Advanced Configuration > PoE System > Interface

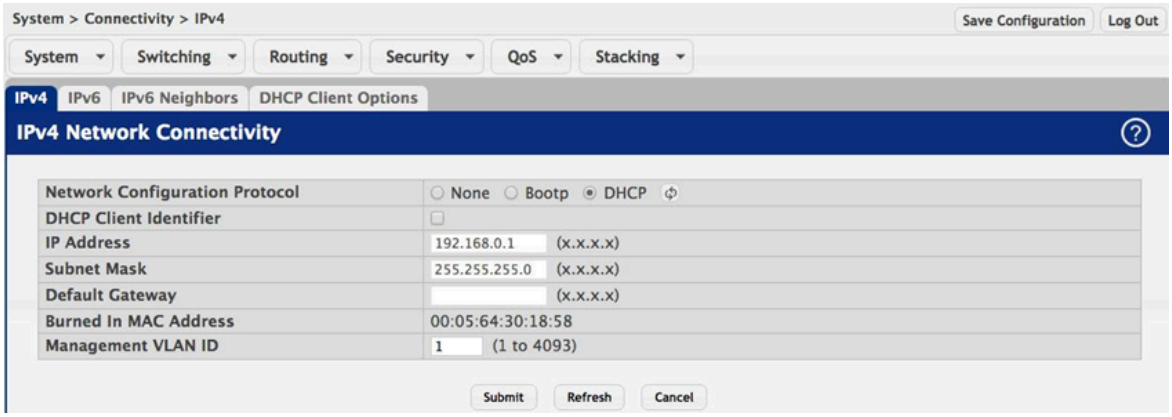


Use this page to configure per-port PoE System settings. Only interfaces that are capable of supporting PoE System modes appear in the table. To configure the settings for one interface, select each interface to configure and click Edit.

Interface	The interface associated with the rest of the data in the row. When configuring the settings for one interface, this field identifies the interface being configured.
Admin Mode	Enables/Disables the ability of the port to deliver a power.
Time Range Name	Indicates the time range being configured to the interface.
Port Status	Indicates the port status.
Class Info	The class information of the Powered Device (PD) defines the range of power a PD is drawing from the system.
Output Voltage (V)	Current voltage being delivered to device in Volts.
Output Current (mA)	Current being delivered to device in mA.
Output Power (mW)	Current power being delivered to device in milliWatts.
Temperature	The temperature measured at this port of the PoE Controller. It is measured in degree celsius.

2.3. System > Connectivity

2.3.1. System > Connectivity > IPv4



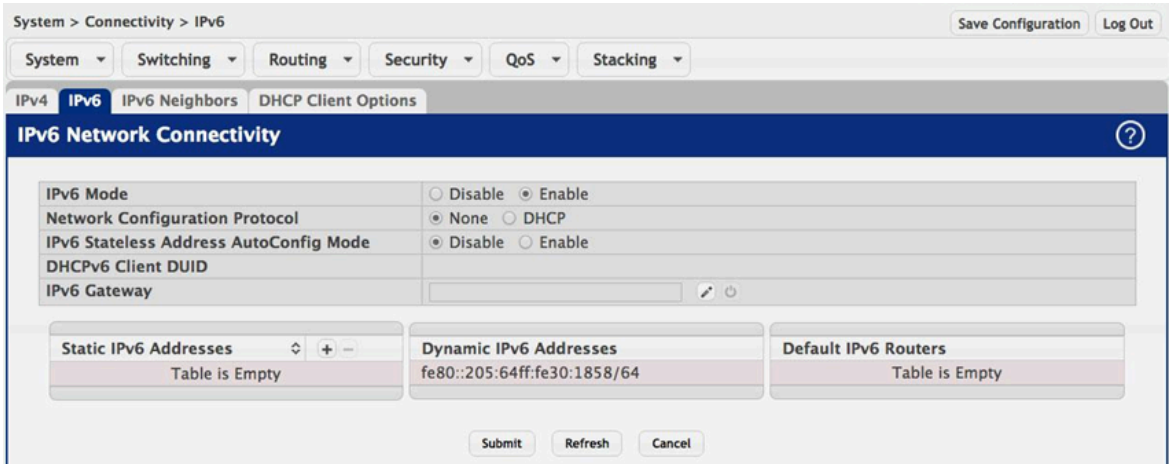
Use this page to configure and view the IPv4 network connectivity information on the network interface. The network interface is the logical interface that allows remote management of the device via any of the front-panel switch ports. To enable management of the device over an IPv4 network by using 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.

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.

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

2.3.2. System > Connectivity > IPv6

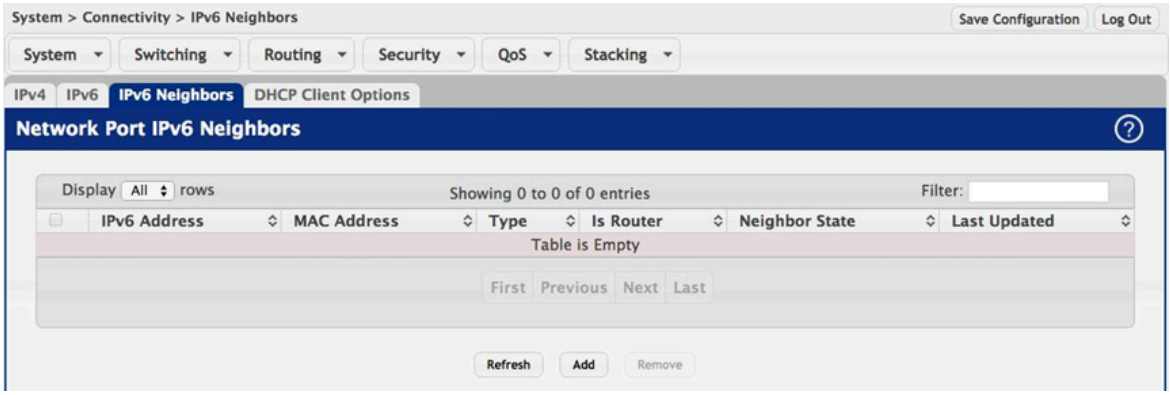


Use this page to configure and view IPv6 information on the network interface. The network interface is the logical interface that allows remote management of the device via any of the front-panel switch ports. To enable management of the device over an IPv6 network by using a Web browser, SNMP, Telnet, 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 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.

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

2.3.3. System > Connectivity > IPv6 Neighbors



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

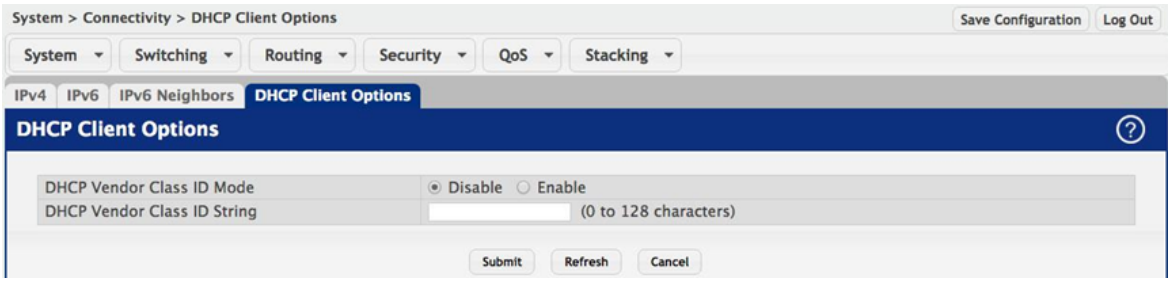
Use the buttons to perform the following tasks:

- 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	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.

2.3.4. System > Connectivity > DHCP Client Options



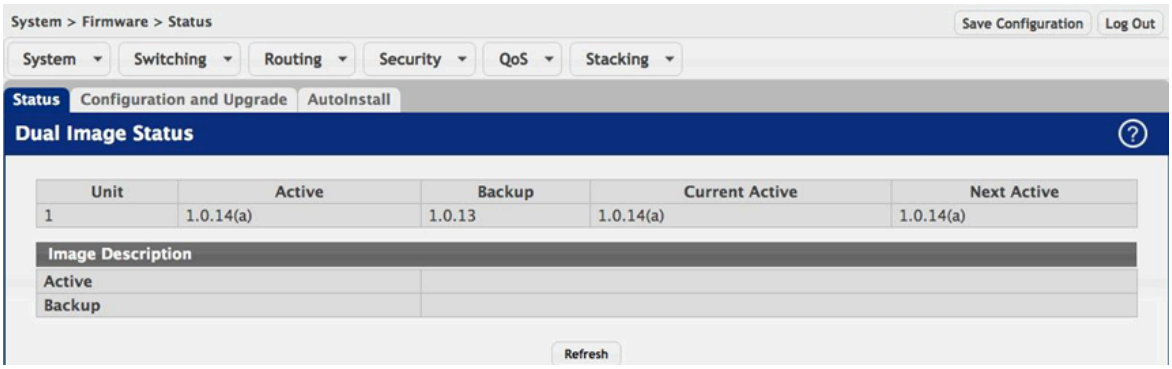
Use this page to set a value for DHCP option 60 in the DHCP requests that the DHCP client on the device broadcasts to network DHCP servers. Option 60, the Vendor Class Identifier (VCI), can help identify the device to the DHCP server, which allows the server to include additional information in the DHCP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

DHCP 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.

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

2.4. System > Firmware

2.4.1. System > Firmware > Status

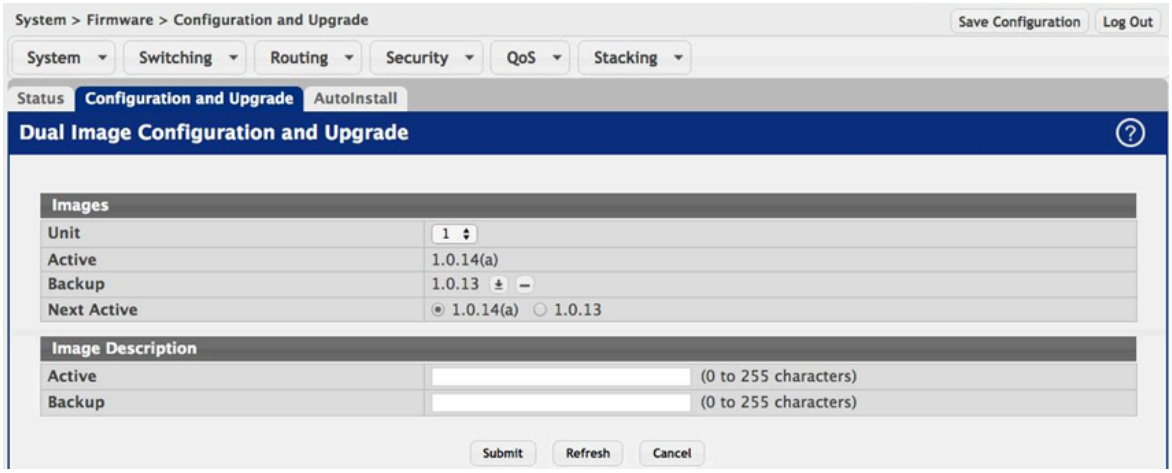


Use this page to view information about the software images on the device. The device can store up to two software images in permanent storage. The dual image feature allows you to upgrade the device without deleting the older software image.

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.

2.4.2. System > Firmware > 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.

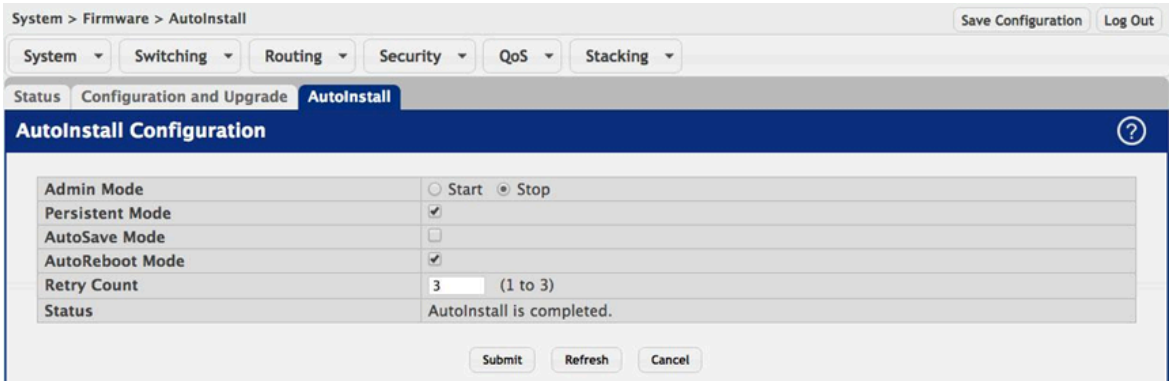
The device uses the HTTP protocol to transfer the image, and the image is saved as the backup image.

Unit	Select the unit with the code image to activate, upgrade, delete, or describe.
Active	The active code file version.
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.
Status	Provides information about the status of the file transfer.

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

2.4.3. System > Firmware > AutoInstall



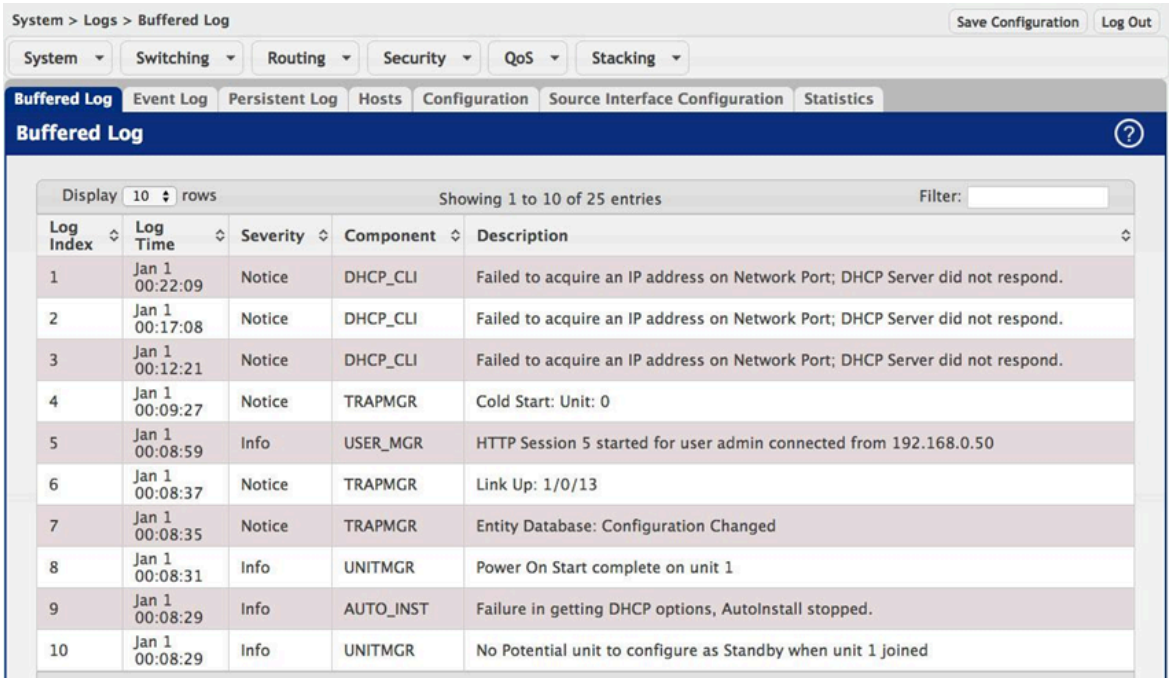
The AutoInstall feature can automatically obtain configuration information and install a new image when the switch boots. The process begins when the switch is initialized and no configuration file (startup-config) is found. If initiated, the AutoInstall feature allows the device to obtain an IP address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

Admin Mode	The current administrative mode of the AutoInstall feature: • Start — Operationally start the AutoInstall process on the switch. • Stop — Operationally stop the AutoInstall process on the switch.
Persistent Mode	If this option is selected, switch will attempt to automatically configure the device during the next boot cycle.
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.

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

2.5. System > Logs

2.5.1. System > Logs > Buffered Log



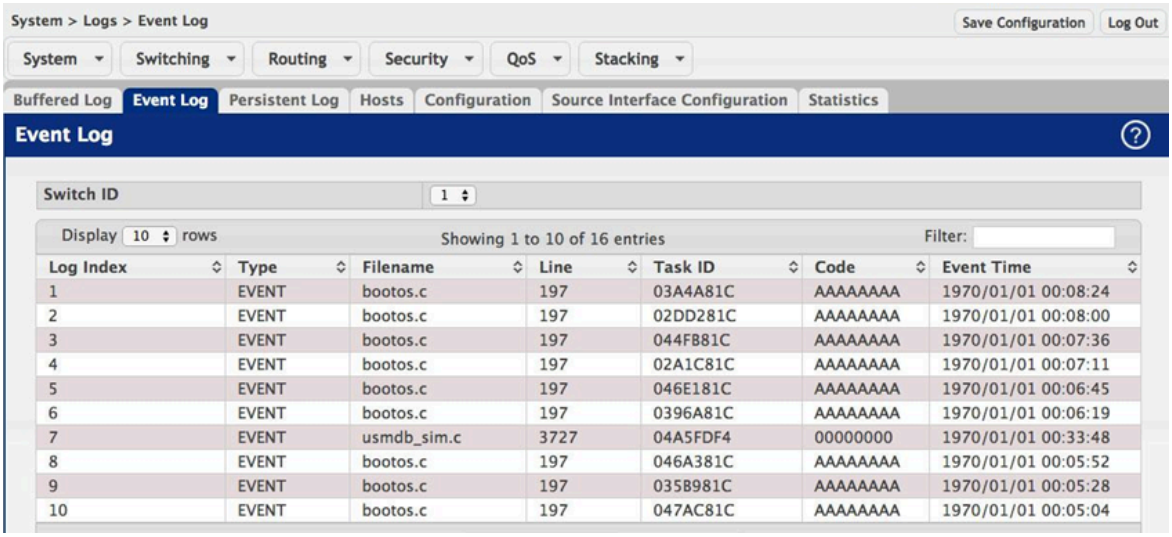
The log messages the device generates in response to events, faults, errors, and configuration changes are stored locally on the device in the RAM (cache). This collection of log files is called the RAM log or buffered log. When the buffered log file reaches the configured maximum size, the oldest message 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	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.

2.5.2. System > Logs > Event Log



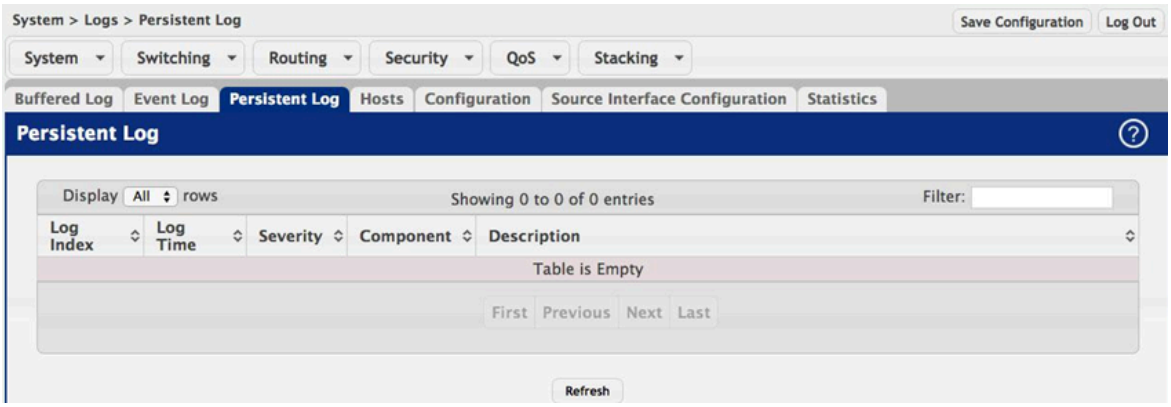
The event log contains error messages which result from catastrophic events that occur during system operation. At least two thousand (2,000) entries can be stored in the event log, although the actual number depends on the specific device hardware and operating system in use.

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.

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 (yyyy/mm/dd, hours, minutes, and seconds) indicating when the event occurred.

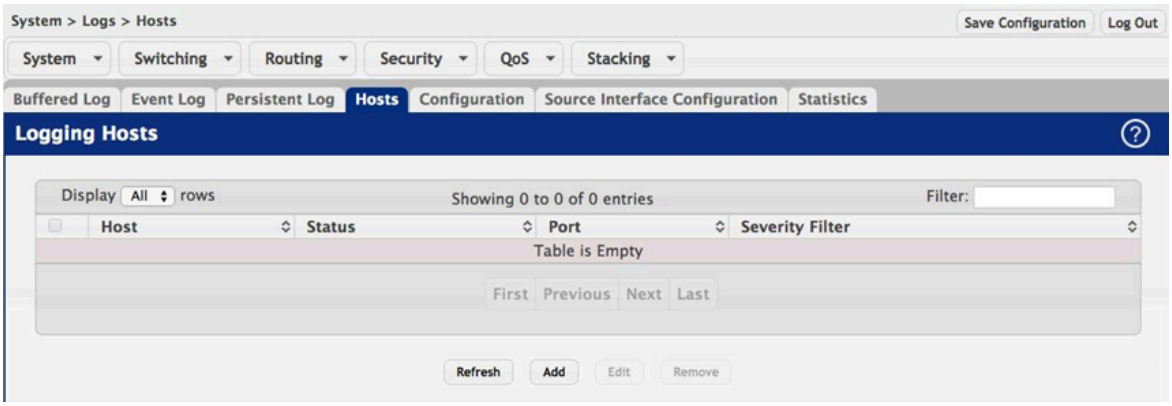
2.5.3. System > Logs > Persistent Log



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.

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.

2.5.4. System > Logs > 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.

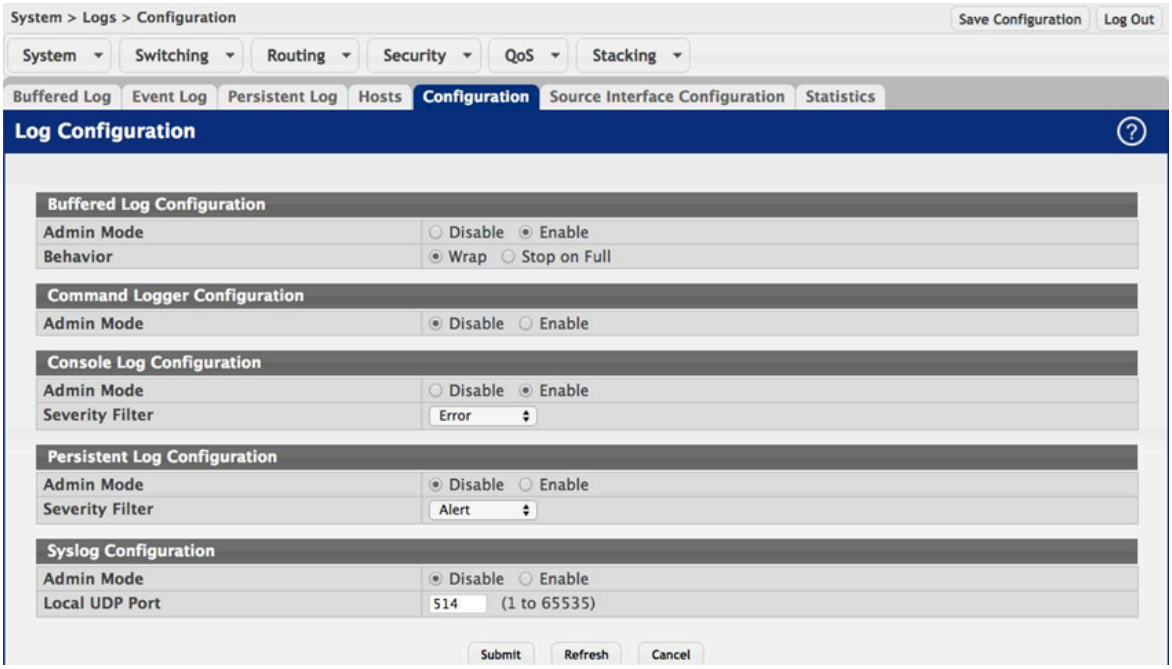
Use the buttons to perform the following tasks:

- 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.

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.

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

2.5.5. System > Logs > 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.

Table 2.12. 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).

Table 2.13. Command Logger Configuration

Admin Mode	Enable or disable logging of the command-line interface (CLI) commands issued on the device.

Table 2.14. 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.

Table 2.15. Persistent Log Configuration

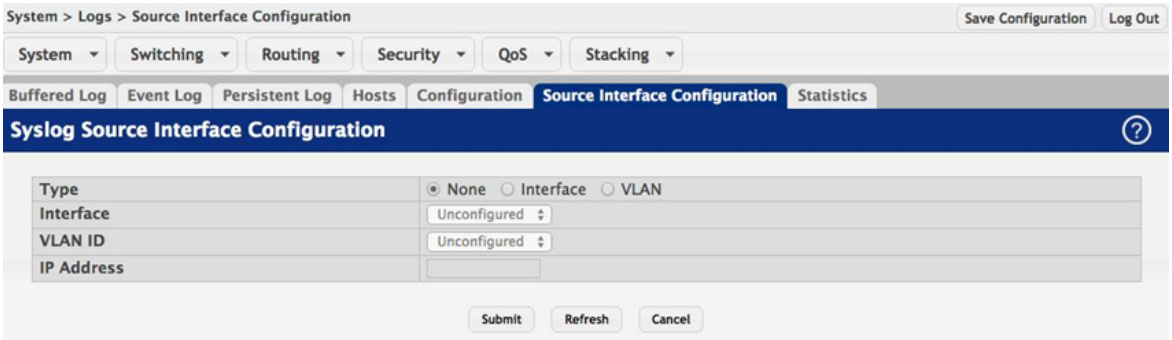
Admin Mode	Enable or disable logging to the persistent log. These messages are not deleted when the device reboots.
Severity Filter	Select the severity of the messages to be logged. All messages at and above the selected threshold are logged to the console. See the previous severity filter description for more information about each severity level.

Table 2.16. Syslog Configuration

Admin Mode	Enable or disable logging to configured syslog hosts. When the syslog admin mode is disabled the device does not relay logs to syslog hosts, and no messages will be sent to any collector/relay. When the syslog admin mode is enabled, messages will be sent to configured collectors/ relays using the values configured for each collector/relay.
Local UDP Port	The UDP port on the local host from which syslog messages are sent.

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

2.5.6. System > Logs > Source Interface Configuration



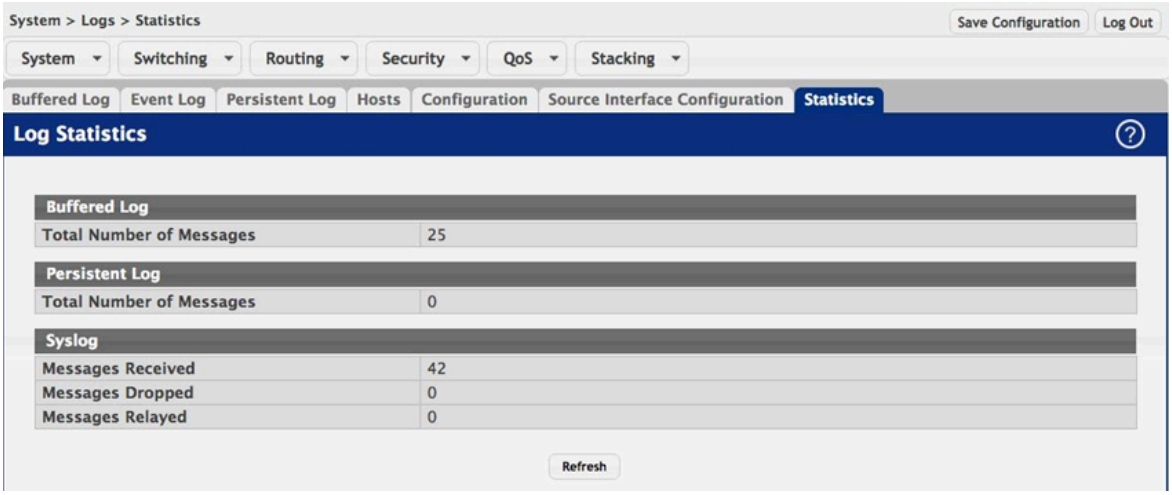
Use this page to specify the physical or logical interface to use as the logging (Syslog) client source interface. When an IP address is configured on the source interface, this address is used for all Syslog communications between the local logging client and the remote Syslog server. The IP address 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.

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.
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.
IP Address	The IP address associated with the configured Source Interface.

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

2.5.7. System > Logs > 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.

Table 2.17. Buffered Log

Total Number of Messages	The number of log messages currently stored in RAM.

Table 2.18. Persistent Log

Total Number of Messages	The number of log messages currently stored in persistent storage.

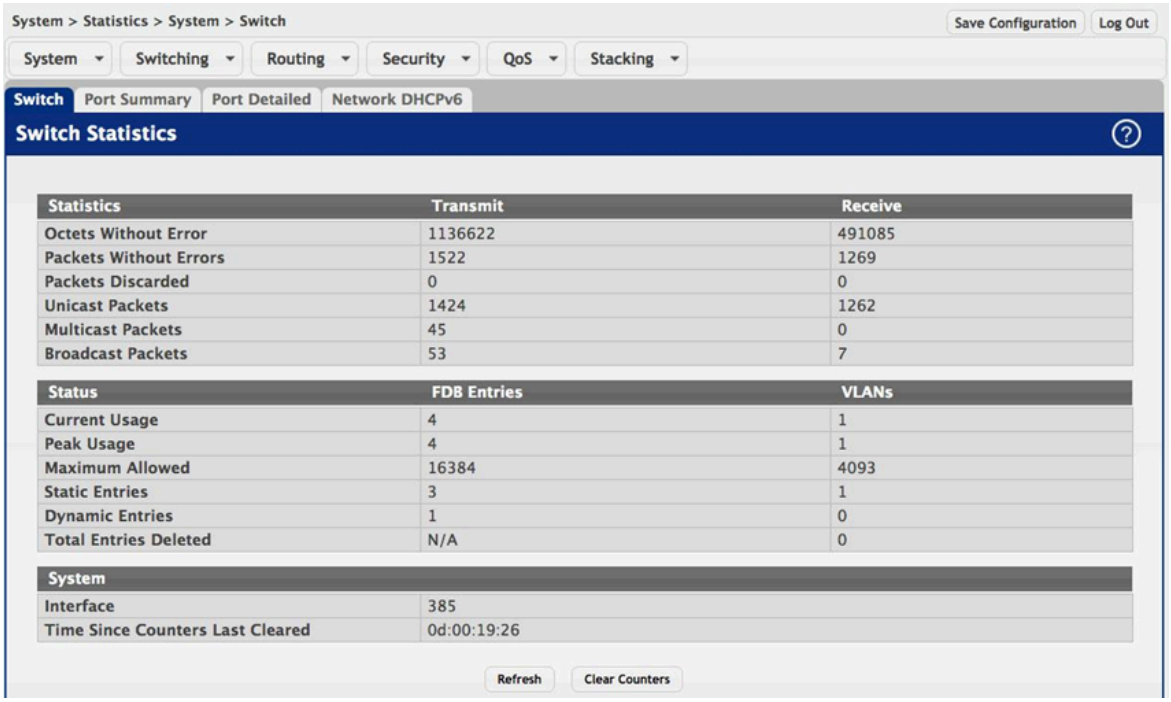
Table 2.19. Syslog

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.

2.6. System > Statistics

2.6.1. System > Statistics > System

2.6.1.1. System > Statistics > System > 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.

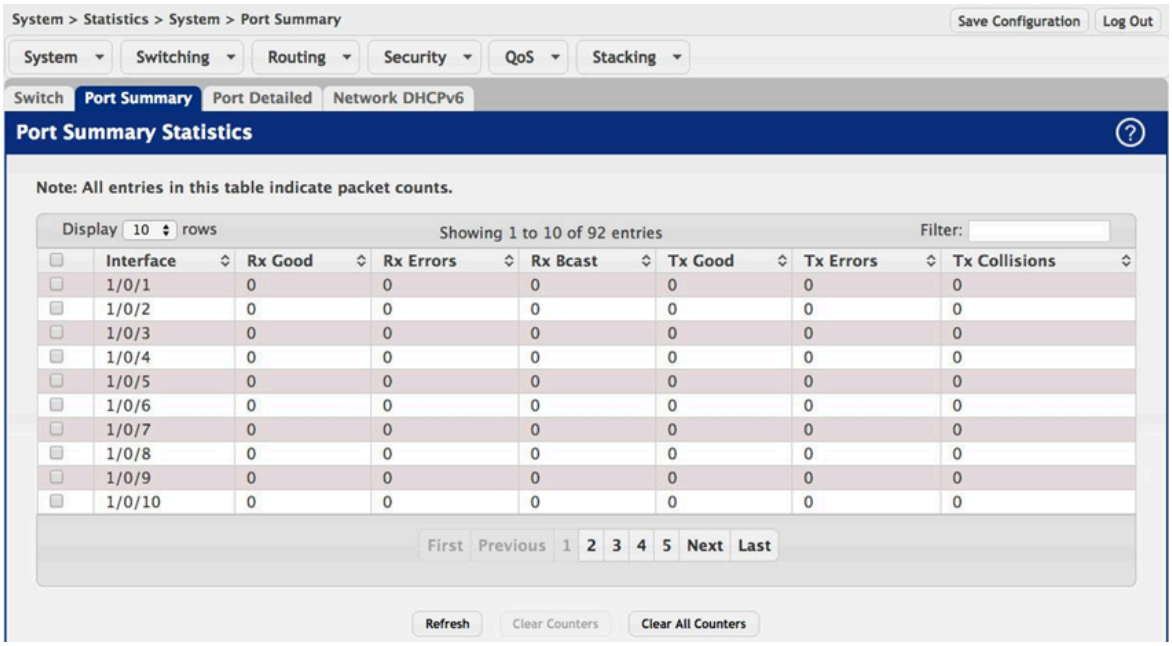
Statistics	The Statistics table shows information about the amount of various types of traffic transmitted and received by the device.
Octets Without Error	The total number of octets (bytes) of data successfully transmitted or received by the processor (excluding framing bits but including FCS octets).
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	The Status table shows summary information about entries in the MAC address table (also known as the forwarding database or FDB) and the VLAN database.
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	The System table shows the SNMP interface index for the system and the amount of time since the statistics information on the page was last reset.
Interface	The interface index object value of the interface table entry associated with the Processor of this switch. This value is used to identify the interface when managing the device by using SNMP.
Time Since Counters Last Cleared	The amount of time in days, hours, minutes, and seconds, that has passed since the statistics for this device were last reset.
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.

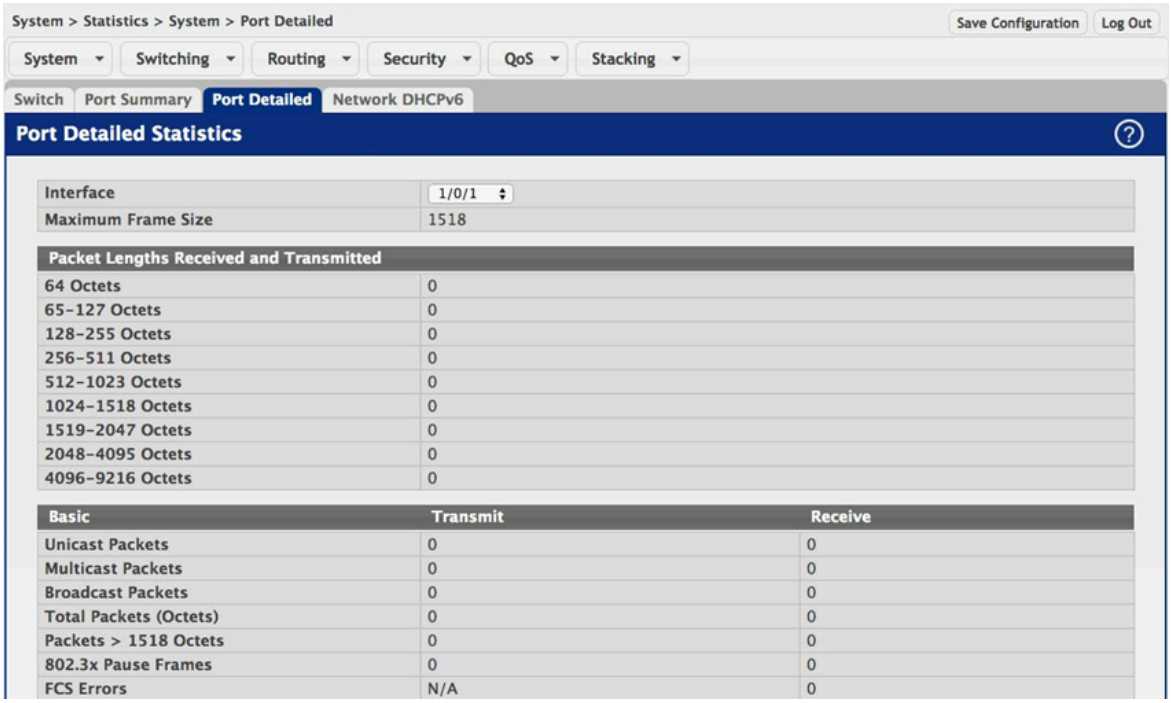
2.6.1.2. System > Statistics > System > Port Summary



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

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.

2.6.1.3. System > Statistics > System > Port Detailed



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

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.

Packet Lengths Received and Transmitted	This table shows how many packets of certain lengths have been received and transmitted by the interface.
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).
1519-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 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	This table shows basic information about the types of packets received or transmitted by the selected interface. Statistics for transmitted traffic and received traffic are shown in separate columns.
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.

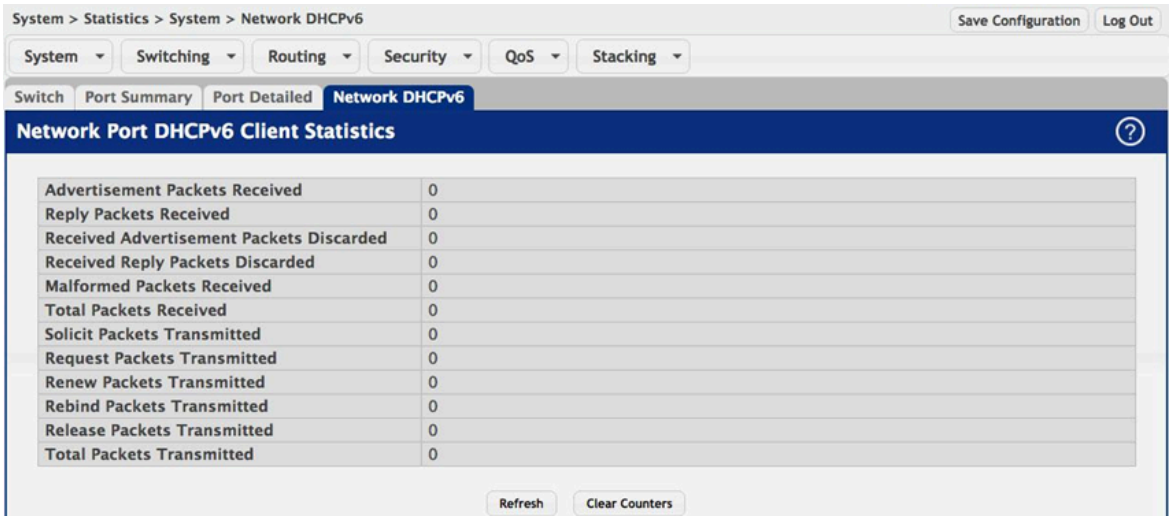
Protocol	This table shows statistics about various protocol data units (PDUs) or EAPOL frames transmitted or received by the interface. Statistics for transmitted traffic and received traffic are shown in separate columns.
STP BPDUs	The number of Spanning Tree Protocol (STP) Bridge Protocol Data Units (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.
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	This table shows statistics about problems that occurred while transmitting traffic.
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.

Advanced - Receive	This table shows statistics about problems that occurred with traffic received on the interface.
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.
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.

2.6.1.4. System > Statistics > System > Network DHCPv6



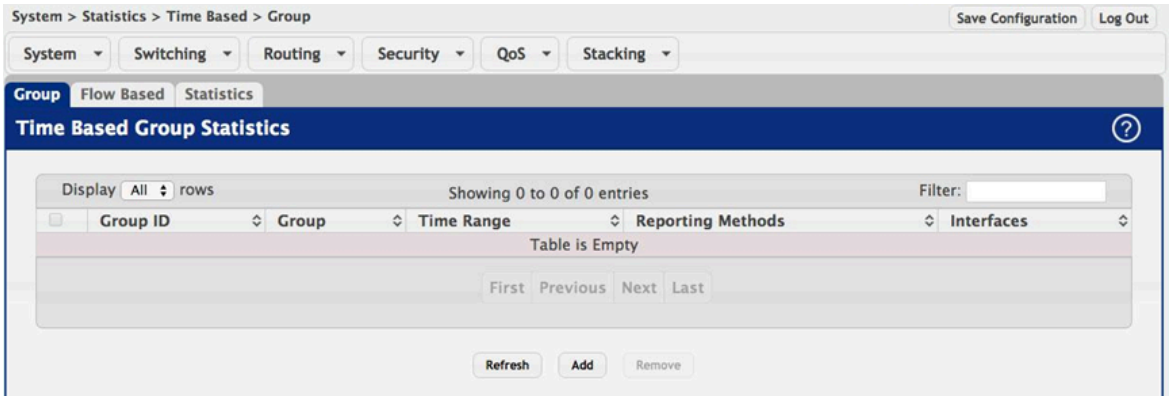
This page displays the DHCPv6 client statistics values for the network interface. The DHCPv6 client on the device exchanges several different types of UDP messages with one or more network DHCPv6 servers during the process of acquiring address, prefix, or other relevant network configuration information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

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.

2.6.2. System > Statistics > Time Based

2.6.2.1. System > Statistics > Time Based > 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:

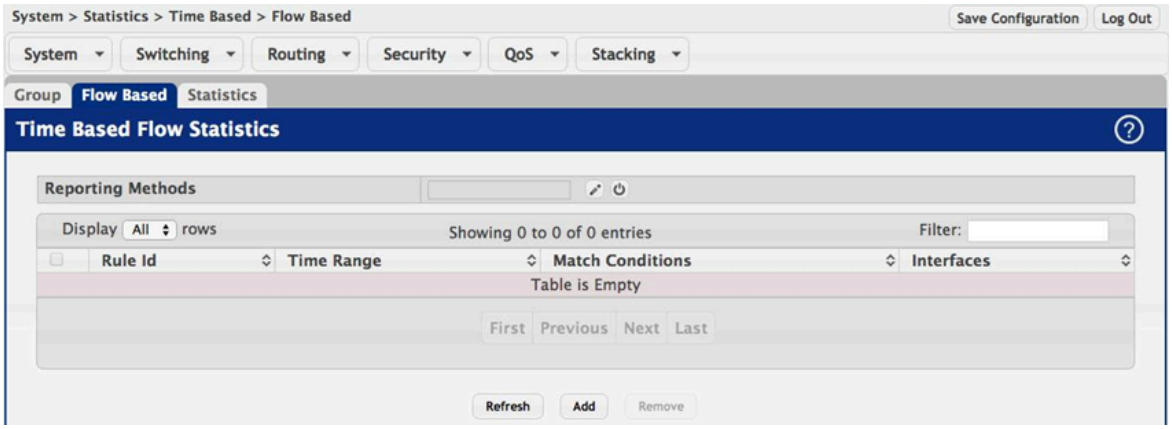
- To add a set of time-based traffic group statistics to collect, click Add and configure the desired settings.
- To delete one or more time-based statistics groups, select each entry to delete and click Remove.

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.
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.

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

2.6.2.2. System > Statistics > Time Based > 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.

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.

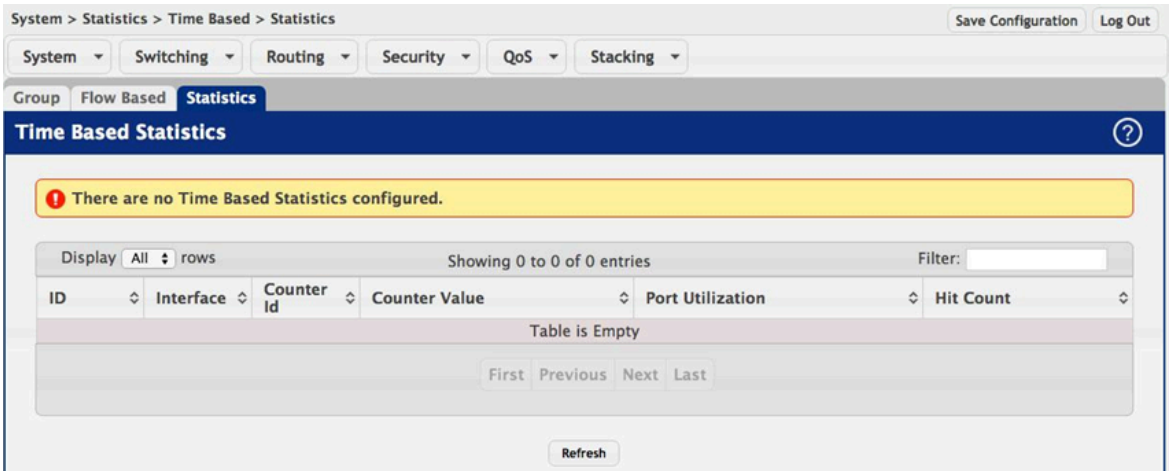
After you click Add, the Time Based Flow Configuration window opens and allows you to configure a rule for traffic flow statistics. The match conditions are optional, but the rule must specify at least one match condition. The following information describes the match criteria fields that are available 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.

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

2.6.2.3. System > Statistics > Time Based > Statistics

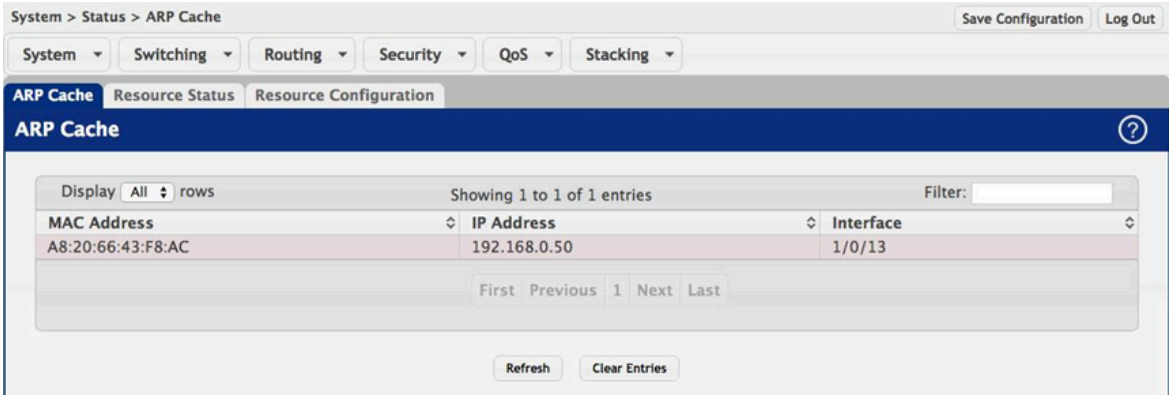


Use this page to view time-based statistics collected for the configured traffic groups and flow-based rules.

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.

2.7. System > Status

2.7.1. System > Status > 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.

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.

2.7.2. System > Status > Resource Status

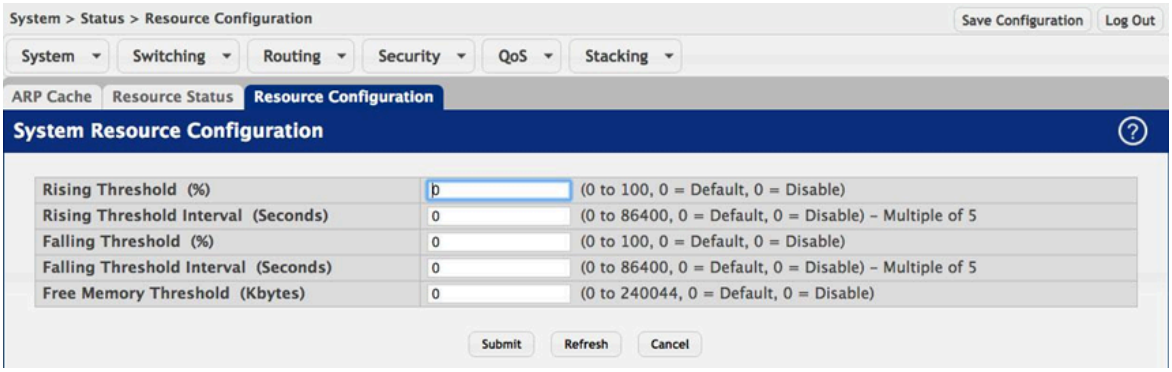
This page displays status information indicating the CPU utilization and free memory in the system.

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.

2.7.3. System > Status > Resource Configuration



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

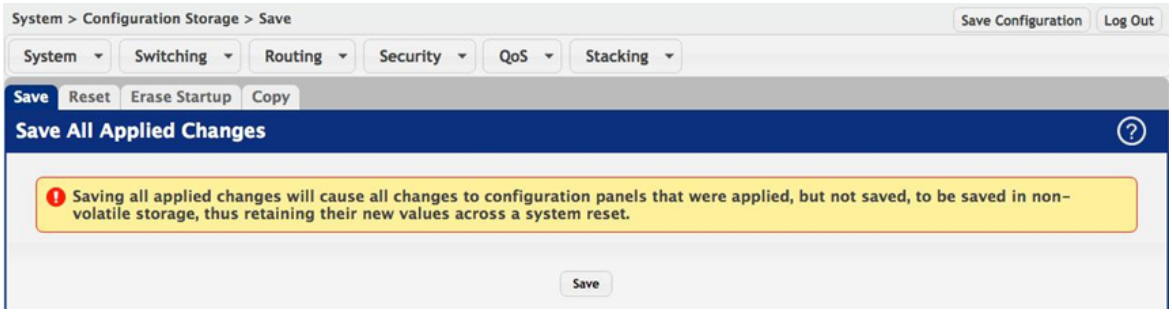
Rising Threshold	The CPU utilization rising threshold, expressed as a percentage. When the CPU utilization is increasing, an event is signaled when it reaches or exceeds this level.
Rising Threshold Interval	The CPU utilization rising threshold interval in seconds. This represents how often the current 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.

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

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

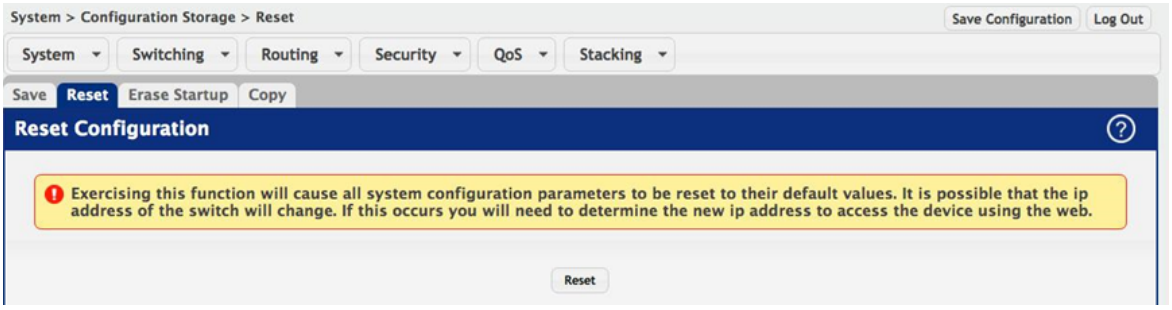
2.8. System > Configuration Storage

2.8.1. System > Configuration Storage > Save



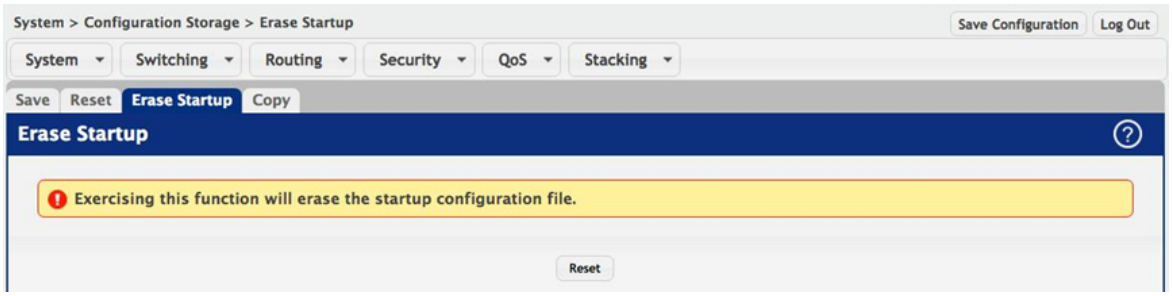
Save (Button)	Initiates a save of all system configuration after displaying a confirmation message. All of the current system configuration settings, including any that have been changed by the user, are stored into non-volatile memory so that they are preserved across a system reset.

2.8.2. System > Configuration Storage > Reset



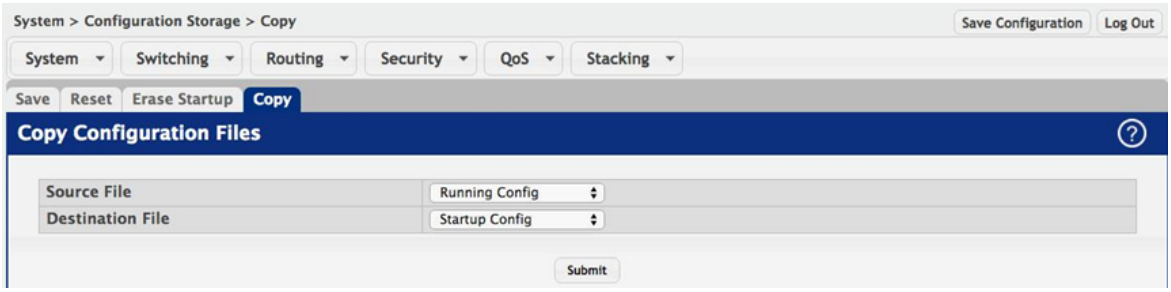
Reset (Button)	Initiates the action to reset all configuration parameters to their factory default settings after displaying a confirmation message. All configuration changes, including those that were previously saved, are reset in the running system by this action. It is possible that the ip address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

2.8.3. System > Configuration Storage > Erase Startup



Reset (Button)	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.

2.8.4. System > Configuration Storage > Copy

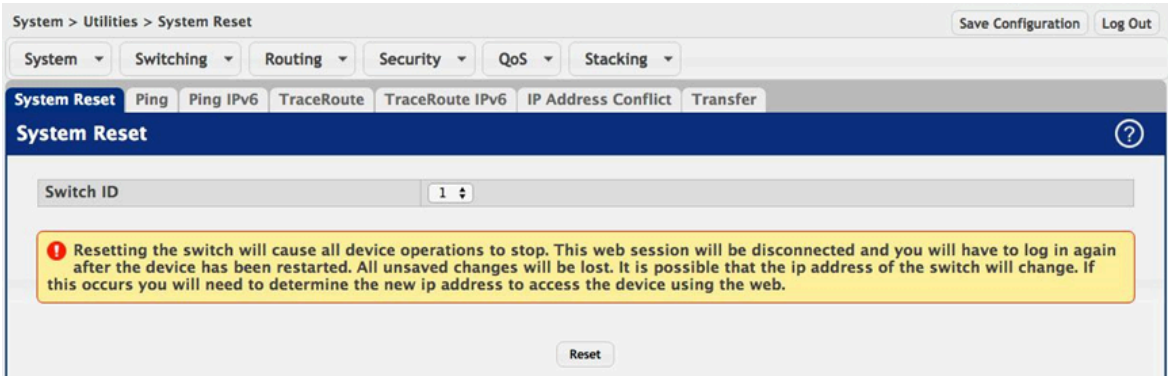


Use this page to copy the information contained in one configuration file to another configuration file on the device. When you click Submit, the copy action takes place immediately, and the source file overwrites the destination file.

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.

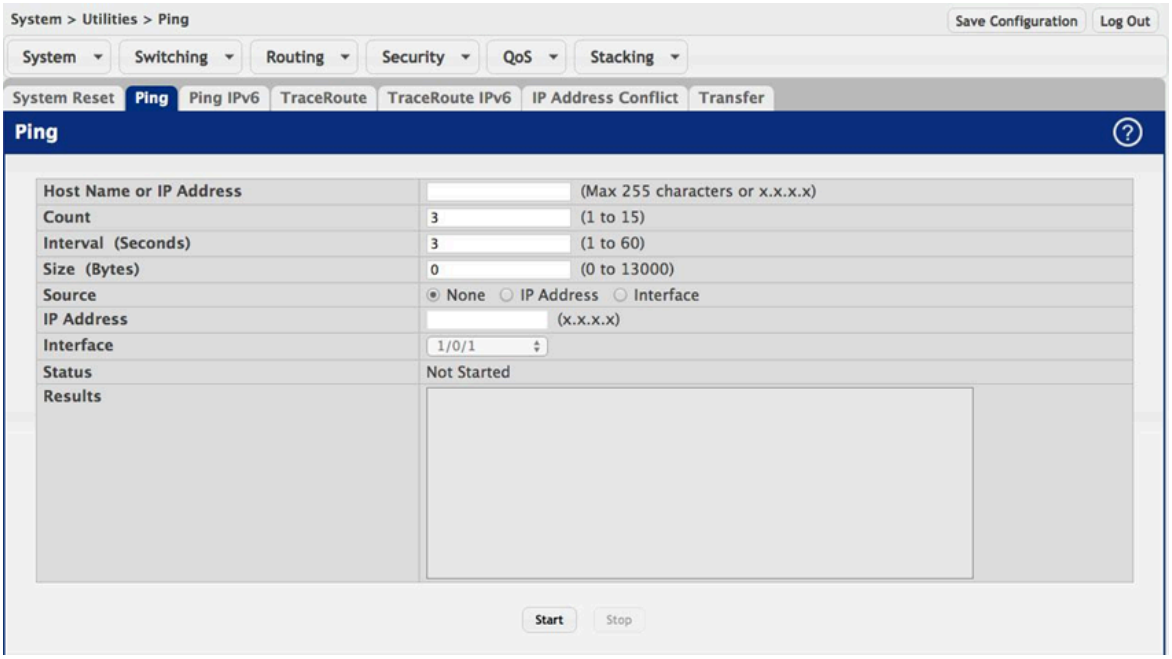
2.9. System > Utilities

2.9.1. System > Utilities > System Reset



Switch ID	Select the specific switch unit to be reset, or specify *All* to reset all units in the stack.
Reset (Button)	Initiates the system reset action after displaying a confirmation message. Note that any configuration changes made since the last successful save are lost whenever a switch is reset. It is possible that the ip address of the switch will change. If this occurs you will need to determine the new ip address to access the device using the web.

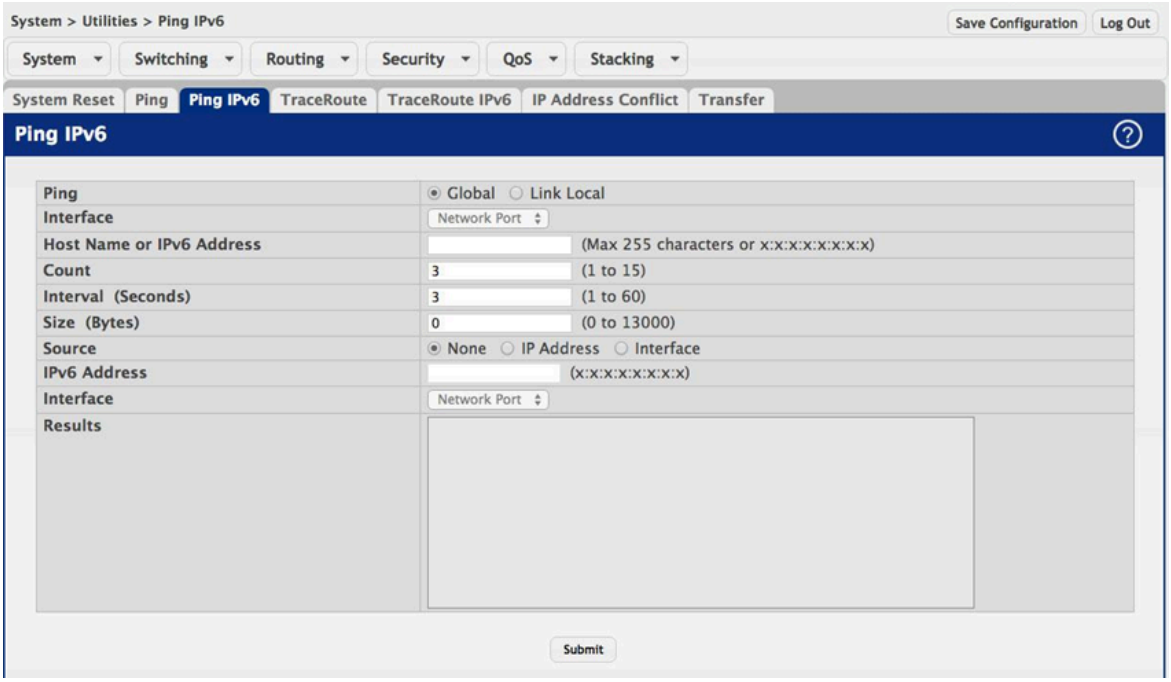
2.9.2. System > Utilities > Ping



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.

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.

2.9.3. System > Utilities > Ping IPv6

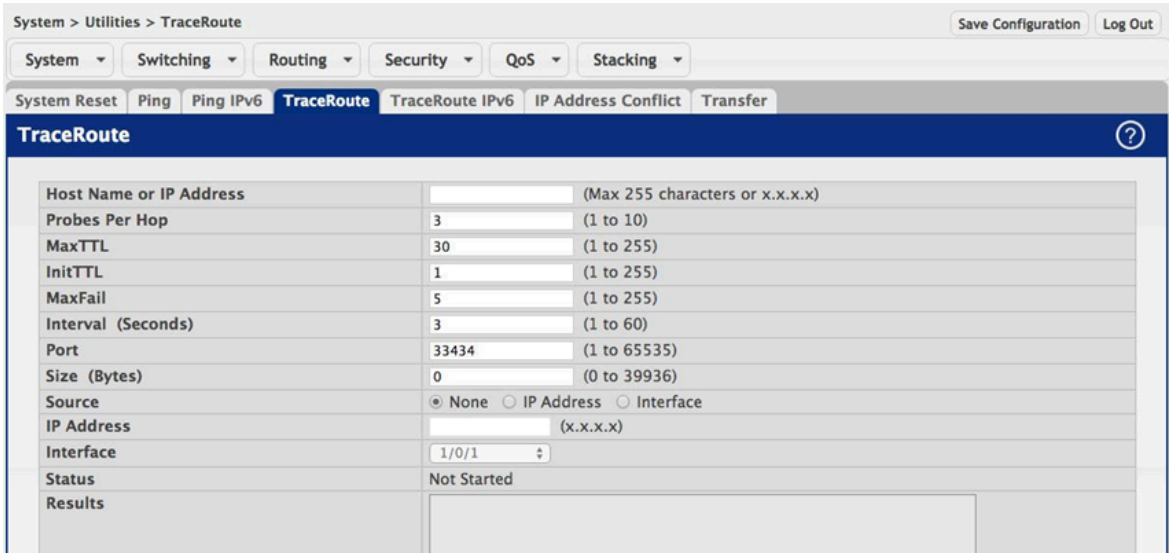


Use this page to tell the device to send one or more ping requests to a specified IPv6 host. You can use the ping request to check whether the device can communicate with a particular host on an IPv6 network. A ping request is an Internet Control Message Protocol version 6 (ICMPv6) echo request packet.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

Ping	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.

2.9.4. System > Utilities > TraceRoute



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

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.

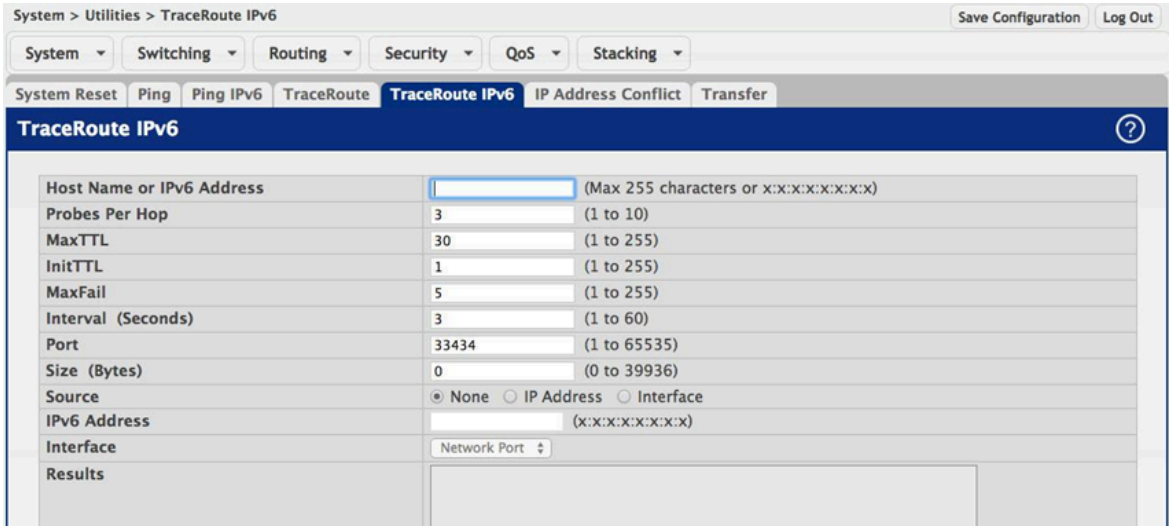
An error code may be printed with the response time for each probe. The error codes signify that either no response was received or an ICMP Destination Unreachable message was received with error codes as follows:

- * 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.

2.9.5. System > Utilities > TraceRoute 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.

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	Specifies the time between probes, in Seconds. If a response is not received within this interval, then traceroute considers the probe a failure

	and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately.
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`

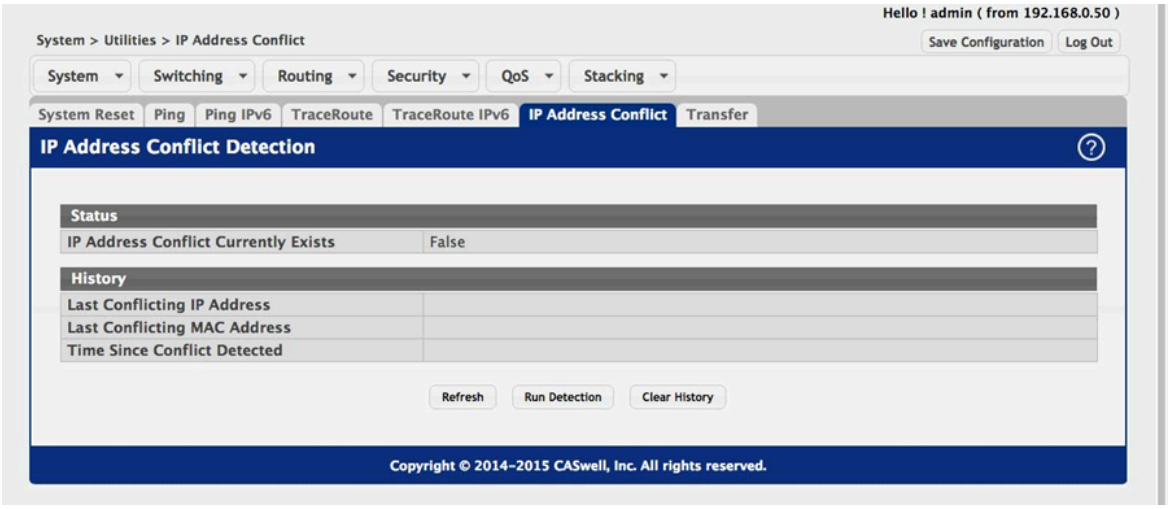
For each TTL value probed, the results show the IP address of the router that responded to the probes and the response time for each probe. If no response is received for probes with a particular TTL, the IP address is reported as 0.0.0.0.

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.

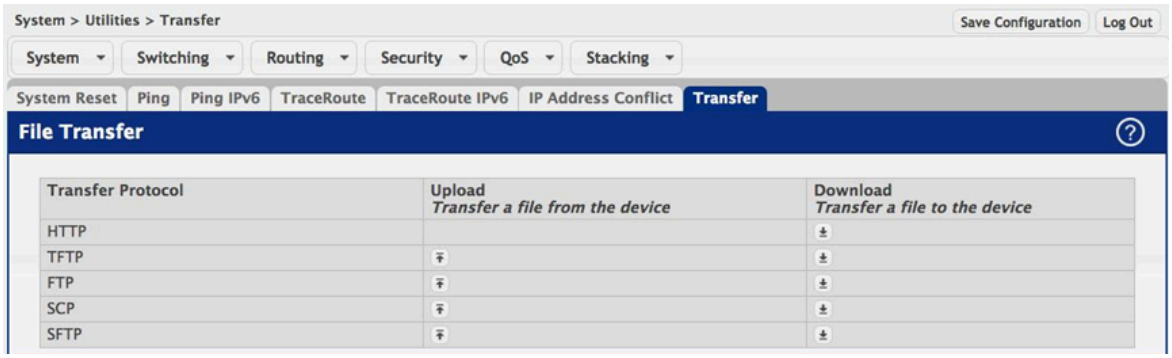
2.9.6. System > Utilities > IP Address Conflict



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 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

2.9.7. System > Utilities > 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.

Transfer Protocol	The protocol to use to transfer the file. Files can be transferred from the device to a remote system using TFTP, FTP, SCP or SFTP. Files can be transferred from a remote system to the device using HTTP, TFTP, FTP, SCP or SFTP.
Upload	To transfer a file from the device to a remote system using TFTP, FTP, SCP or SFTP, click the upload icon in the same row as the desired transfer protocol. The File Upload window appears. Configure the information for the file transfer (described below), and click the upload icon to the right of the Progress field to begin the transfer.
Download	To transfer a file from a remote system to the device using HTTP, TFTP, FTP, SCP or SFTP, click the download icon in the same row as the desired transfer protocol. The File Download window appears. Configure the information for the file transfer (described below), and click the download icon to the right of the Progress field to begin the transfer.

After you click the upload icon, the File Upload window appears. The following information describes the fields in the File Upload window for all protocols.

File Type	Specify the type of file to transfer from the device to a remote system. • Code – Select this option to transfer an 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 (backup-config) 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 FTP, SCP and SFTP transfers, if the server requires authentication, specify the user name for remote login to the server that will receive the file.
Password	For FTP, SCP and SFTP transfers, if the server requires authentication, specify the password for remote login to the server that will receive the file.
Progress	Represents the completion percentage of the file transfer. The file transfer begins after you complete the required fields and click the upload icon to the right of this field.
Status	Provides information about the status of the file transfer.

After you click the download icon, the File Download window appears. The following information describes the fields in the File Download window for all protocols.

File Type	Specify the type of file to transfer to the device: • 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 configuration file (startup-config). 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. • 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. 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.

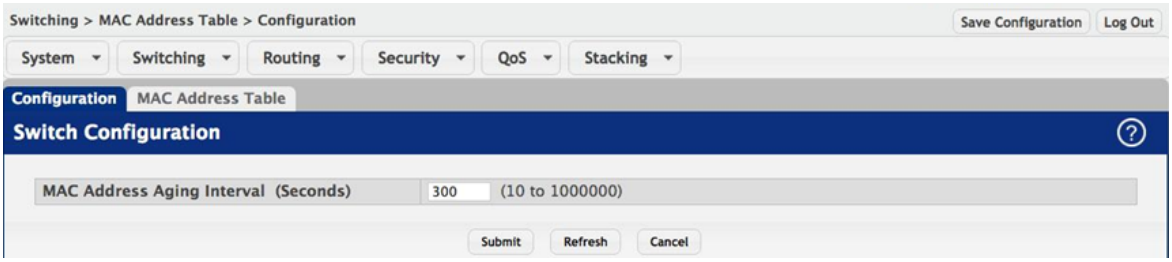
Server Address	For TFTP, FTP, SCP or SFTP transfers, specify the IPv4 address, IPv6 address, or DNS-resolvable hostname of the remote server.
File Path	For TFTP, FTP, SCP or SFTP transfers, specify the path on the server where the file is located.
File Name	For TFTP, FTP, SCP or SFTP transfers, specify the name of the file you want to transfer to the device.
User Name	For FTP, SCP or SFTP transfers, if the server requires authentication, specify the user name for remote login to the server where the file resides.
Password	For FTP, SCP or SFTP transfers, if the server requires authentication, specify the password for remote login to the server where the file resides.
Progress	Represents the completion percentage of the file transfer. The file transfer begins after you complete the required fields and click the download icon to the right of this field.
Status	Provides information about the status of the file transfer.

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

Chapter 3. Switching

3.1. Switching > MAC Address Table

3.1.1. Switching > MAC Address Table > Configuration

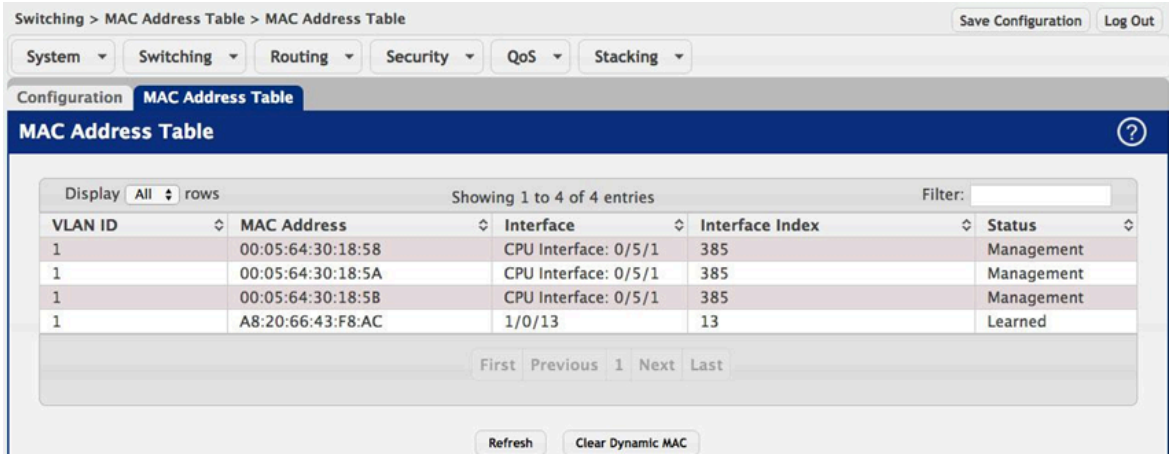


Use this page to configure the MAC address aging timeout for the forwarding database.

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.

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

3.1.2. Switching > MAC Address Table > MAC Address Table



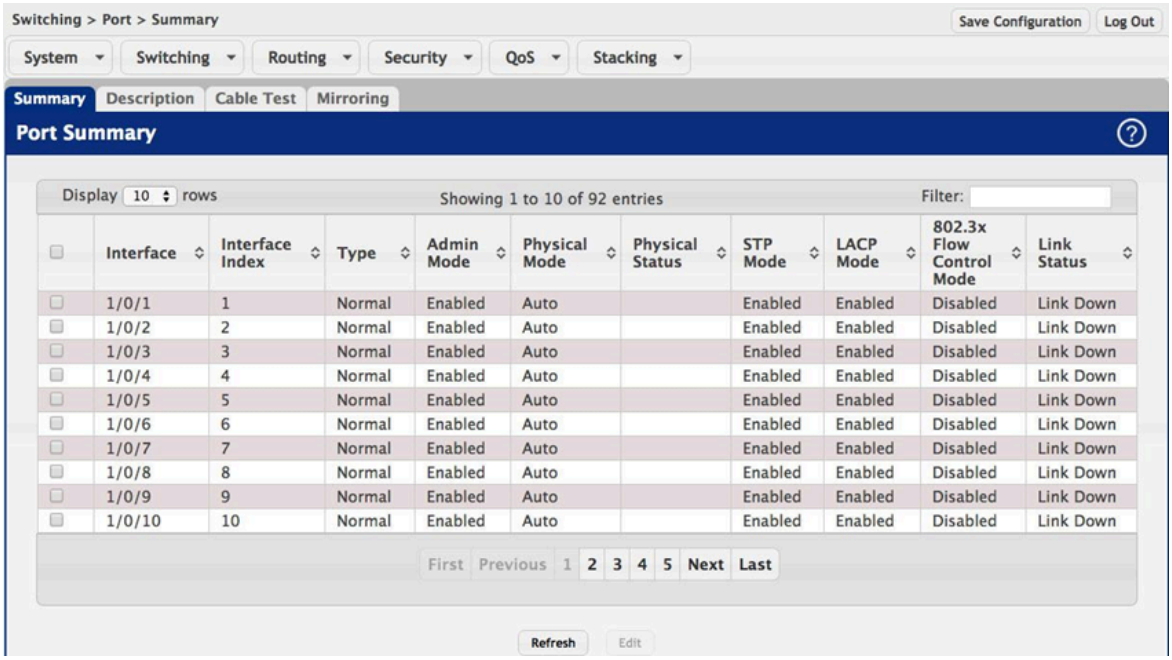
The MAC address table keeps track of the Media Access Control (MAC) addresses that are associated with each port. This table allows the device to forward unicast traffic through the appropriate port. The MAC address table is sometimes called the bridge table or the forwarding database.

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.

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.

3.2. Switching > Port

3.2.1. Switching > Port > 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.

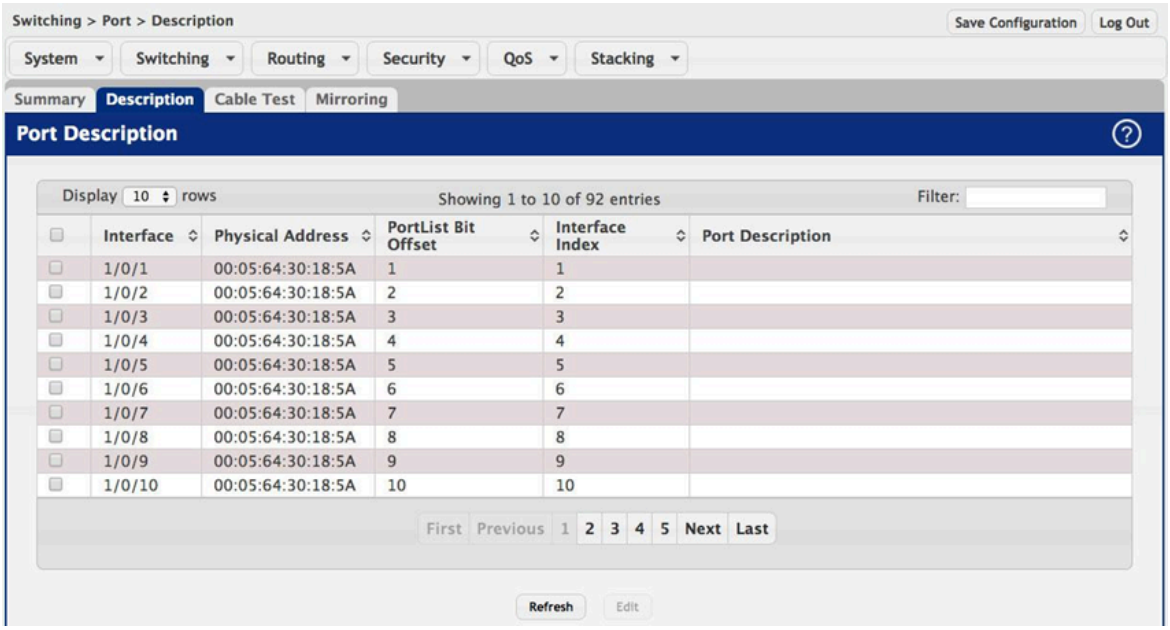
Interface	Identifies the port or LAG.
Interface Index	The interface index object value assigned by the IF-MIB. This value is used to identify the interface when managing the device by using SNMP.
Type	The interface type, which is one of the following: • Normal - The port is a normal port, which means 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	The port speed and duplex mode. If the mode is Auto, the port's maximum capability are advertised, and the duplex mode and speed are set from the auto-negotiation process. The physical mode for a LAG is reported as "LAG."

Physical Status	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.
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 is 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.
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.
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.

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.
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.
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.

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

3.2.2. Switching > Port > Description



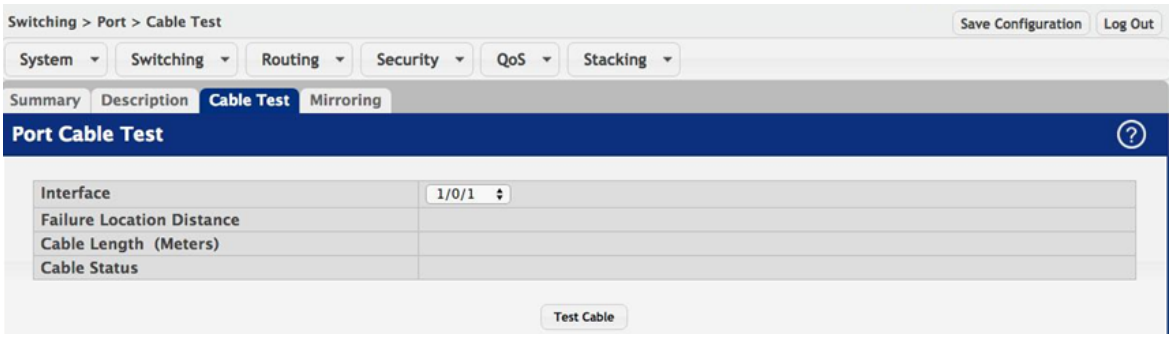
Use this page to view information that helps identify each interface. Also, the description field associated with the port(s) or LAG(s) on the device can be edited.

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.

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

3.2.3. Switching > Port > Cable Test

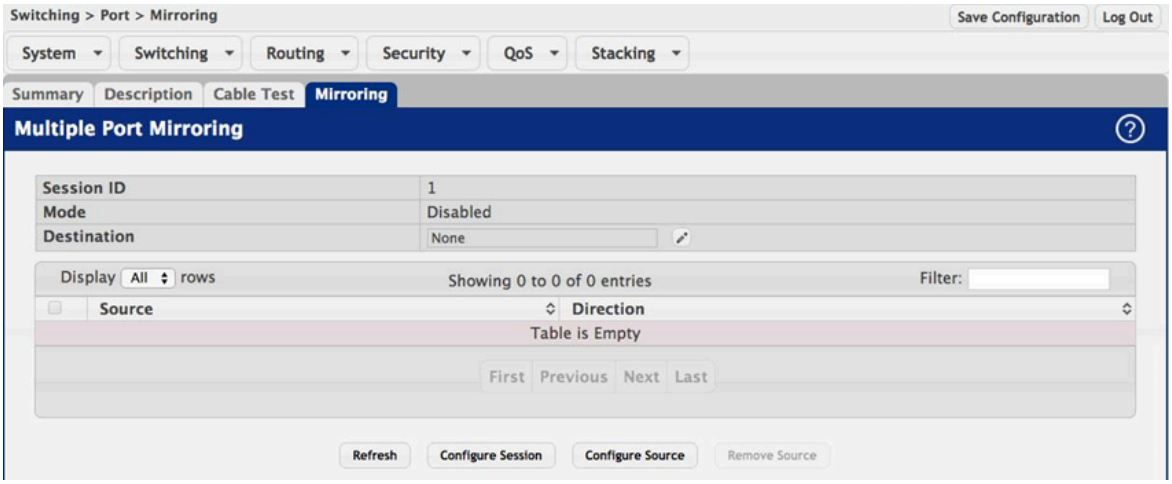


Use this page to test the cable connected to a port on the device. The cable test uses Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested.

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. 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. 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. 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.

3.2.4. Switching > Port > 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. 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, 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.

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.
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.

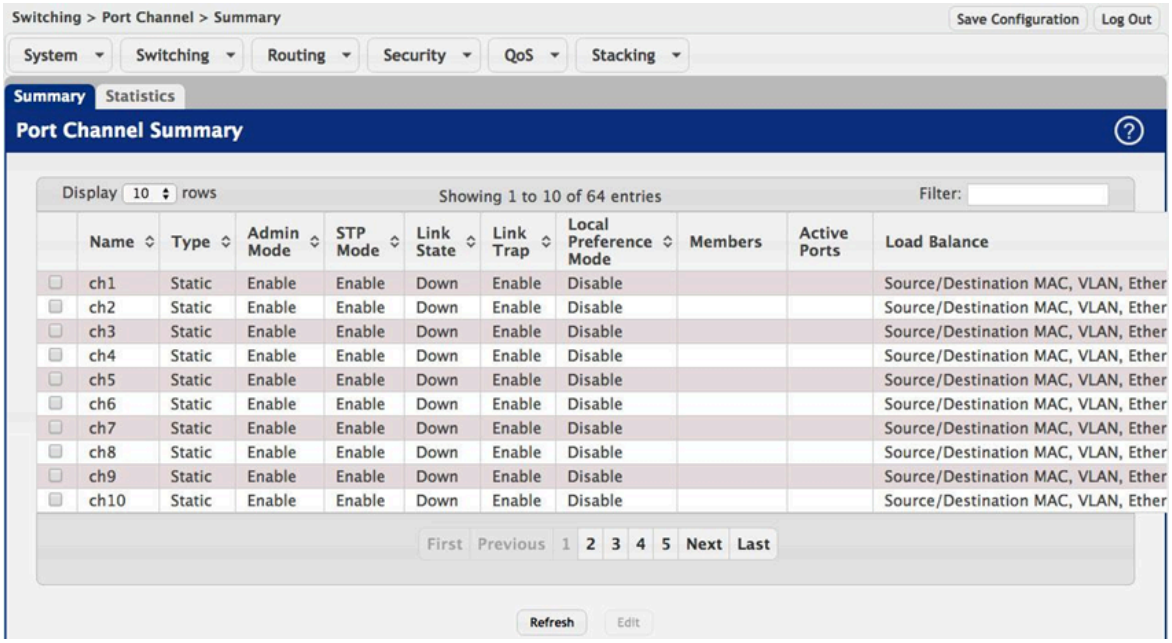
Type	The type of interface to use as the source, which is one of the following: • None – The source is not configured. • Remote VLAN – The VLAN configured as the RSPAN VLAN is the source. In an RSPAN configuration, the remote VLAN is the source

	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.

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

3.3. Switching > Port Channel

3.3.1. Switching > Port Channel > 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.

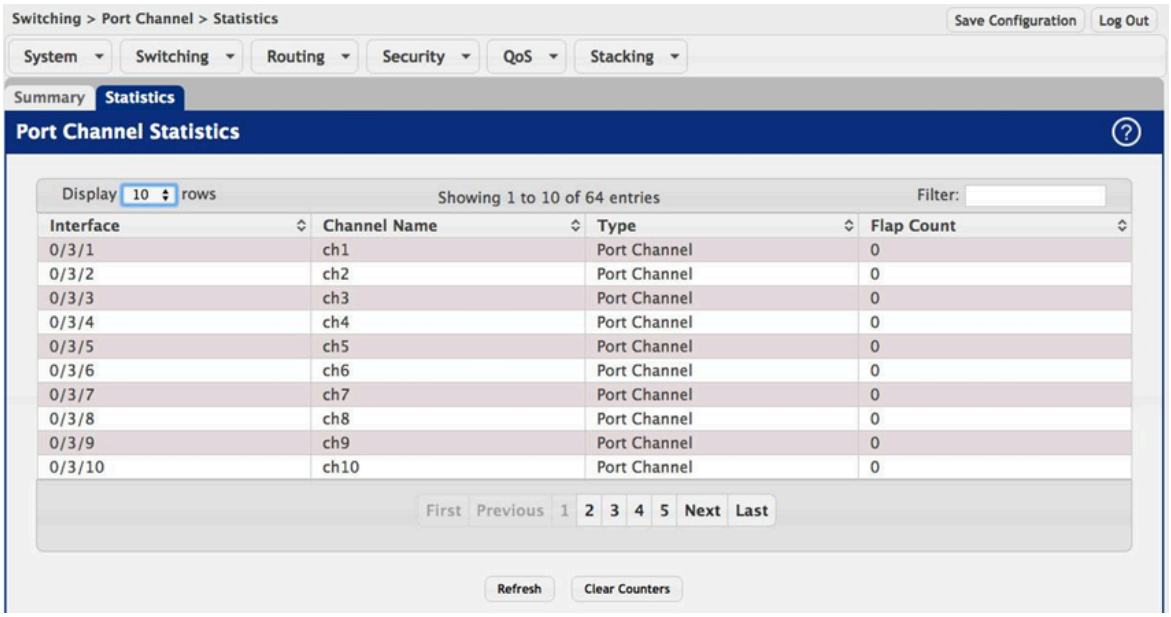
Name	A unique name to identify the port channel. Depending on the type of port channel, this name is automatically assigned by the system or can be configured by a system administrator.
Type	The type of port channel: • Dynamic – Uses Link Aggregation Control Protocol (LACP) Protocol Data Units (PDUs) 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.

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.
Local Preference Mode	The local preference mode for the port channel: • Enabled – Known unicast traffic that is destined for a LAG egresses only out of members (if it has any) of the LAG interface on the local unit. This ensures that the LAG-destined known unicast traffic does not cross the external stack link when the LAG has members on the local unit. Unknown unicast, broadcast and multicast traffic behavior remains unchanged. • Disabled – Known unicast traffic that is destined for a LAG may egress out of any of the member ports depending upon the traffic pattern and the configured LAG hashing algorithm for the LAG interface. It is possible that this traffic may egress out of a member port on another unit. In this case, the traffic has to cross the external stacking link, which results in unnecessary bandwidth utilization of the external stack link.
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

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

3.3.2. Switching > Port Channel > Statistics



This page displays the flap count for each port channel and their member ports. A flap occurs when a port-channel interface or port-channel member port goes down.

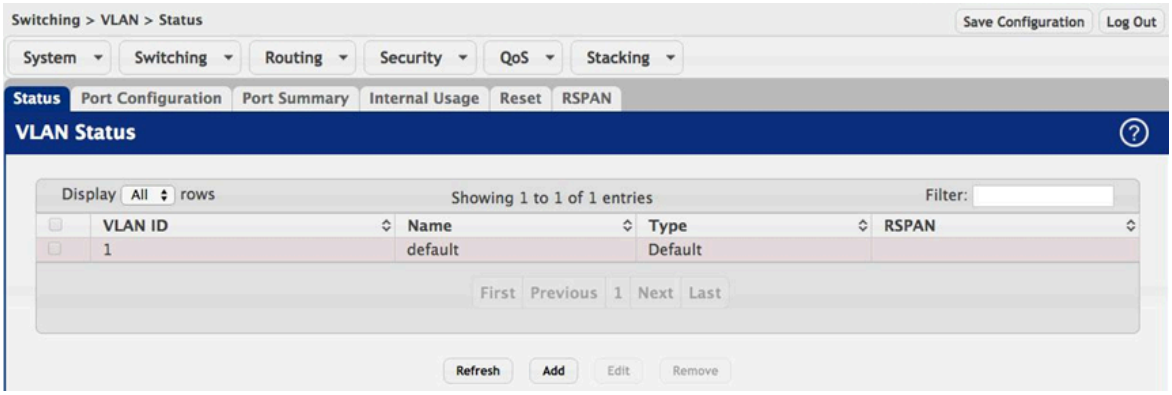
Interface	The port channel or member port (physical port) associated with the rest of the data in the row.
Channel Name	The port channel name associated with the port channel. For a physical port, this field identifies the name of the port channel of which the port is a member.
Type	The interface type, 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.

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

3.4. Switching > VLAN

3.4.1. Switching > VLAN > 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.

You cannot remove or rename VLAN 1.

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.

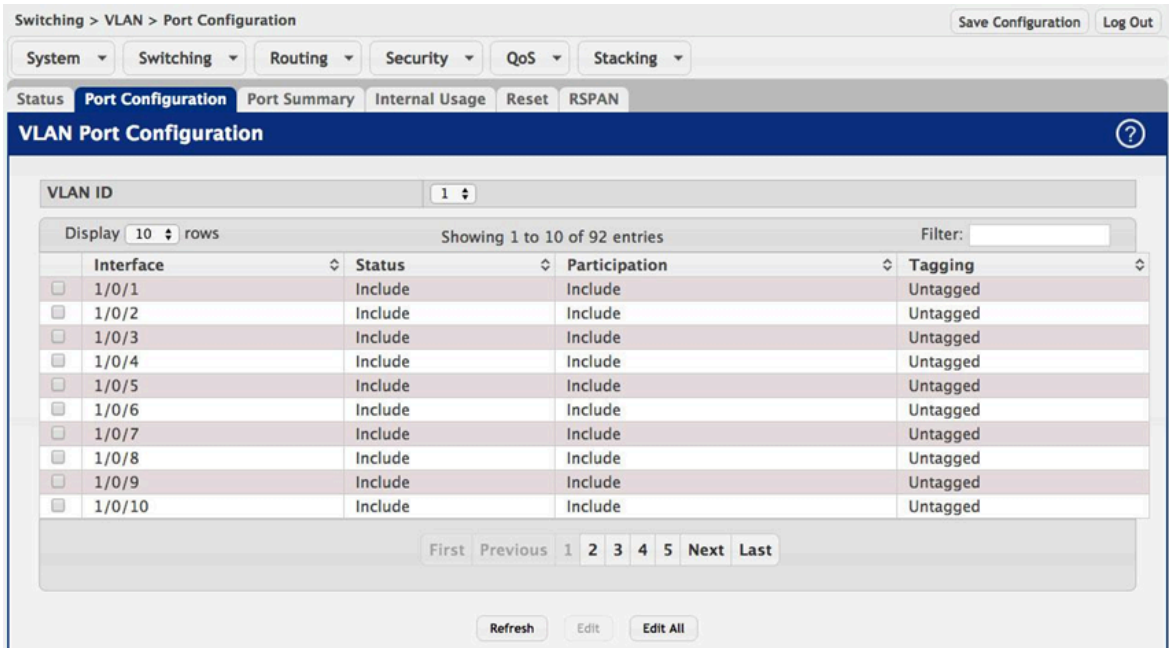
VLAN ID or Range	Specify VLAN ID(s). Use - to specify a range and , to separate VLAN IDs or VLAN ranges in the list.

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

Name	For static VLANs, specify a name for the VLAN. This field is optional and is used to help identify the VLAN. This field is not available for other VLAN types.
Convert VLAN Type to Static	For dynamic VLANs, select this option to convert the dynamic VLAN to a static VLAN. This option is not available for other VLAN types. A dynamic VLAN is learned by using GVRP, which is an industry-standard protocol that propagates VLAN information from one network device to another. GVRP can also remove dynamic VLANs. If you convert a dynamic VLAN to a static VLAN, it cannot be removed by GVRP.

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

3.4.2. Switching > VLAN > 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.

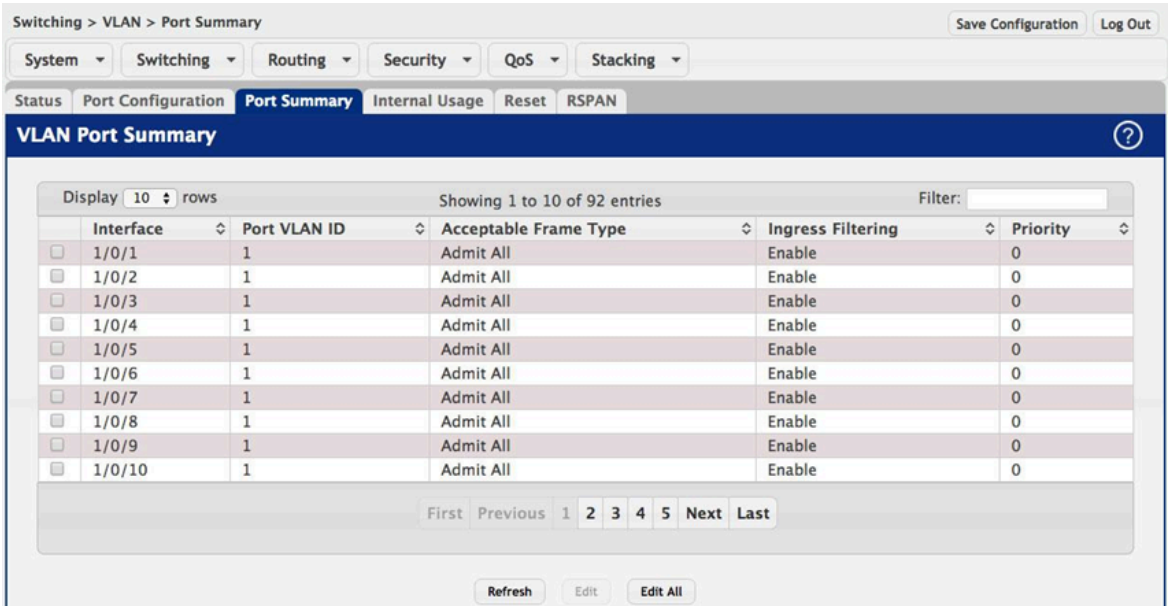
To configure VLAN membership and tagging settings for one or more interfaces, select the appropriate VLAN from the VLAN ID menu and use the buttons to perform the following tasks:

- 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 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. • Dash – The port is configured with Private VLAN. It can’t be modified on VLAN Port Config Page.
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.

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

3.4.3. Switching > VLAN > 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:

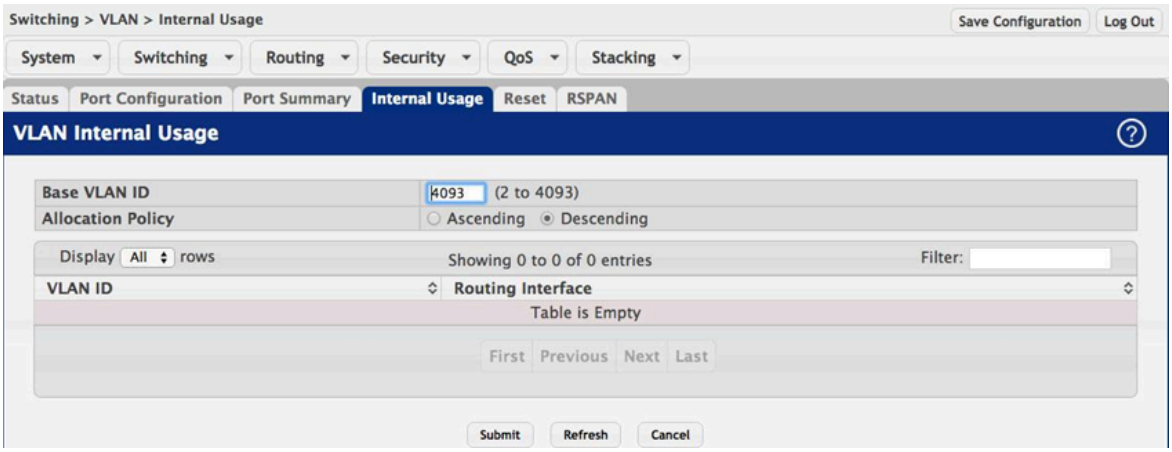
- To configure the settings for one or more interfaces, select each entry to modify and click Edit.
- To apply the same settings to all interfaces, click Edit All.

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: • Enable – A tagged frame is discarded if this interface is not a member of the VLAN identified by the VLAN ID in the tag. • Disable – All tagged frames are accepted.
Priority	The default 802.1p priority assigned to untagged packets arriving at the interface.

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

3.4.4. Switching > VLAN > Internal Usage

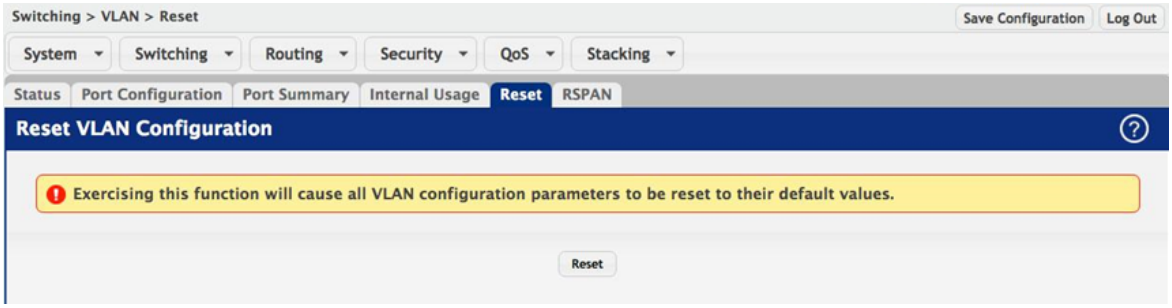


Use this page to configure which VLAN IDs to use for port-based routing interfaces. When a port-based routing interface is created, an unused VLAN ID is assigned internally. This page also displays a list of VLANs assigned to routing interfaces.

Base VLAN ID	The first VLAN ID to be assigned to a port-based routing interface.
Allocation Policy	Determines whether VLAN IDs assigned to port-based routing interfaces start at the base and decrease in value (Descending) or start at the base and increase in value (Ascending).
VLAN ID	The VLAN ID assigned to a port-based routing interface. The device automatically assigns an unused VLAN ID when the routing interface is created.
Routing Interface	The port-based routing interface associated with the VLAN.

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

3.4.5. Switching > VLAN > Reset

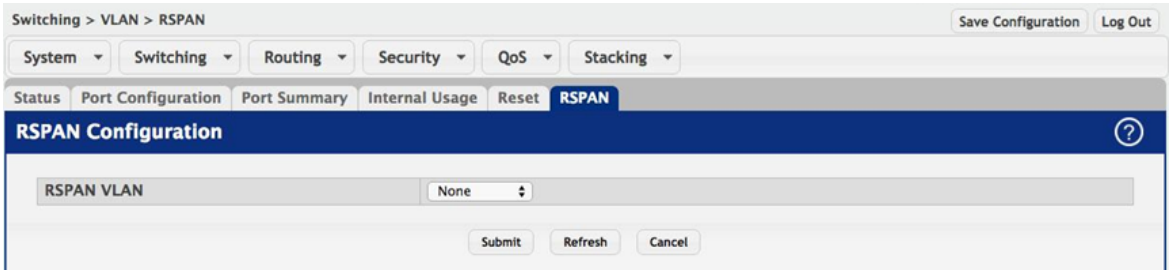


Use this page to reset all VLAN settings to their default values. Any VLANs that have been created on the system will be deleted.

Reset (Button)	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.

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

3.4.6. Switching > VLAN > RSPAN



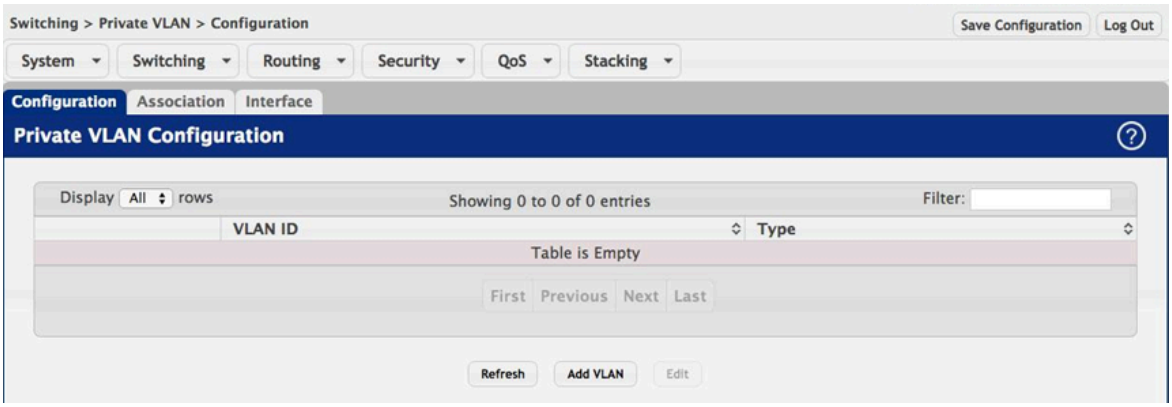
Use this page to configure the VLAN to use as the Remote Switched Port Analyzer (RSPAN) VLAN. RSPAN allows you to mirror traffic from multiple source ports (or from all ports that are members of a VLAN) from different network devices and send the mirrored traffic to a destination port (a probe port connected 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.

RSPAN VLAN	The menu includes all VLANs on the device. Select the VLAN to use as the RSAN VLAN.

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

3.5. Switching > Private VLAN

3.5.1. Switching > Private VLAN > 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.

The default VLAN and management VLAN are not displayed on the page because they cannot be configured as private VLANs.

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.

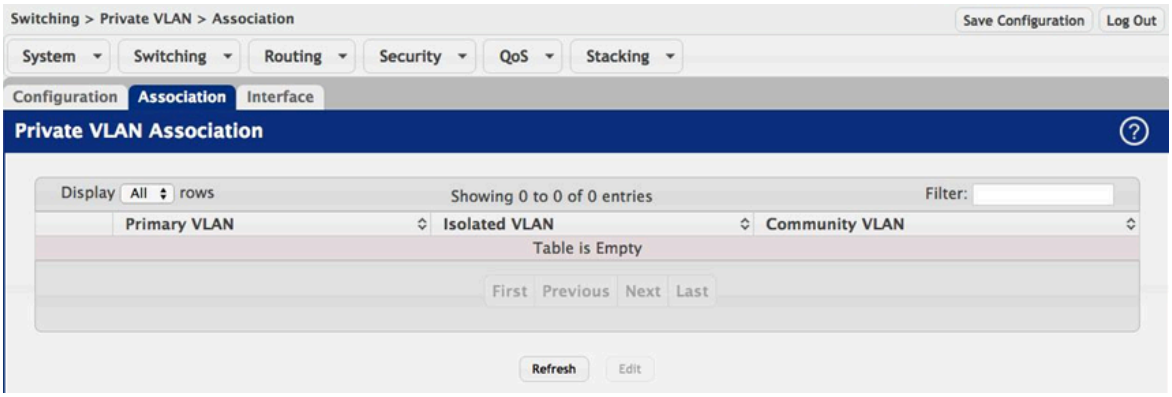
	• Community – A secondary VLAN that forwards traffic between ports that belong to the same community and to the promiscuous ports. Multiple community VLANs can be configured per private VLAN.

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.

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.

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

3.5.2. Switching > Private VLAN > Association



Use this page to configure the association between the primary VLAN and secondary VLANs. Associating a secondary VLAN with a primary VLAN allows host ports in the secondary VLAN to communicate outside the private VLAN. To configure a primary VLAN association, select the entry to modify and click Edit.

Isolated VLANs and Community VLANs are collectively called Secondary VLANs.

Primary VLAN	The VLAN ID of each VLAN configured as a primary VLAN.
Isolated VLAN	The VLAN ID of the isolated VLAN associated with the primary VLAN. If the field is blank, no isolated VLAN has been associated with the primary VLAN. An isolated VLAN is a secondary VLAN that carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN.

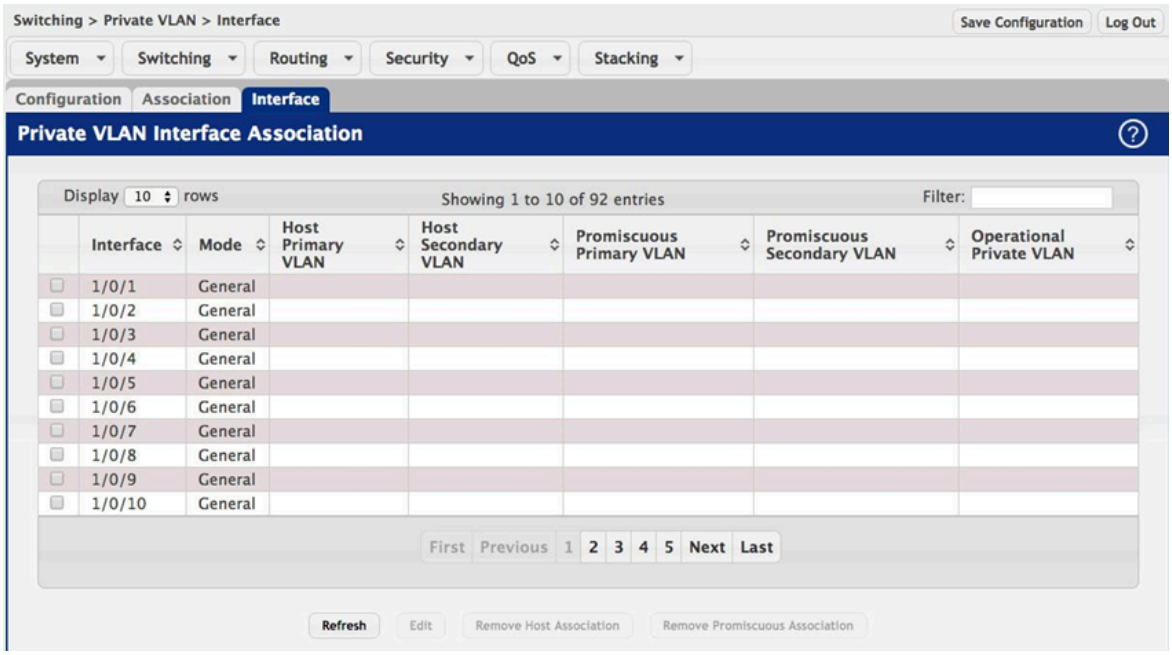
Community VLAN	The VLAN ID of each community VLAN associated with the primary VLAN. If the field is blank, no community VLANs have been associated with the primary VLAN. A community VLAN is a secondary VLAN that forwards traffic between ports that belong to the same community and to the promiscuous ports. Multiple community VLANs can be configured per private VLAN.

After you click Edit, the Edit Private VLAN Association window opens and allows you to create associations with the selected primary VLAN. The following information describes the field in this window.

Secondary VLAN	The isolated or community VLANs that can be associated with the primary VLAN. Secondary VLANs that are already associated with a primary VLAN do not appear in the list and cannot be associated with another primary VLAN. To select multiple secondary VLANs, Ctrl + click each VLAN to associate with the primary VLAN.

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

3.5.3. Switching > Private VLAN > 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.

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.

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

3.6. Switching > GARP

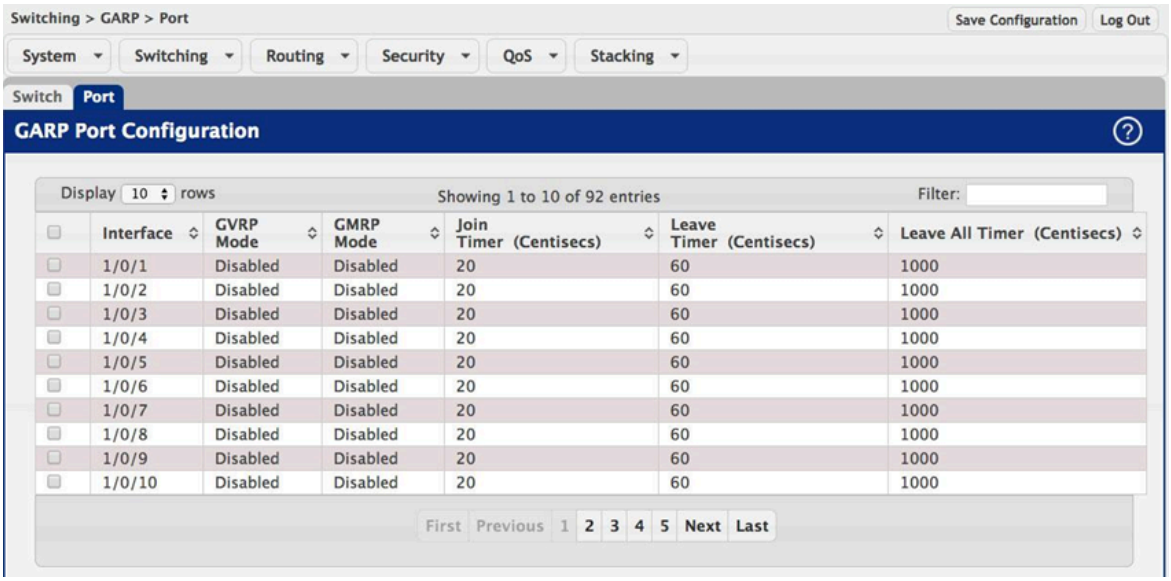
3.6.1. Switching > GARP > Switch

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.

GVRP Mode	The administrative mode of GVRP on the system. When enabled, GVRP can help dynamically manage VLAN memberships on trunk ports. Please notice that GVRP can't be enabled if private VLAN is configured.
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.

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

3.6.2. Switching > GARP > 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.

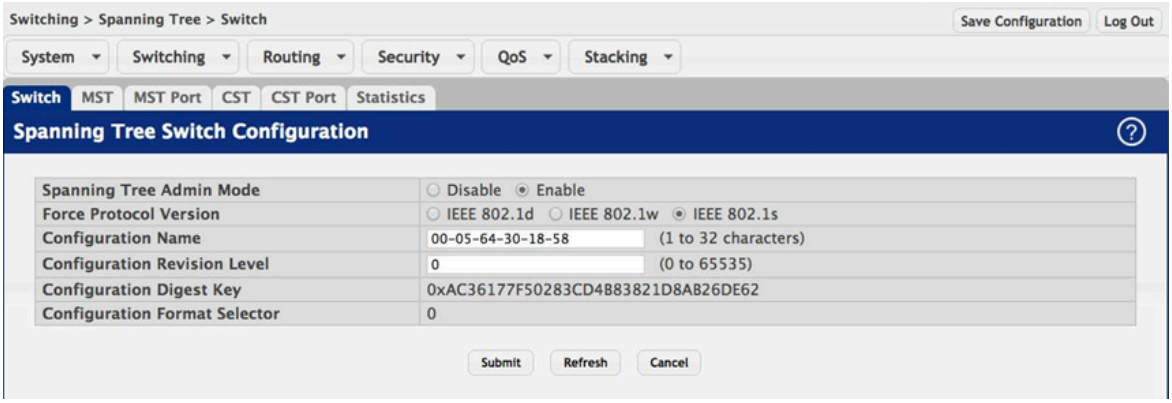
Interface	The interface associated with the rest of the data in the row. When configuring one or more interfaces in the Edit GARP Port Configuration window, this field identifies the interfaces that are being configured.
GVRP Mode	The administrative mode of GVRP on the interface. When enabled, GVRP can 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.

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

3.7. Switching > Spanning Tree

3.7.1. Switching > Spanning Tree > Switch



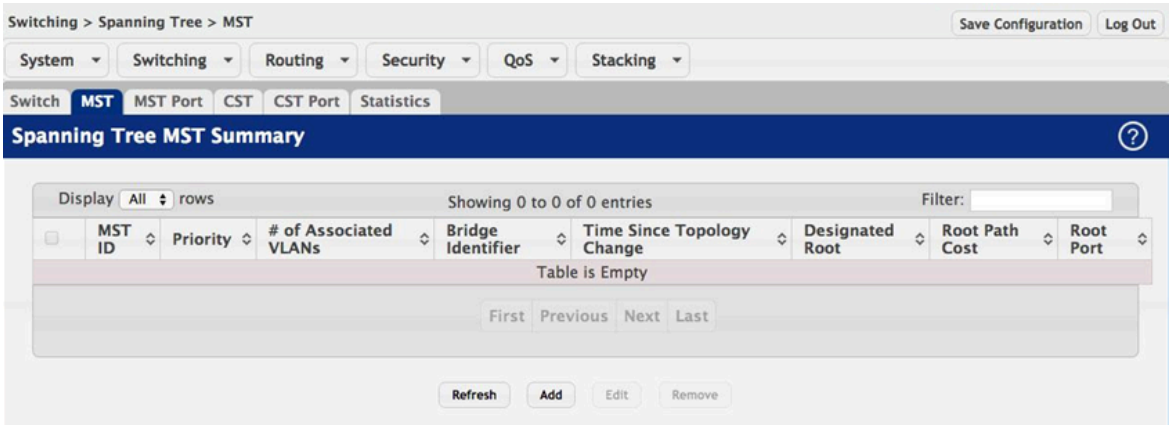
Use this page to view and configure global Spanning Tree Protocol (STP) settings for the device. STP is a Layer 2 protocol that provides a tree topology for switches on a bridged LAN. STP allows a network to have redundant paths without the risk of network loops. STP uses the spanning-tree algorithm to provide a single path between end stations on a network.

Spanning Tree Admin Mode	The administrative mode of STP on the device. When enabled, the device participates in the root bridge election process and exchanges Bridge Protocol Data Units (BPDUs) with other switches in the spanning tree to determine the root path costs and maintain topology information.
Force Protocol Version	The STP version the device uses, which is one of the following: • IEEE 802.1d – Classic STP provides a single path between end stations, avoiding and eliminating loops. • IEEE 802.1w – Rapid Spanning Tree Protocol (RSTP) behaves like classic STP but also has the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notifications. • IEEE 802.1s – Multiple Spanning Tree Protocol (MSTP) includes all the advantages of RSTP and also supports multiple spanning tree instances to efficiently channel VLAN traffic over different interfaces. MSTP is compatible with both RSTP and STP.
Configuration Name	The name of the MSTP region. Each switch that participates in the same MSTP region must share the same Configuration Name, Configuration Revision Level, and MST-to-VLAN mappings.
Configuration Revision Level	The revision number of the MSTP region. This number must be the same on all switches that participate in the MSTP region.
Configuration Digest Key	The 16 byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID-to-MST ID mapping).

Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.

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

3.7.2. Switching > Spanning Tree > 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:

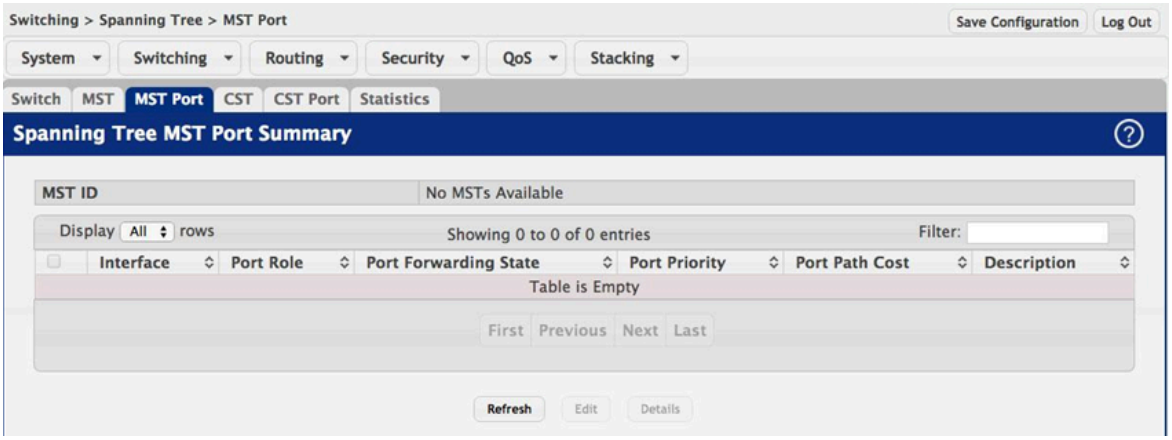
- To configure a new MSTI, click Add and specify the desired settings.
- To change the Priority or the VLAN associations for an existing MSTI, select the entry to modify and click Edit.
- To remove one or more MSTIs, select each entry to delete and click Remove. You must confirm the action before the entry is deleted.

MST ID	The number that identifies the MST instance.
Priority	The bridge priority for the spanning-tree instance. This value affects the likelihood that the bridge is selected as the root bridge. A lower value increases the probability that the bridge is selected as the root bridge.
# of Associated VLANs	The number of VLANs that are mapped to the MSTI. This number does not contain any information about the VLAN IDs that are mapped to the instance.
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value of the MSTI and the base MAC address of the bridge. When electing the root bridge for an MST instance, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.

Time Since Topology Change	The amount of time that has passed since the topology of the MSTI has changed.
Designated Root	The bridge identifier of the root bridge for the MST instance. The identifier is made up of the bridge priority and the base MAC address.
Root Path Cost	The path cost to the designated root for this MST instance. Traffic from a connected device to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Root Port	The port on the bridge with the least-cost path to the designated root for the MST instance.

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

3.7.3. Switching > Spanning Tree > 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.

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	The role of the port within the MST, which is one of the following: • Root – A port on the non-root bridge that has the least-cost path to the root bridge. • Designated – A port that has the least-cost path to the root bridge on its segment.

	• Alternate – A blocked port that has an alternate path to the root bridge. • Backup – A blocked port that has a redundant path to the same network segment as another port on the bridge. • Master – The port on a bridge within an MST instance that links the MST instance to other STP regions. • Disabled – The port is administratively disabled and is not part of the spanning tree.
Port Forwarding State	• Blocking – The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. • Listening – The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. • Learning – The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. • Forwarding – The port sends and receives user traffic. • Disabled – The port is administratively disabled and is not part of the spanning tree.
Port Priority	The priority for the port within the MSTI. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost from the port to the root bridge.
Description	A user-configured description of the port.

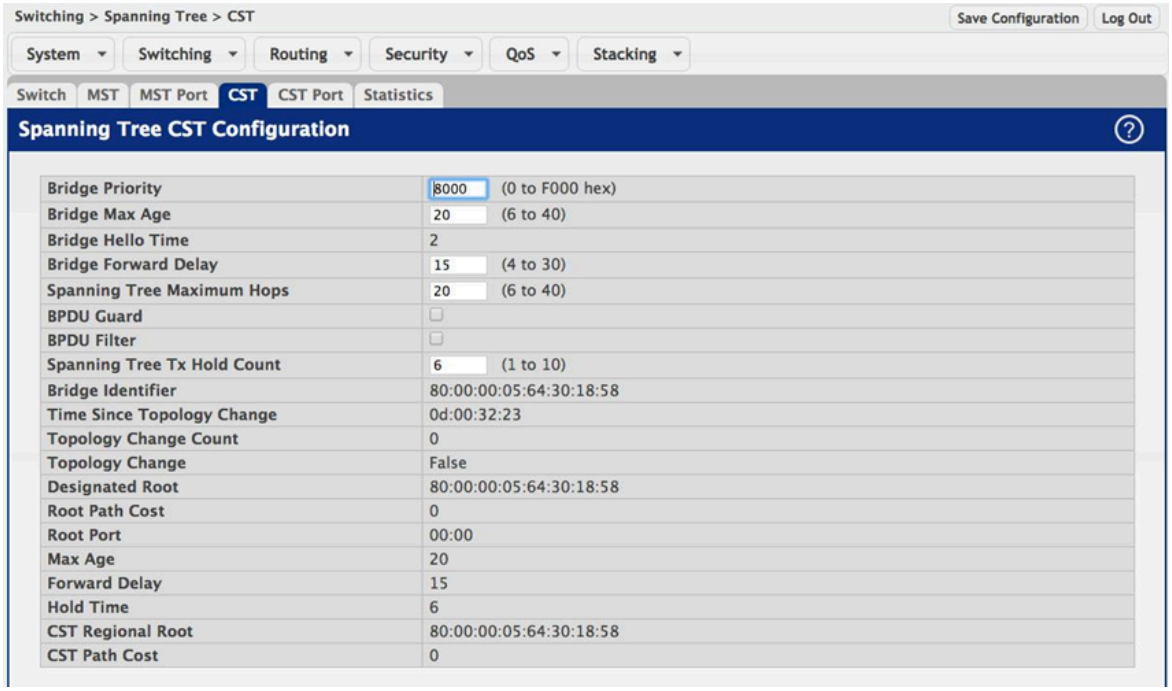
After you select an interface and click Edit, a window opens and allows you to edit the MST port settings and view additional MST information for the interface. The following information describes the additional fields available in this window.

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

Designated Root	The bridge ID of the root bridge for the MST instance.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
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.

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

3.7.4. Switching > Spanning Tree > 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.

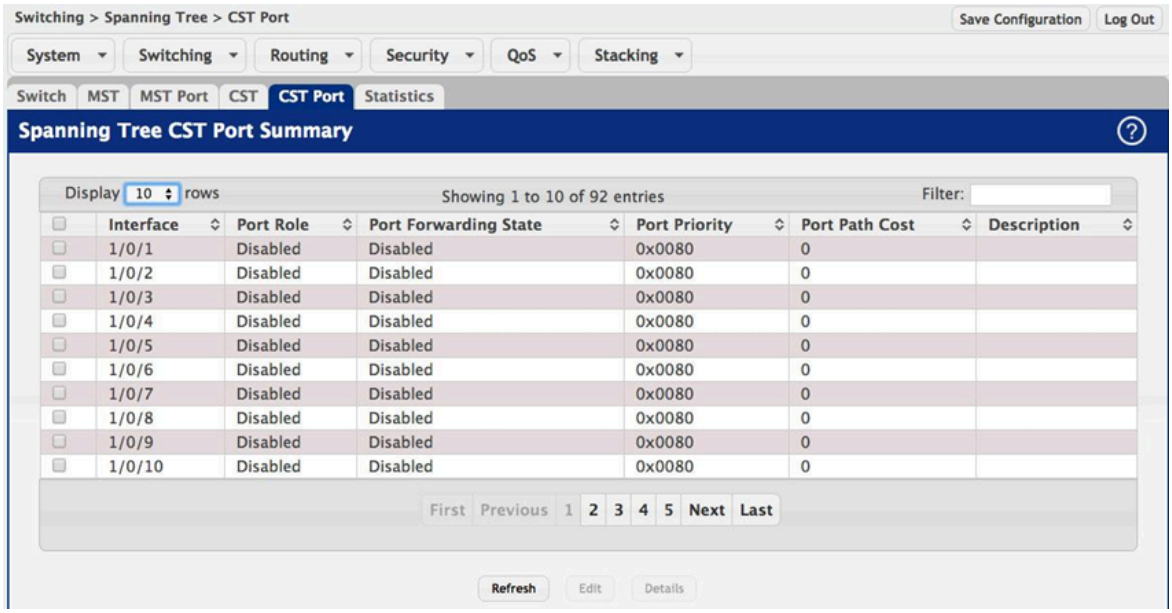
Bridge Priority	The value that helps determine which bridge in the spanning tree is elected as the root bridge during STP convergence. A lower value increases the probability that the bridge becomes the root bridge.

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.

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

3.7.5. Switching > Spanning Tree > 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.

Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
Port Role	The role of the port within the CST, which is one of the following: • Root – A port on the non-root bridge that has the least-cost path to the root bridge. • Designated – A port that has the least-cost path to the root bridge on its segment. • Alternate – A blocked port that has an alternate path to the root bridge. • Backup – A blocked port that has a redundant path to the same network segment as another port on the bridge. • Master – The port on a bridge within an MST instance that links the MST instance to other STP regions.

	• Disabled – The port is administratively disabled and is not part of the spanning tree.
Port Forwarding State	• Blocking – The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. • Listening – The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. • Learning – The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. • Forwarding – The port sends and receives user traffic. • Disabled – The port is administratively disabled and is not part of the spanning tree.
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost from the port to the root bridge.
Description	A user-configured description of the port.

After you select an interface and click Edit, a window opens and allows you to edit the CST port settings and view additional CST information for the interface. The following information describes the additional fields available in the Edit CST Port Entry window.

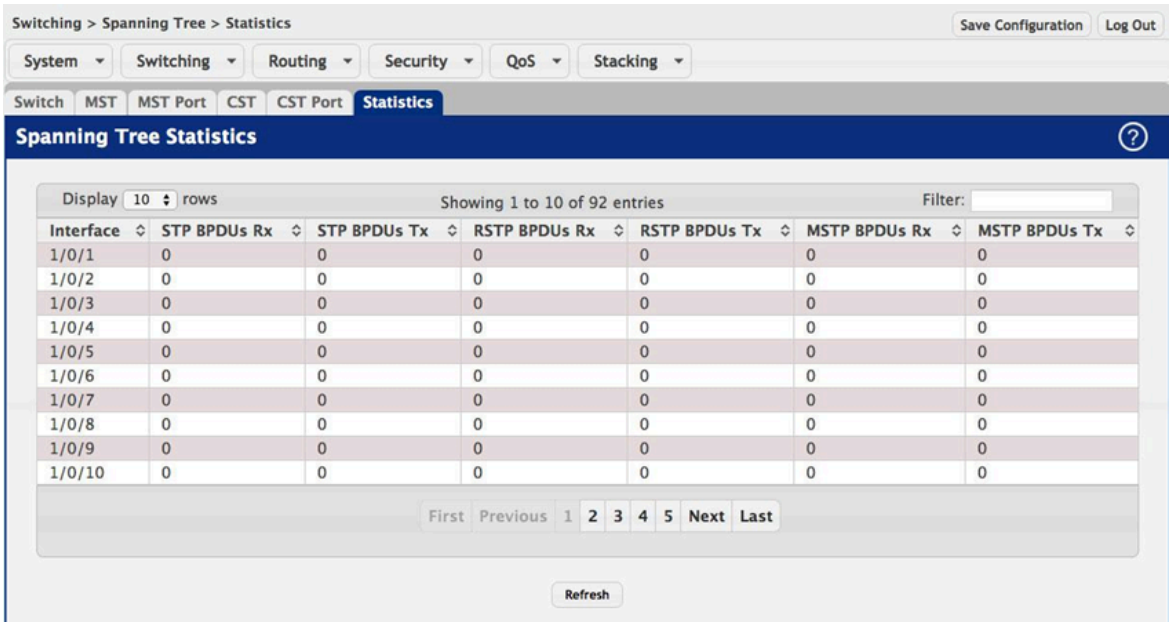
Admin Edge Port	Select this option administratively configure the interface as an edge port. An edge port is an interface that is directly connected to a host and is not at risk of causing a loop.
Auto-calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
Hello Timer	The amount of time the port waits between sending hello BPDUs.
External Port Path Cost	The cost of the path from the port to the CIST root. This value becomes important when the network includes multiple regions.
Auto-calculate External Port Path Cost	Shows whether the path cost from the port to the CIST root is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
BPDU 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.

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

3.7.6. Switching > Spanning Tree > Statistics



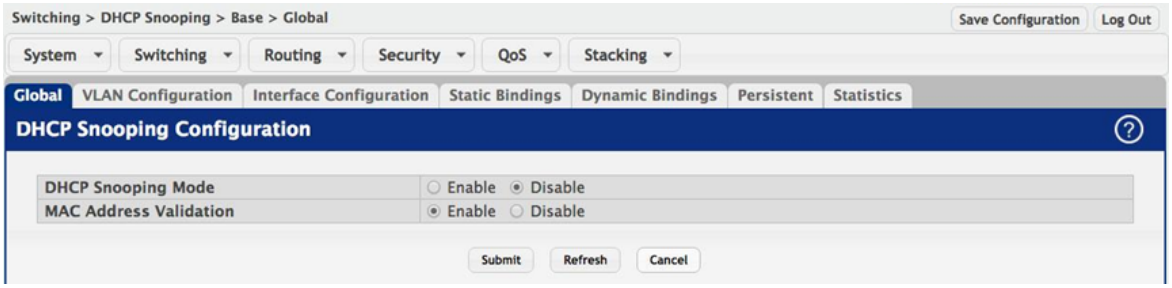
This page displays information about the number of bridge protocol data units (BPDUs) sent and received by each interface for each STP version.

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.

3.8. Switching > DHCP Snooping

3.8.1. Switching > DHCP Snooping > Base

3.8.1.1. Switching > DHCP Snooping > Base > Global

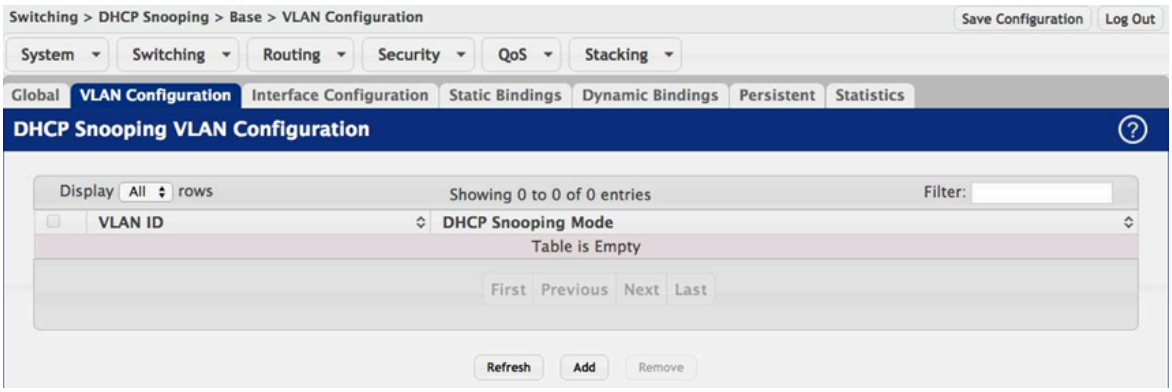


Use this page to view and configure the global settings for DHCP Snooping. DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are 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 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.

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

3.8.1.2. Switching > DHCP Snooping > 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.

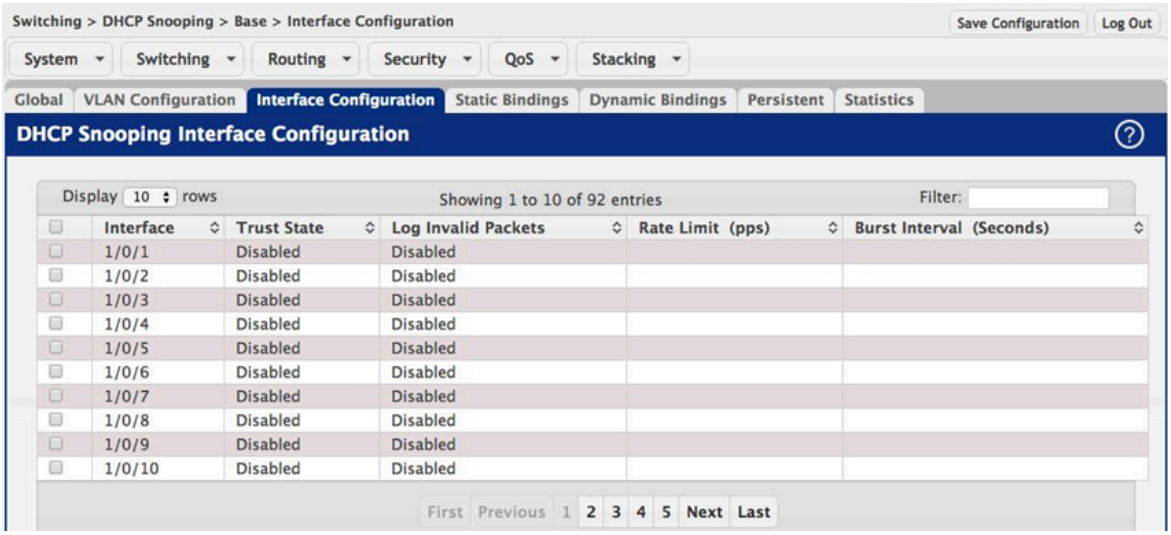
Use the buttons to perform the following tasks:

- 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.

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.

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

3.8.1.3. Switching > DHCP Snooping > Base > Interface Configuration



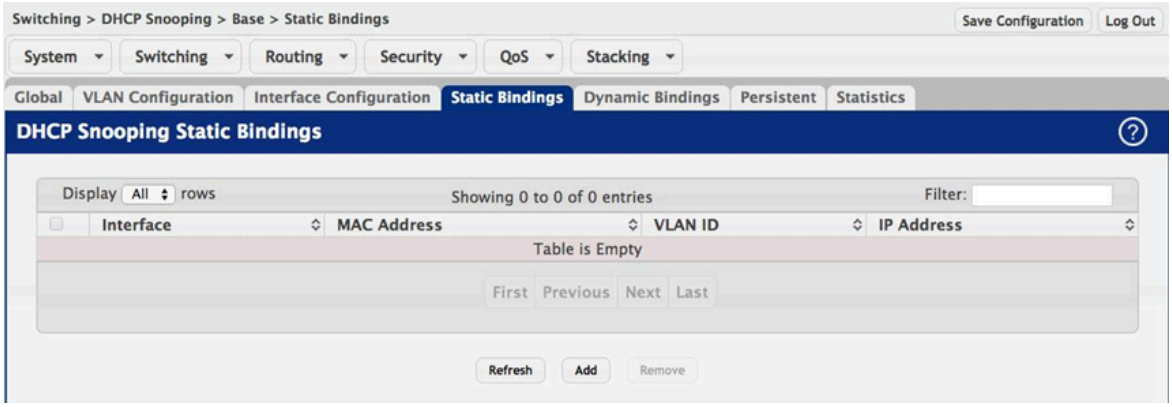
Use this page to view and configure the DHCP snooping settings for each interface. The DHCP snooping feature processes incoming DHCP messages. For DHCPRELEASE and

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.

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.

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

3.8.1.4. Switching > DHCP Snooping > Base > Static Bindings



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

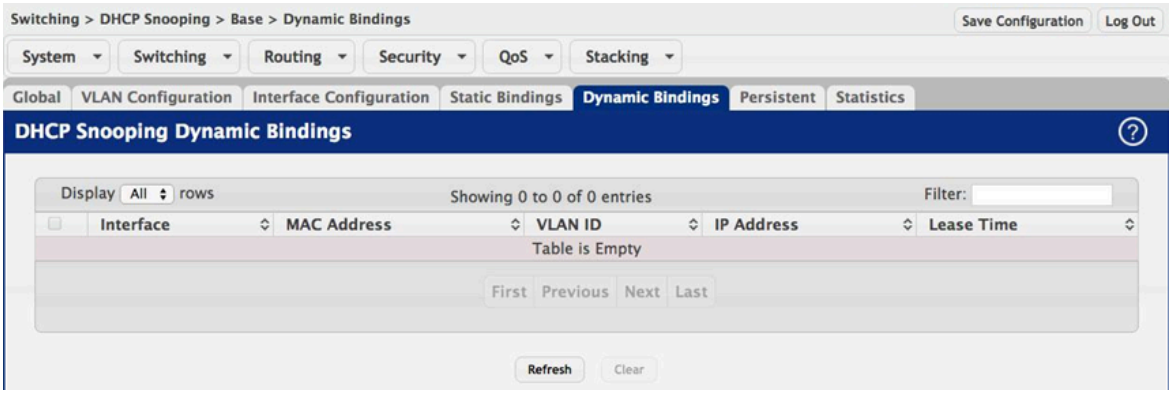
Use the buttons to perform the following tasks:

- 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.

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.

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

3.8.1.5. Switching > DHCP Snooping > Base > Dynamic Bindings

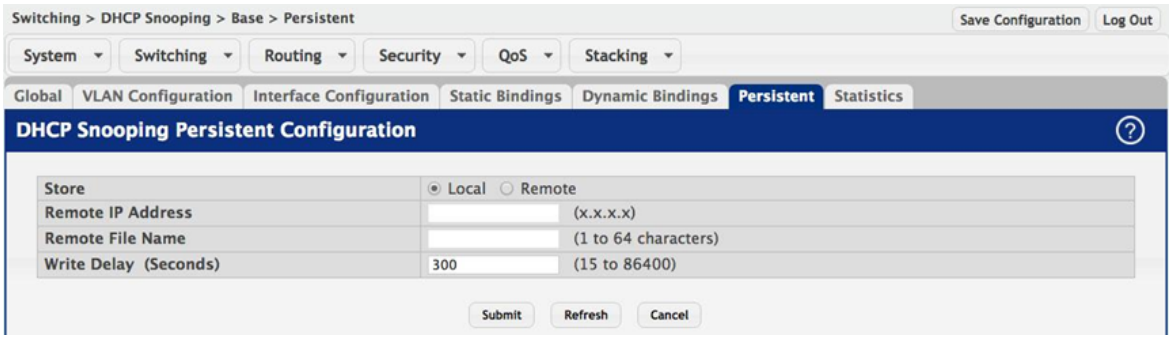


Use this page to view and clear dynamic bindings in the DHCP snooping bindings database. The DHCP snooping feature uses DHCP messages to build and maintain the bindings database. The bindings database includes data for clients only on untrusted ports. DHCP snooping creates a tentative binding from DHCP 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.

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.

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

3.8.1.6. Switching > DHCP Snooping > Base > Persistent



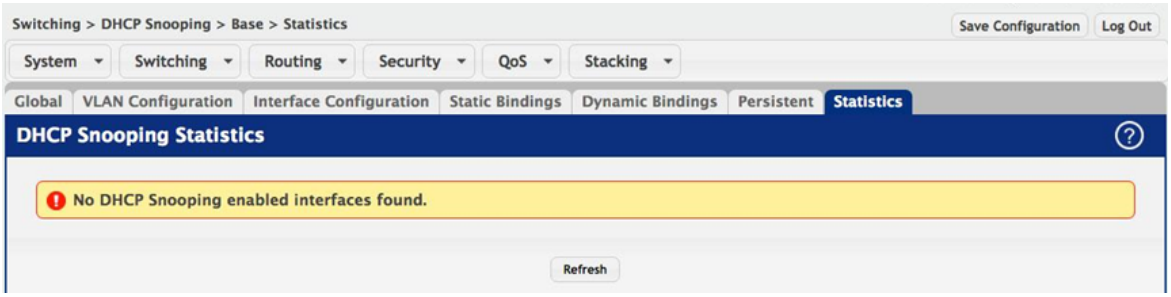
Use this page to configure the persistent location of the DHCP snooping bindings database. The bindings database can be stored locally on the device or on a remote system somewhere else in the network. The device must be able to reach the IP address of the remote system to send bindings to a remote database.

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.

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

3.8.1.7. Switching > DHCP Snooping > Base > Statistics

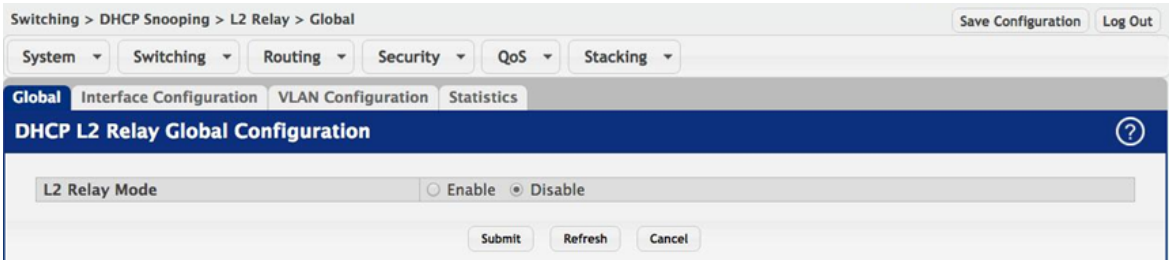


Use this page to view and clear per-interface statistics about the DHCP messages filtered by the DHCP snooping feature. Only interfaces that are enabled for DHCP snooping and are untrusted appear in the table.

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.

3.8.2. Switching > DHCP Snooping > L2 Relay

3.8.2.1. Switching > DHCP Snooping > L2 Relay > Global

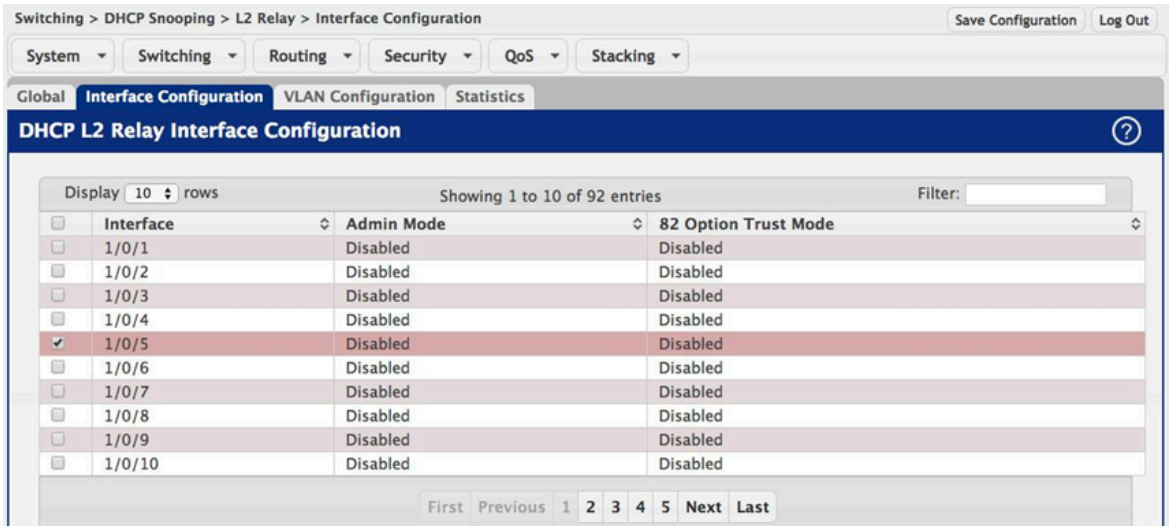


Use this page to enable or disable the switch to act as a DHCP L2 relay agent. This functionality must also be enabled on each port you want this service to operate on. The switch can also be configured to relay requests only when the VLAN of the requesting client corresponds to a service provider's VLAN ID that has been enabled with the L2 DHCP relay functionality.

L2 Relay Mode	The administrative mode of DHCP l2 relay on the device.

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

3.8.2.2. Switching > DHCP Snooping > L2 Relay > Interface Configuration



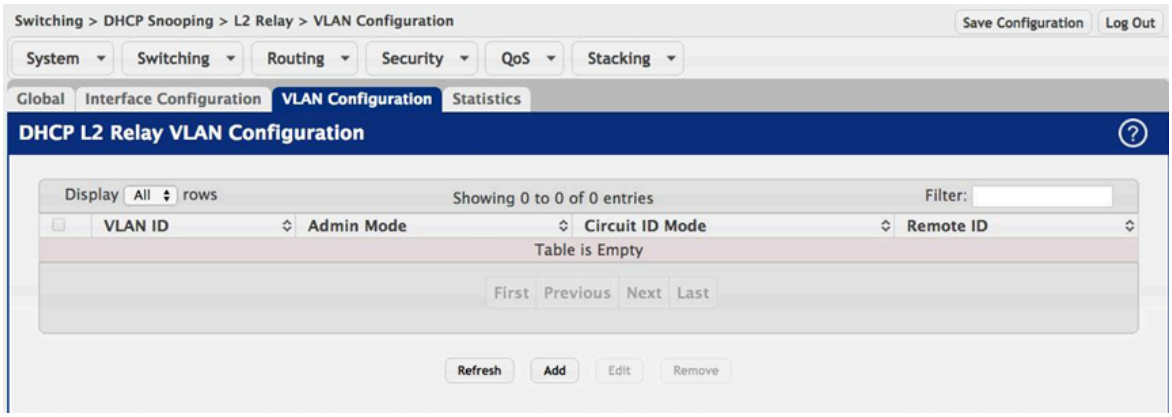
Use this page to enable L2 DHCP relay on individual ports. Note that L2 DHCP relay must also be enabled globally on the switch.

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.

Admin Mode	Enable or disable L2 Relay mode on the selected interface.
82 Option Trust Mode	Enable or disable L2 Relay Trust Mode on the selected interface. • Trusted interfaces usually connect to other agents or servers participating in the DHCP interaction (e.g. other L2 or L3 Relay Agents or Servers). When enabled in Trust Mode, the interface always expects to receive DHCP packets that include Option 82 information. If Option 82 information is not included, these packets are discarded. • Untrusted interfaces are generally connected to clients. DHCP packets arriving on an untrusted interface are never expected to carry Option 82 and are discarded if they do.

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

3.8.2.3. Switching > DHCP Snooping > L2 Relay > VLAN Configuration



You can enable L2 DHCP relay on a particular VLAN. The VLAN is identified by a service VLAN ID (S-VID), which a service provider uses to identify a customer's traffic while traversing the provider network to multiple remote sites. The switch uses the VLAN membership of the switch port client (the customer VLAN ID, or C-VID) to perform a lookup a corresponding S-VID.

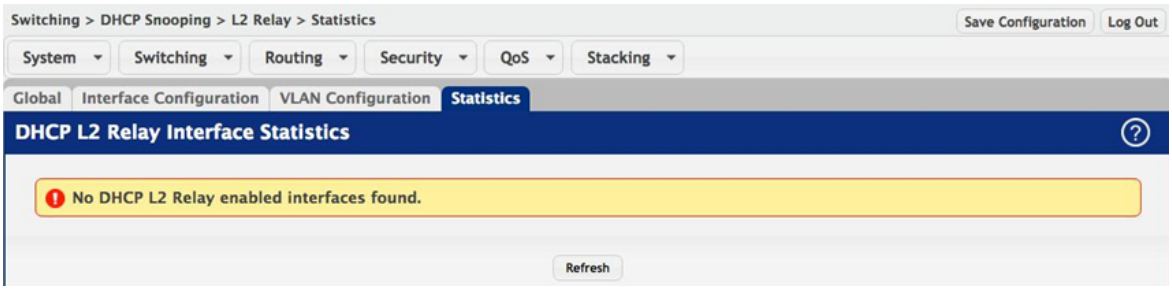
If the S-VID is enabled for DHCP L2 Relay, the packet can be forwarded. If the C-VID does not correspond to an S-VID that is enabled for DHCP L2 relay, the switch will not relay the DHCP request packet.

VLAN ID	Select a VLAN ID from the list for configuration. This is an S-VID (as indicated by the service provider) that identifies a VLAN that is authorized to relay DHCP packets through the provider network
Circuit ID Mode	Enable or disable the selected VLAN for DHCP L2 relay services.
Remote ID	When enabled, if a client sends a DHCP request to the switch and the client is in a VLAN that corresponds to the selected S-VID, the switch adds the client's interface number to the Circuit ID sub-option of Option

	82 in the DHCP request packet. This enables the switch to reduce the broadcast domain to which the server replies are switched when the broadcast bit is set for DHCP packets. When this bit is set, the server is required to echo the Option-82 in replies. Since the circuit-id field contains the client interface number, the L2 relay agent can forward the response to the requesting interface only, rather to all ports in the VLAN).

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

3.8.2.4. Switching > DHCP Snooping > L2 Relay > Statistics



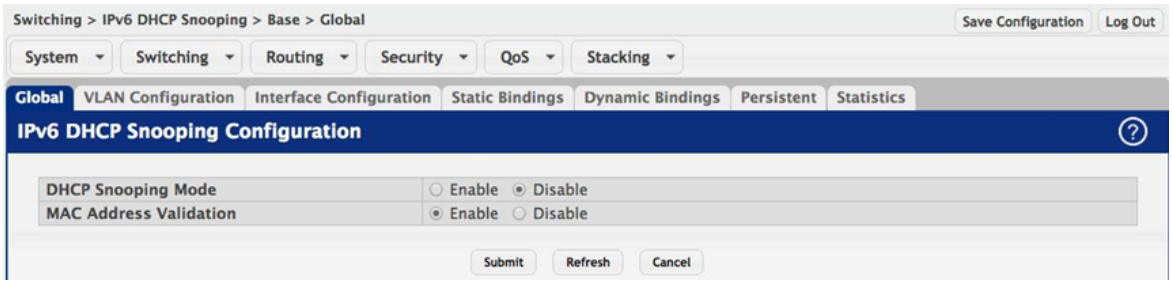
Use this page to view and clear per-interface statistics about the DHCP messages filtered by the DHCP L2 Relay feature. Only interfaces that are enabled for DHCP L2 Relay appear in the table.

Interface	The interface associated with the rest of the data in the row.
Untrusted Server Messages With Option-82	If the selected interface is configured in untrusted mode, this field shows the number of messages received on the interface from a DHCP server that contained Option 82 data.These messages are dropped.
Untrusted Client Messages With Option-82	If the selected interface is configured in untrusted mode, this field shows the number of messages received on the interface from a DHCP client that contained Option 82 data.These messages are dropped.
Trusted Server Messages Without Option-82	If the selected interface is configured in trusted mode, this field shows the number of messages received on the interface from a DHCP server that did not contain Option 82 data. These messages are dropped.
Trusted Client Messages Without Option-82	If the selected interface is configured in trusted mode, this field shows the number of messages received on the interface from a DHCP client that did not contain Option 82 data. These messages are dropped.
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.

3.9. Switching > IPv6 DHCP Snooping

3.9.1. Switching > IPv6 DHCP Snooping > Base

3.9.1.1. Switching > IPv6 DHCP Snooping > Base > Global

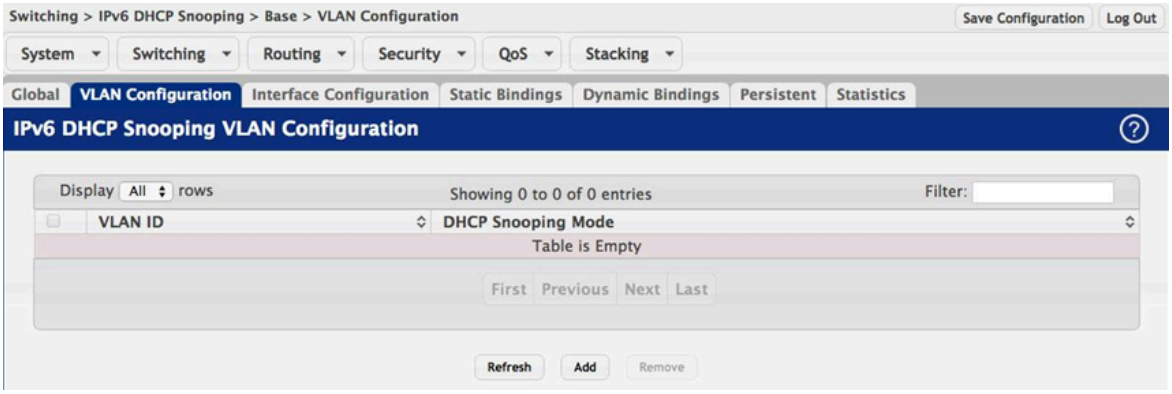


Use this page to view and configure the global settings for IPv6 DHCP snooping. IPv6 DHCP snooping is a security feature that monitors DHCPv6 messages between a DHCPv6 client and DHCPv6 servers to filter harmful DHCPv6 messages and to build a bindings database of {MAC address, IPv6 address, VLAN ID, 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	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.

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

3.9.1.2. Switching > IPv6 DHCP Snooping > 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.

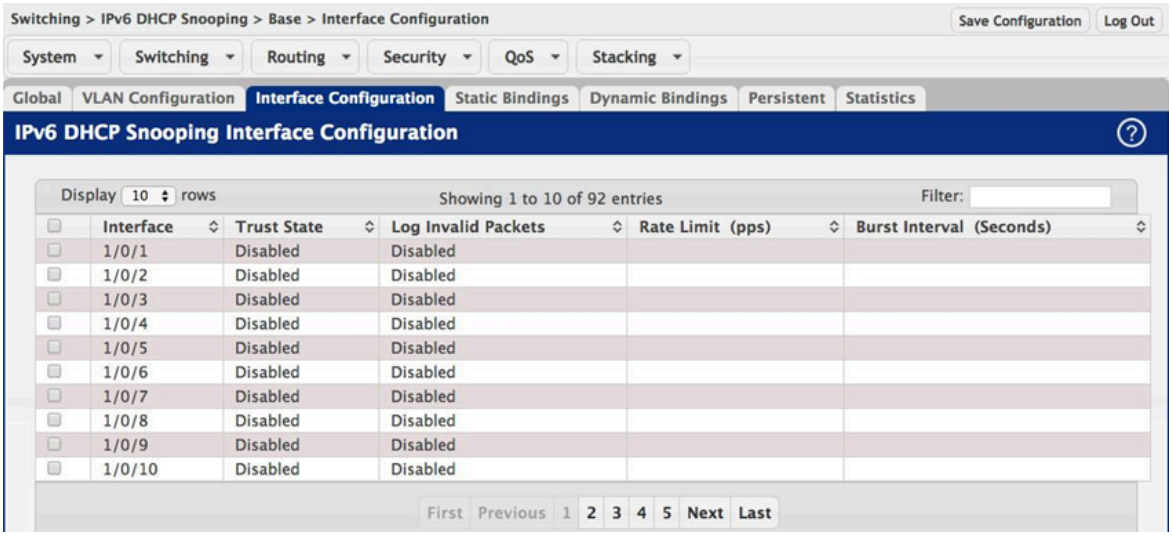
Use the buttons to perform the following tasks:

- 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.

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.

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

3.9.1.3. Switching > IPv6 DHCP Snooping > Base > Interface Configuration



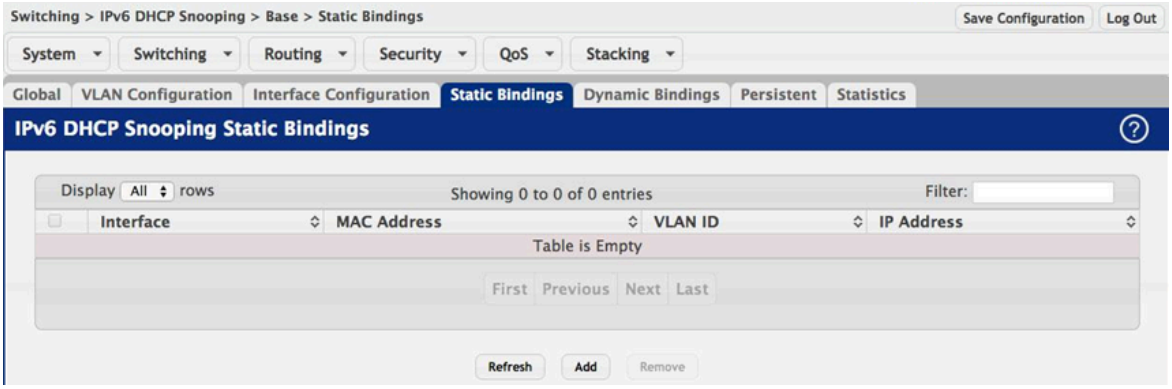
Use this page to view and configure the IPv6 DHCP snooping settings for each interface. The IPv6 DHCP snooping feature processes incoming DHCPv6 messages. For RELEASE and DECLINE messages, the feature compares the receive interface and VLAN with the client's interface and VLAN in the binding database. 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.

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 Packets	The administrative mode of invalid packet logging on the interface. 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.

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

3.9.1.4. Switching > IPv6 DHCP Snooping > Base > Static Bindings



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

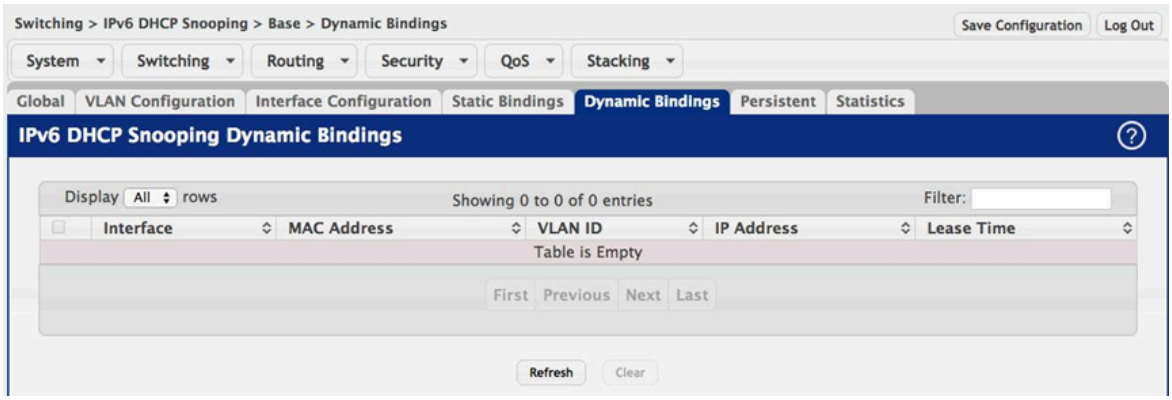
Use the buttons to perform the following tasks:

- 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.

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.

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

3.9.1.5. Switching > IPv6 DHCP Snooping > Base > Dynamic Bindings

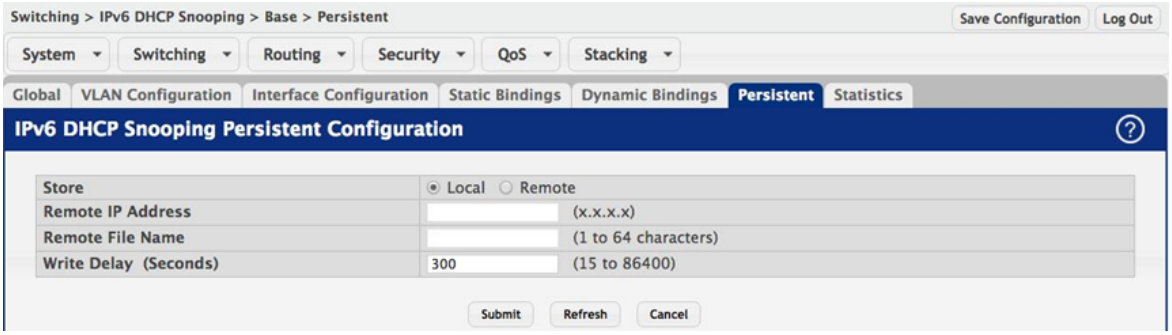


Use this page to view and clear dynamic bindings in the IPv6 DHCP snooping bindings database. The IPv6 DHCP snooping feature uses DHCPv6 messages to build and maintain the bindings database. The bindings database includes data for clients only on untrusted ports. IPv6 DHCP snooping creates a tentative 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.

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.

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

3.9.1.6. Switching > IPv6 DHCP Snooping > Base > Persistent

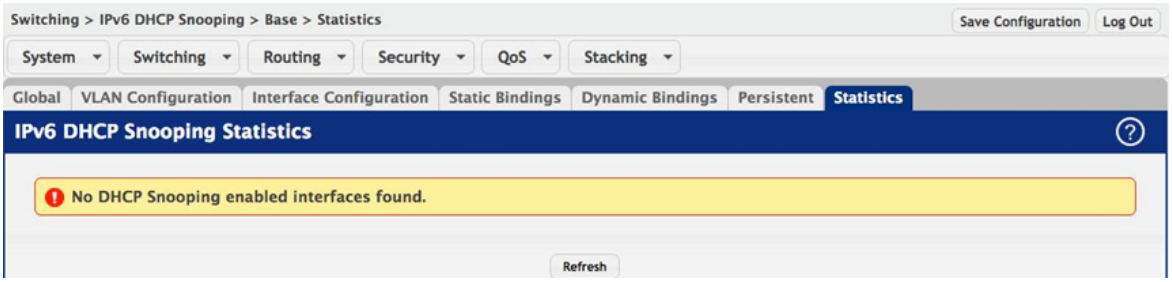


Use this page to configure the persistent location of the IPv6 DHCP snooping bindings database. The bindings database can be stored locally on the device or on a remote system somewhere else in the network. The device must be able to reach the IP address of the remote system to send bindings to a remote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

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.

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

3.9.1.7. Switching > IPv6 DHCP Snooping > Base > Statistics

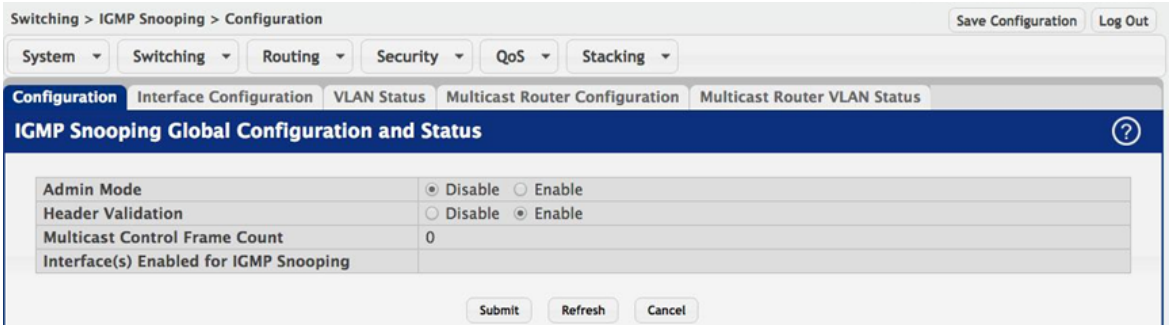


Use this page to view and clear per-interface statistics about the DHCPv6 messages filtered by the IPv6 DHCP snooping feature. Only interfaces that are enabled for IPv6 DHCP snooping and are untrusted appear in the table.

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.

3.10. Switching > IGMP Snooping

3.10.1. Switching > IGMP Snooping > Configuration

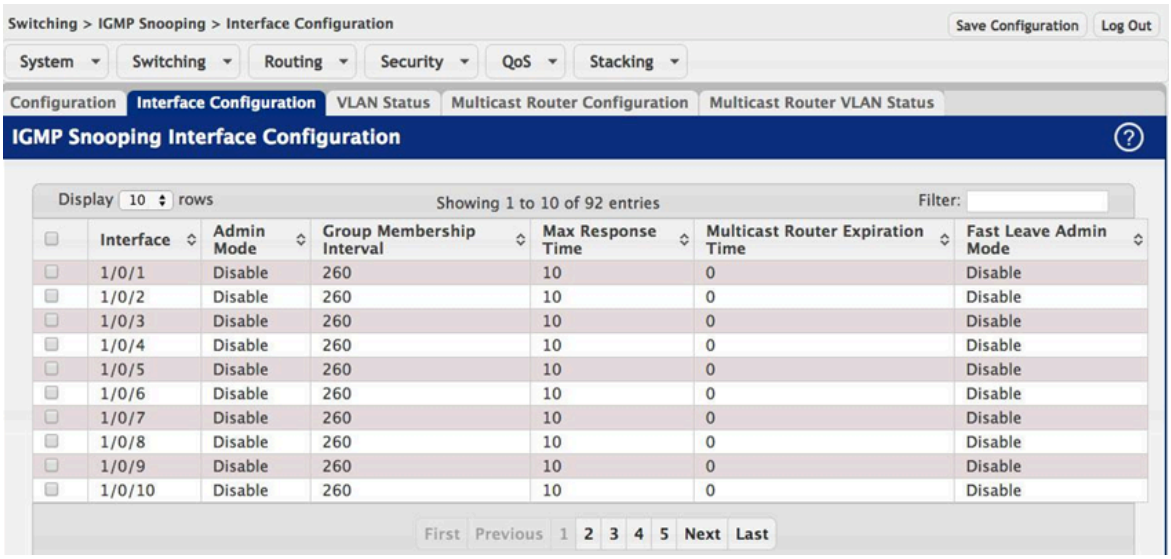


Use this page to enable Internet Group Management Protocol (IGMP) snooping on the device and to view global status information. IGMP snooping allows a device to forward multicast traffic intelligently. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class 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.

Admin Mode	The administrative mode of IGMP snooping on the device.
Header Validation	Enables or disables header validation for all IGMP messages.
Interface(s) Enabled for IGMP Snooping	The interface(s) 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.
Multicast Control Frame Count	The number of multicast control frames that have been processed by the CPU.

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

3.10.2. Switching > IGMP Snooping > Interface Configuration

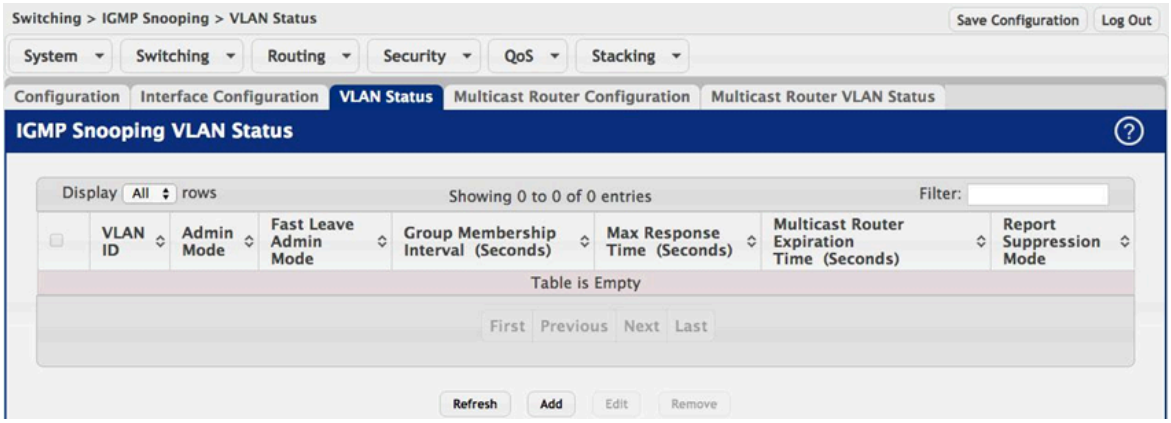


Use this page to configure IGMP snooping settings on specific interfaces. To configure the settings for one or more interfaces, select each entry to modify and click Edit. The same IGMP snooping settings are applied to all selected interfaces.

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.

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

3.10.3. Switching > IGMP Snooping > 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:

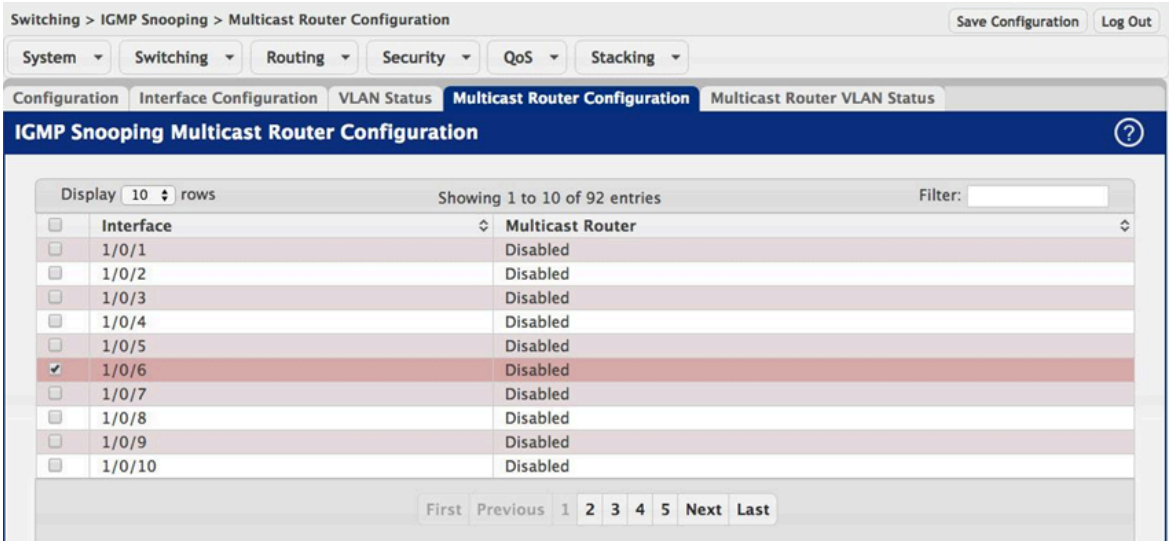
- To enable IGMP snooping on a VLAN, click Add and configure the settings in the available fields.
- To change the IGMP snooping settings for an IGMP-snooping enabled VLAN, select the entry with the settings to change and click Edit.
- To disable IGMP snooping on one or more VLANs, select each VLAN to 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.

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.

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

3.10.4. Switching > IGMP Snooping > Multicast Router Configuration

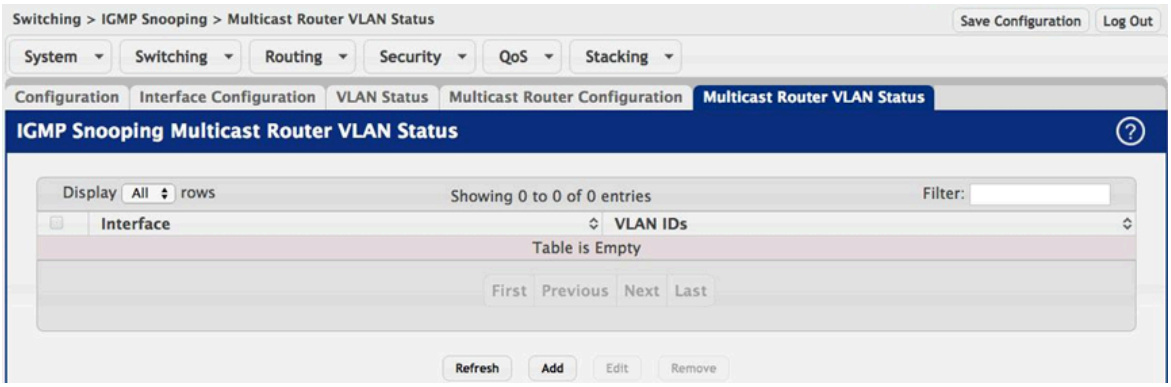


If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure an interface as a multicast router interface, which is an interface that faces a multicast router or IGMP querier and receives multicast traffic. Use this page to manually configure 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.

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.

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

3.10.5. Switching > IGMP Snooping > 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.

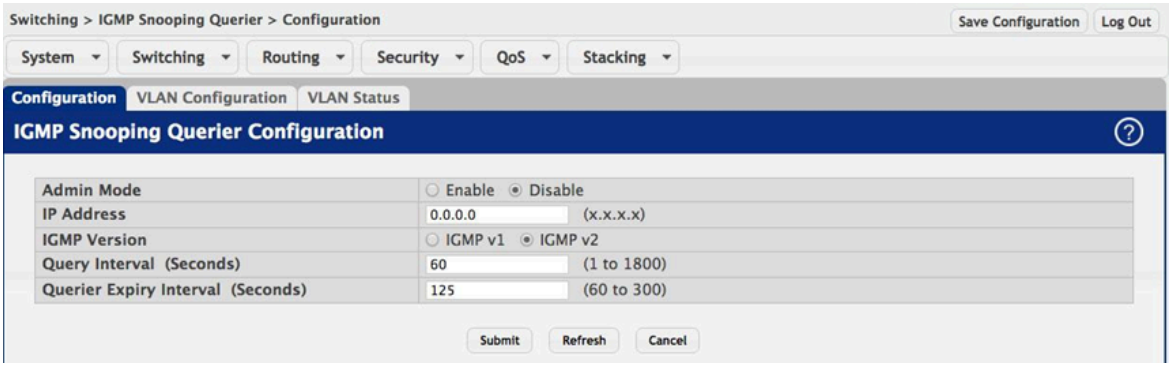
Use this page to view the multicast router VLAN status for each interface. From this page, you can also click the Add and Edit buttons to be redirected to the Multicast Router VLAN Configuration page for the selected interface to enable or disable VLANs as multicast router interfaces. To disable all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

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.

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

3.11. Switching > IGMP Snooping Querier

3.11.1. Switching > IGMP Snooping Querier > Configuration

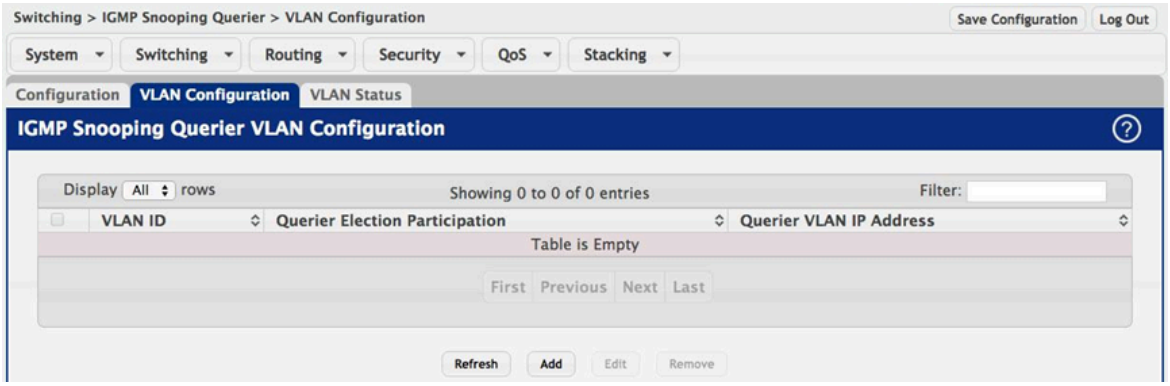


Use this page to configure the global IGMP snooping querier settings on the device. IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP querier. When layer 3 IP multicast routing 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.

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.

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

3.11.2. Switching > IGMP Snooping Querier > 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:

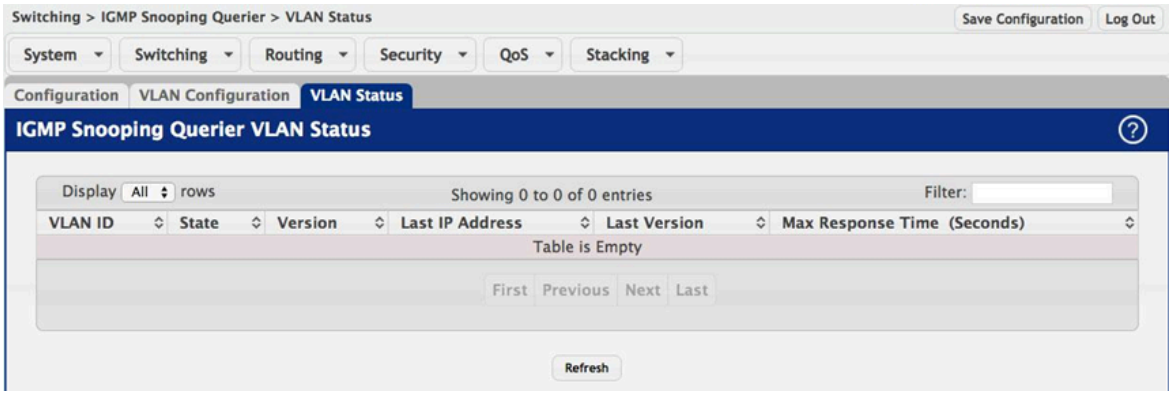
- To enable the IGMP snooping querier feature on a VLAN, click Add and specify the desired settings.
- To change the IGMP snooping querier settings for a VLAN, select the entry to modify and click Edit.
- To disable the IGMP snooping querier feature on one or more VLANs, select each entry to change and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

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.

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

3.11.3. Switching > IGMP Snooping Querier > VLAN Status



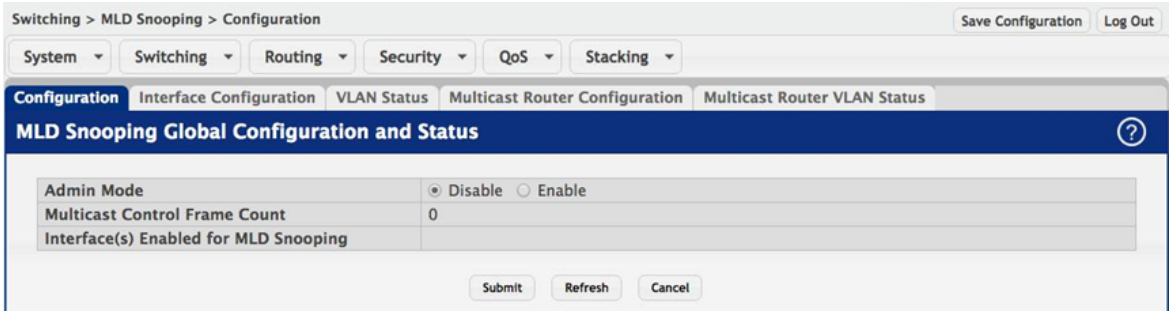
Use this page to view information about the IGMP snooping querier status for all VLANs that have the snooping querier enabled.

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.

3.12. Switching > MLD Snooping

3.12.1. Switching > MLD Snooping > Configuration

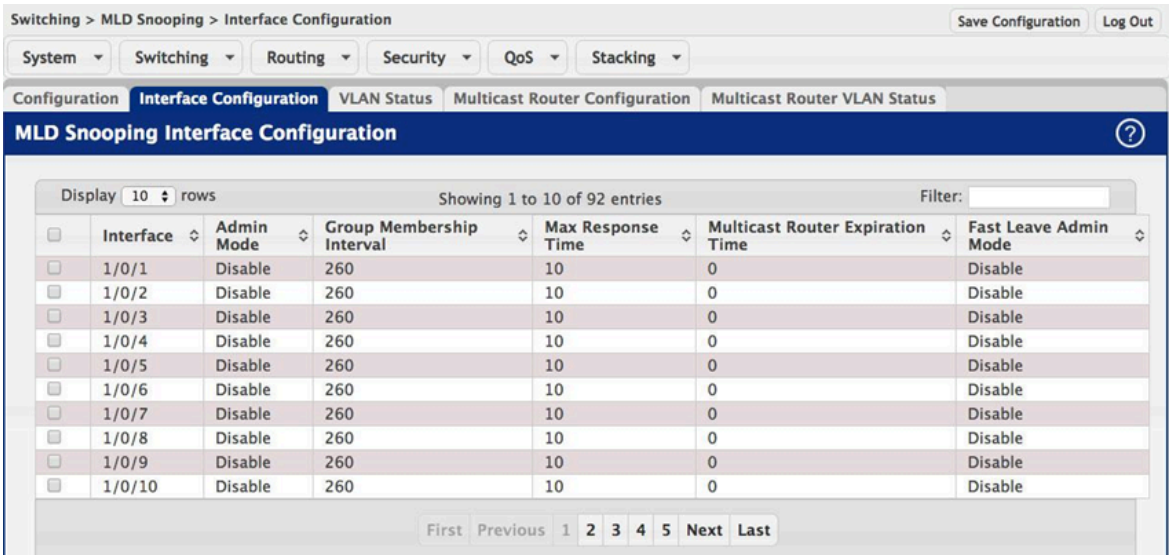


MLD is protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly-attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1(MLDv1) is equivalent to IGMPv2 and MLD version 2(MLDv2) os equivalent to IGMPv3. MLD is a subprotocol of internet Control Message Protocol version 6(ICMPv6), and MLD messages are a subset of ICMPv6 messages. The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data base on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

Admin Mode	The administrative mode of MLD snooping on the device.
Interface(s) Enabled for MLD Snooping	The interface(s) on which MLD snooping is administratively enabled. MLD snooping must be enabled globally and on an interface for the interface to be able to snoop MLD packets to determine which segments should receive multicast packets directed to the group address.
Multicast Control Frame Count	The number of multicast control frames that have been processed by the CPU.

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

3.12.2. Switching > MLD Snooping > Interface Configuration

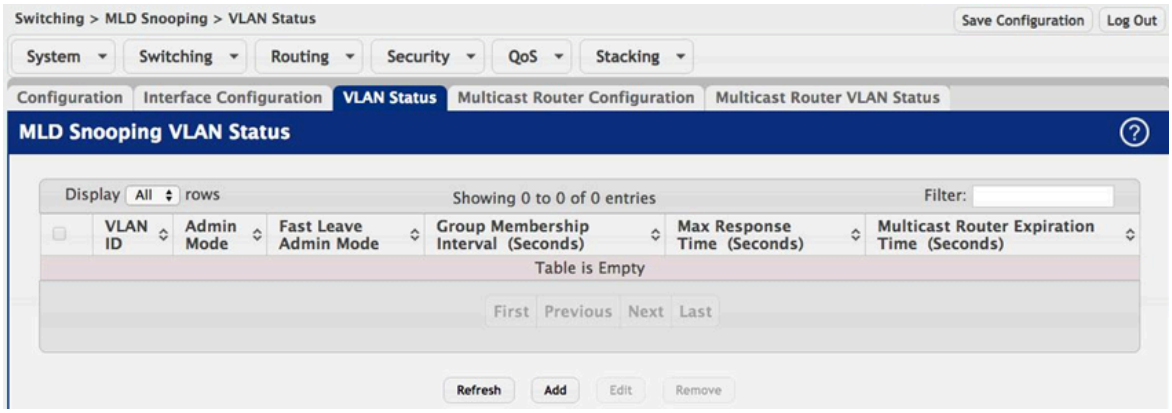


Use this page to configure MLD snooping settings on specific interfaces. To configure the settings for one or more interfaces, select each entry to modify and click Edit. The same MLD snooping settings are applied to all selected interfaces.

Interface	The interface associated with the rest of the data in the row. When configuring MLD snooping settings, this field identifies the interface(s) that are being configured.
Admin Mode	The administrative mode of MLD snooping on the interface. MLD snooping must be enabled globally and on an interface for the interface to be able to snoop MLD packets to determine which segments should receive multicast packets directed to the group address.
Group Membership Interval	The number of seconds the interface should wait for a report for a particular group on the interface before the MLD snooping feature deletes the interface from the group.
Max Response Time	The number of seconds the interface should wait after sending a query if it does not receive a report for a particular group. The specified value should be less than the Group Membership Interval.
Multicast Router Expiration Time	The number of seconds the interface should wait to receive a query before it is removed from the list of interfaces with multicast routers attached.
Fast Leave Admin Mode	The administrative mode of Fast Leave on the interface. If Fast Leave is enabled, the interface can be immediately removed from the layer 2 forwarding table entry upon receiving an MLD leave message for a multicast group without first sending out MAC-based general queries.

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

3.12.3. Switching > MLD Snooping > VLAN Status



Use this page to enable or disable MLD snooping on system VLANs and to view and configure per-VLAN MLD snooping settings. Only VLANS that are enabled for MLD snooping appear in the table.

Use the buttons to perform the following tasks:

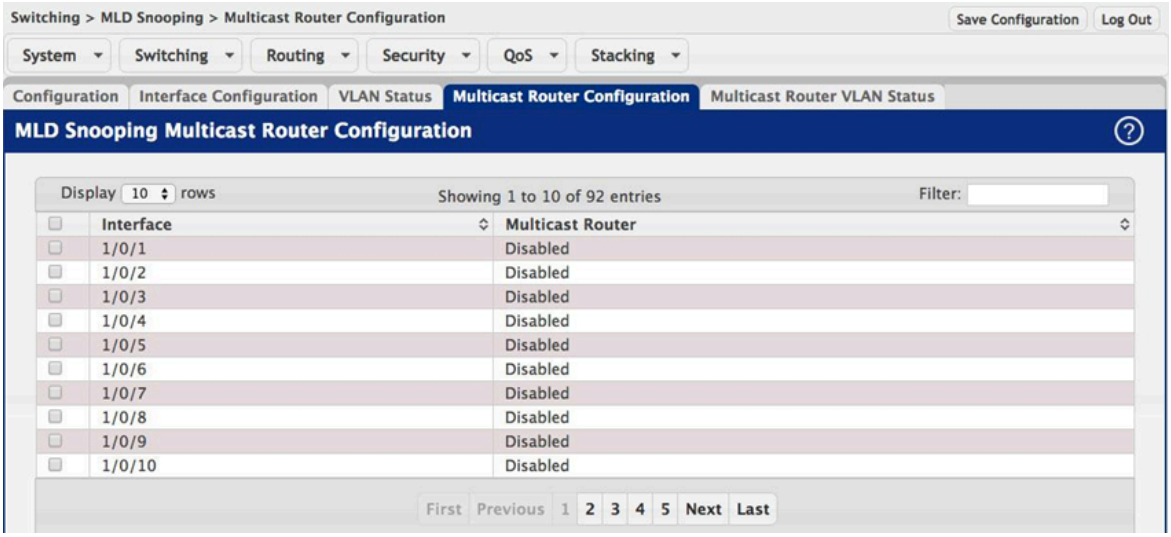
- To enable MLD snooping on a VLAN, click Add and configure the settings in the available fields.
- To change the MLD snooping settings for an MLD-snooping enabled VLAN, select the entry with the settings to change and click Edit.
- To disable MLD snooping on one or more VLANs, select each VLAN to modify and click Remove. You must confirm the action before MLD snooping is disabled on the selected VLANs. When MLD snooping is disabled, the VLAN entry is removed from the table, but the VLAN itself still exists on the system.

VLAN ID	The VLAN associated with the rest of the data in the row. When enabling MLD snooping on a VLAN, use this menu to select the desired VLAN. Only VLANs that have been configured on the system and are not already enabled for MLD snooping appear in the menu. When modifying MLD snooping settings, this field identifies the VLAN that is being configured.
Admin Mode	The administrative mode of MLD snooping on the VLAN. MLD snooping must be enabled globally and on an VLAN for the VLAN to be able to snoop MLD 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 MLD 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 MLD 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.

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

3.12.4. Switching > MLD Snooping > Multicast Router Configuration

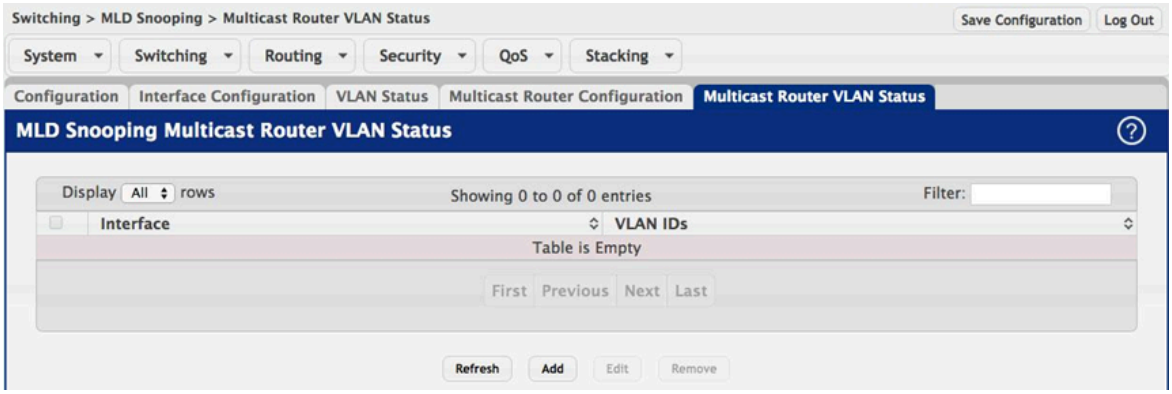


If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure an interface as a multicast router interface, which is an interface that faces a multicast router or MLD querier and receives multicast traffic. Use this page to manually configure 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.

Interface	The interface associated with the rest of the data in the row. When configuring the MLD 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.

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

3.12.5. Switching > MLD Snooping > Multicast Router VLAN Status



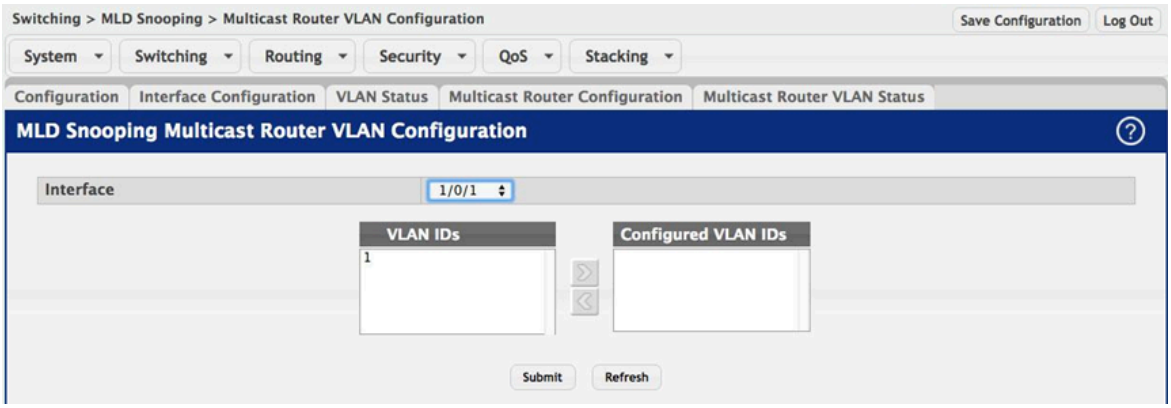
If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure one or more VLANs on each interface to act as a multicast router interface, which is an interface that faces a multicast router or MLD querier and receives multicast traffic.

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.

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.

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

3.12.6. Switching > MLD Snooping > Multicast Router VLAN Configuration



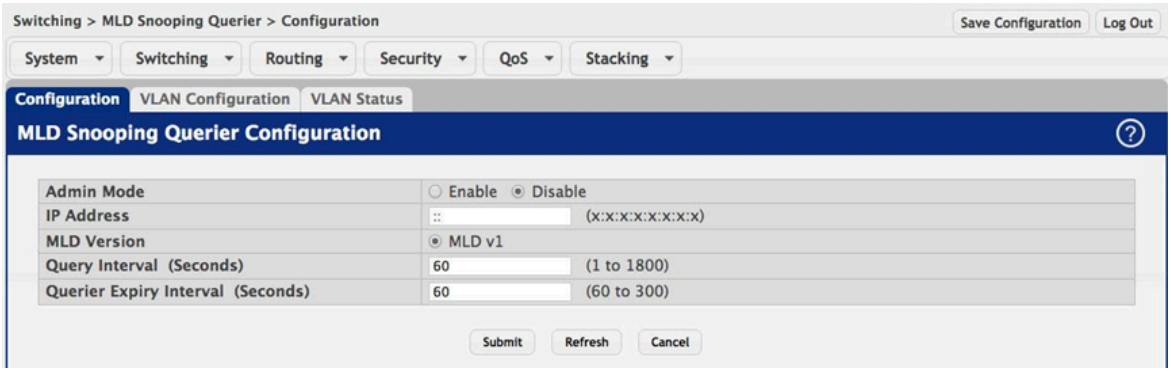
Use this page to enable or disable specific VLANs as multicast router interfaces for a physical port or LAG. A multicast router interface faces a multicast router or MLD querier and receives multicast traffic.

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.

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

3.13. Switching > MLD Snooping Querier

3.13.1. Switching > MLD Snooping Querier > Configuration

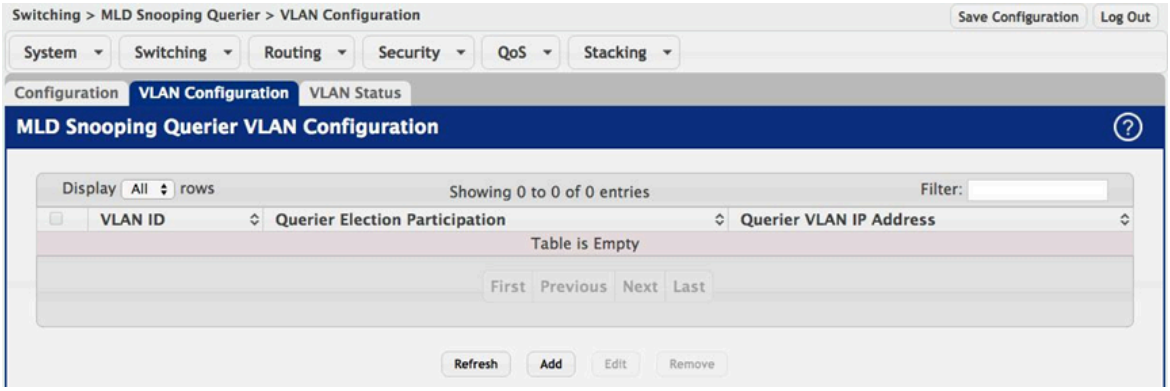


Use this page to configure the global MLD snooping querier settings on the device. MLD snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the MLD querier. When layer 3 IP multicast routing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

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

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

3.13.2. Switching > MLD Snooping Querier > VLAN Configuration



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

Use the buttons to perform the following tasks:

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

VLAN ID	The VLAN on which the MLD snooping querier is enabled. When enabling the MLD snooping querier on a VLAN, use this menu to select the desired VLAN. Only VLANs that have been configured on the system and are not already enabled for the MLD snooping querier appear in the menu. When modifying MLD snooping querier settings, this field identifies the VLAN that is being configured.
Querier Election Participation	The participation mode for the MLD snooping querier election process: • Enabled – The MLD snooping querier on this VLAN participates in the querier election process when it discovers the presence of another querier in the VLAN. If the snooping querier finds that the other querier source 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 MLD snooping querier on this VLAN sees other queriers of the same version in the VLAN, the snooping querier moves to the non-querier state and stops sending periodic queries.

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

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

3.13.3. Switching > MLD Snooping Querier > VLAN Status

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

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 MLD 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 MLD 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 MLD 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 MLD protocol version of the last querier from which a query was snooped on the VLAN.
Max Response Time (Seconds)	The maximum response time to be used in the queries that are sent by the snooping querier.

3.14. Switching > Multicast Forwarding Database

3.14.1. Switching > Multicast Forwarding Database > 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.

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. • MLD Snooping – A layer 2 feature that allows the device to dynamically add or remove ports from IPv6 multicast groups by listening to MLD join and leave requests. • GMRP – Generic Address Resolution Protocol (GARP) Multicast Registration Protocol, which helps 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.

3.14.2. Switching > Multicast Forwarding Database > GMRP

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

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.

3.14.3. Switching > Multicast Forwarding Database > 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.

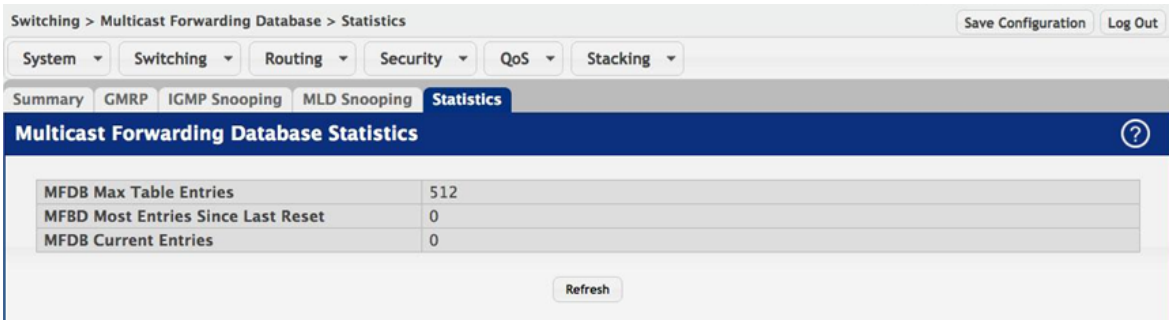
VLAN ID	The VLAN ID associated with the entry in the MFDB.
MAC Address	The multicast MAC address associated with the entry in the MFDB.
Type	The type of entry, which is one of the following: • Static – The entry has been manually added to the MFDB by an administrator. • Dynamic – The entry has been added 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.

3.14.4. Switching > Multicast Forwarding Database > MLD Snooping

This page displays the entries in the multicast forwarding database (MFDB) that were added because they were discovered by the MLD snooping feature. MLD snooping allows the device to dynamically add or remove ports from IPv6 multicast groups by listening to MLD join and leave requests.

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 MLD 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 MLD snooping entries from the MFDB table, click Clear Entries. The table is repopulated as new addresses are discovered by the MLD snooping feature.

3.14.5. Switching > Multicast Forwarding Database > Statistics

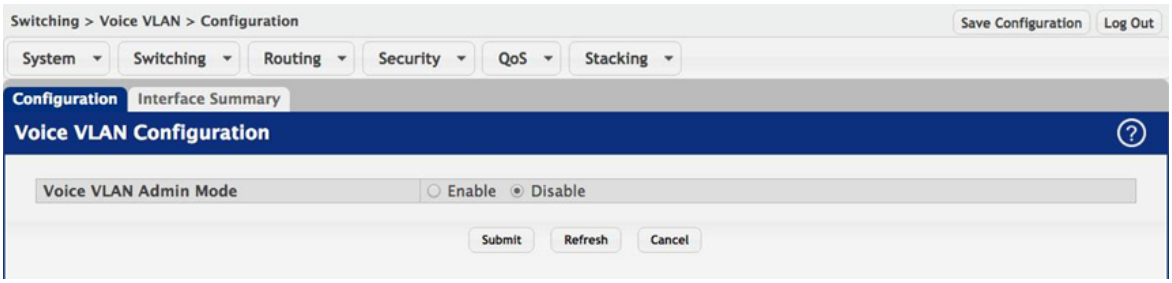


This page displays statistical information about the multicast forwarding database (MFDB).

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.

3.15. Switching > Voice VLAN

3.15.1. Switching > Voice VLAN > Configuration

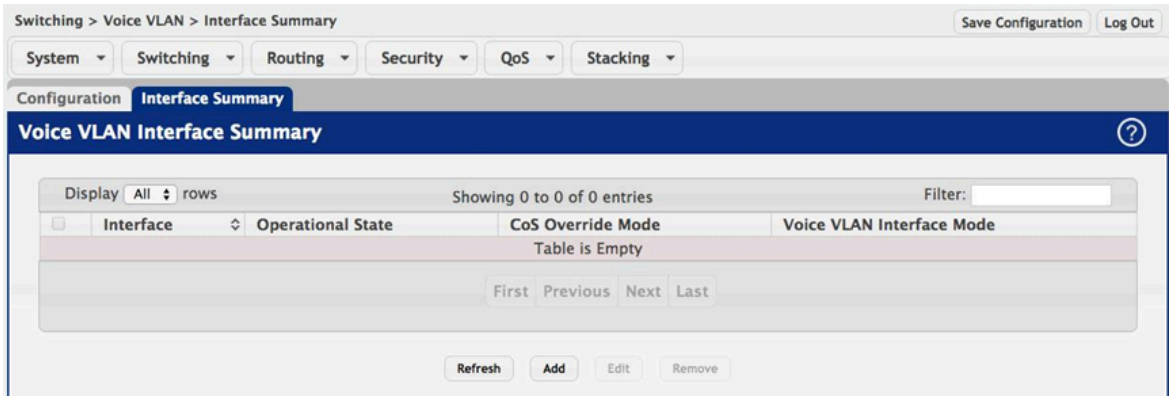


Use this page to control the administrative mode of the Voice VLAN feature, which enables ports to carry voice traffic that has a defined priority. Voice over IP (VoIP) traffic is inherently time-sensitive: for a network to provide acceptable service, the transmission rate is vital. The priority level enables the separation of voice and data traffic entering the port.

Voice VLAN 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.

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

3.15.2. Switching > Voice VLAN > 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.

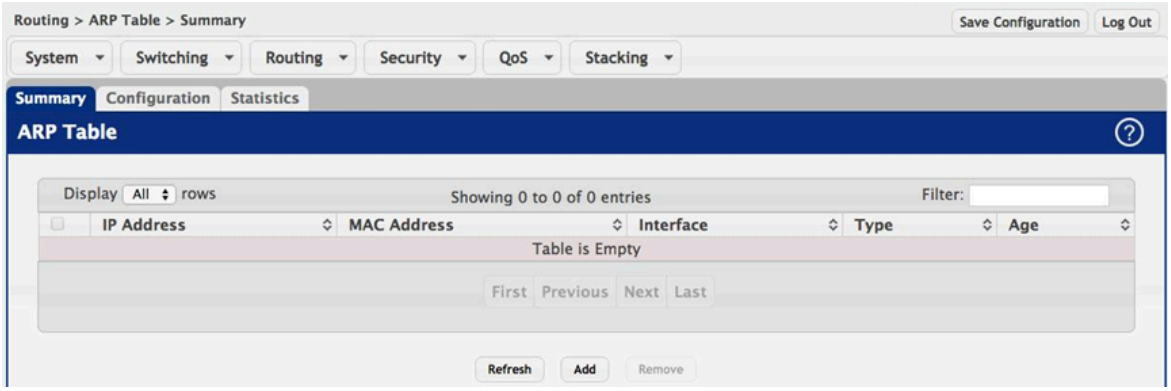
Interface	The interface associated with the rest of the data in the row. When adding a Voice VLAN configuration to a port, the Interface menu allows you to select the port to configure. Only interfaces that have not been configured with Voice VLAN settings can be selected from the menu.
Operational State	The operational status of the Voice VLAN feature on the interface. To be enabled, Voice VLAN must be globally enabled and enabled on the interface. Additionally, the interface must be up and have a link.
CoS Override Mode	The Class of Service override mode: • Enabled – The port ignores the 802.1p priority value in the Ethernet frames it receives from connected devices. • Disabled – The port trusts the priority value in the received frame.
Voice VLAN Interface Mode	Indicates how an IP phone connected to the port should send voice traffic: • VLAN ID – The IP phone will send voice traffic to the switch in the specified voice VLAN. • Dot1p – This option configures the IP phone to send traffic to the switch in the access VLAN tagged with a Layer2 CoS priority value. In other words, it will configure the phone to use IEEE 802.1p priority tagging for voice traffic and use the default (native) access VLAN (VLAN 0) to carry all traffic. • None – Normally switch will communicate the IP phone's voice VLAN using LLDP-MED. This option can be used to disable this behavior and allow the phone to use its own manual configuration to send untagged voice traffic. • Untagged – Use this option to instruct the IP phone to 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.

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

Chapter 4. Routing

4.1. Routing > ARP Table

4.1.1. Routing > ARP Table > Summary



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.

Use the buttons to perform the following tasks:

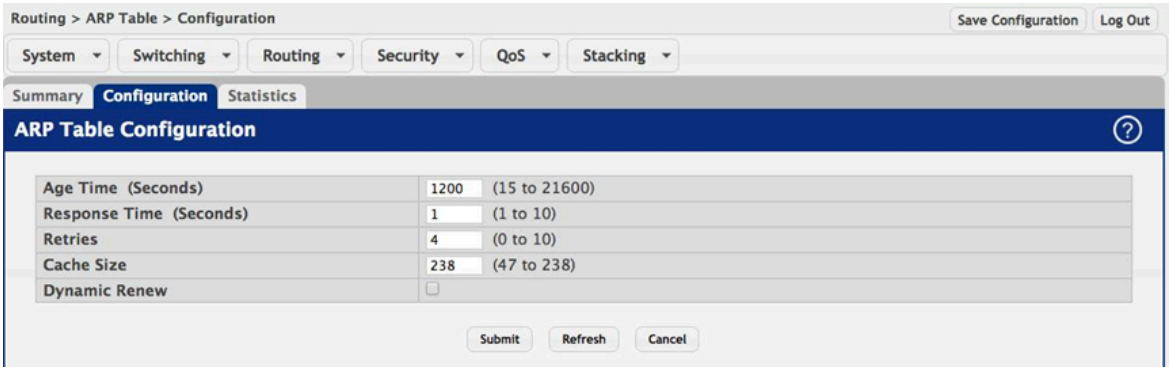
- To add a static ARP entry, click Add. The Add Static ARP Entry dialog box opens. Specify the new entry information in the available fields.
- To delete one or more ARP entries, select each entry to delete and click Remove. Note that ARP entries designated as Local cannot be removed.

IP Address	The IP address of a network host on a subnet attached to one of the device's routing interfaces. When adding a static ARP entry, specify the IP address for the entry after you click 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).

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

4.1.2. Routing > ARP Table > Configuration

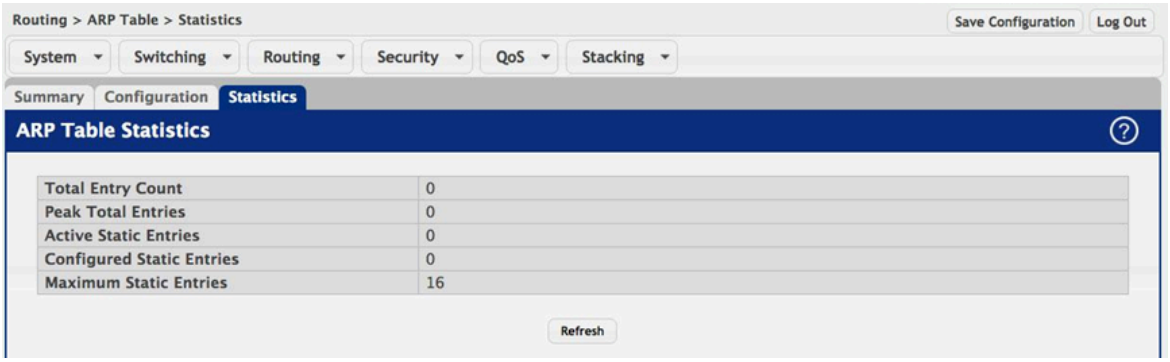


Use this page to configure ARP table settings.

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 does not include 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.

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

4.1.3. Routing > ARP Table > Statistics

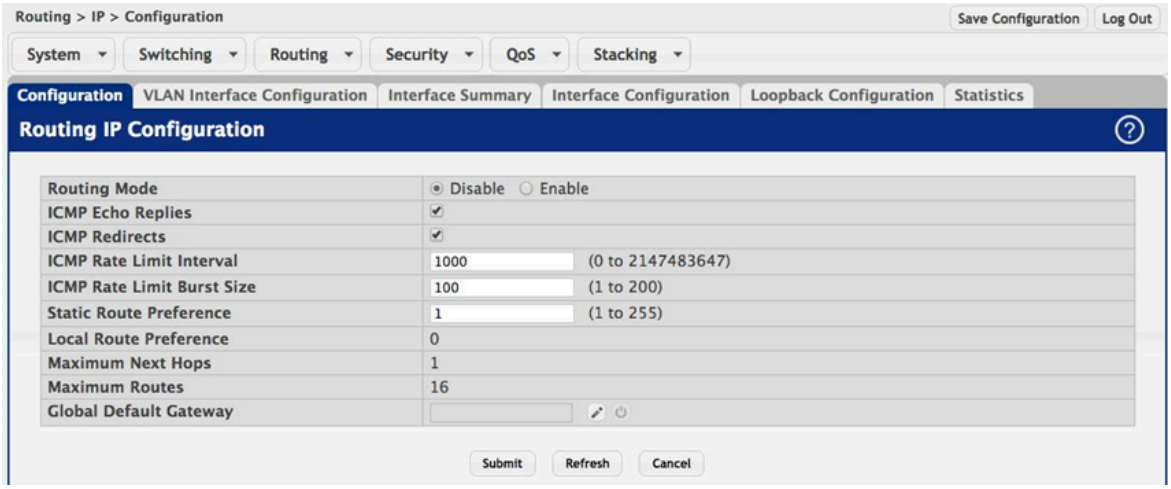


This page displays information about the number and type of entries in the system ARP table. The ARP table contains entries that map IP addresses to MAC addresses.

Total Entry Count	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.

4.2. Routing > IP

4.2.1. Routing > IP > Configuration



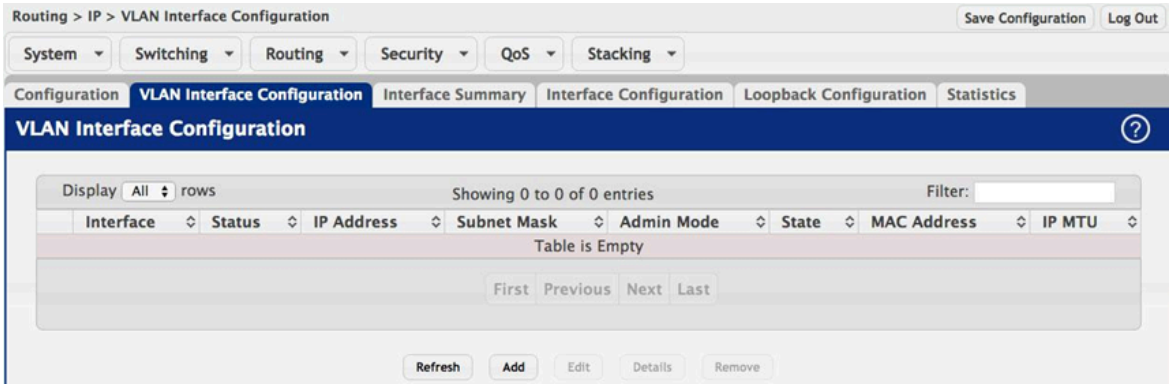
Use this page to configure global routing settings on the device. Routing provides a means of transmitting IP packets between subnets on the network. Routing configuration is necessary only if the device is used as a Layer 3 device that routes packets between subnets. If the device is used as a Layer 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	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.

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

4.2.2. Routing > IP > VLAN Interface Configuration



This page shows summary information about the VLAN routing configuration. To create a VLAN routing interface, click Add. To delete a VLAN routing interface, select the interface to remove and click Remove. 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.

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.
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.

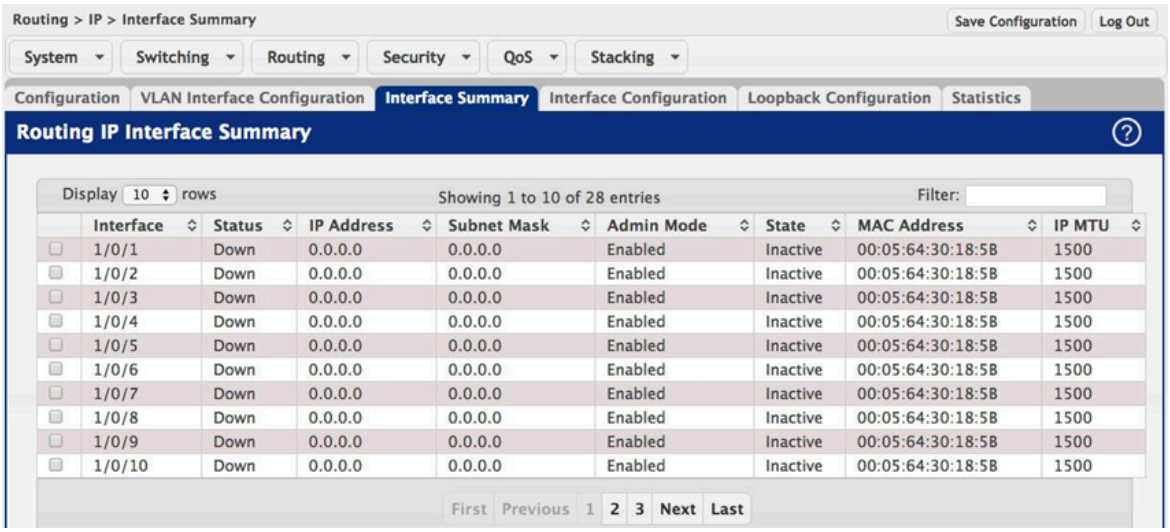
After you click **Add**, the **Add window** opens and ask to enter the VLAN ID for the VLAN routing interface.

After you click **Remove**, the **Remove window** opens and ask to confirm if this VLAN routing interface is to be removed.

After you click **Edit**, the navigation is redidected to the respective configuration page for the selected interface based on interface type.

After you click **Details**, the **Details window** opens and displays detailed routing information for the selected interface.

4.2.3. Routing > IP > 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.

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.
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.

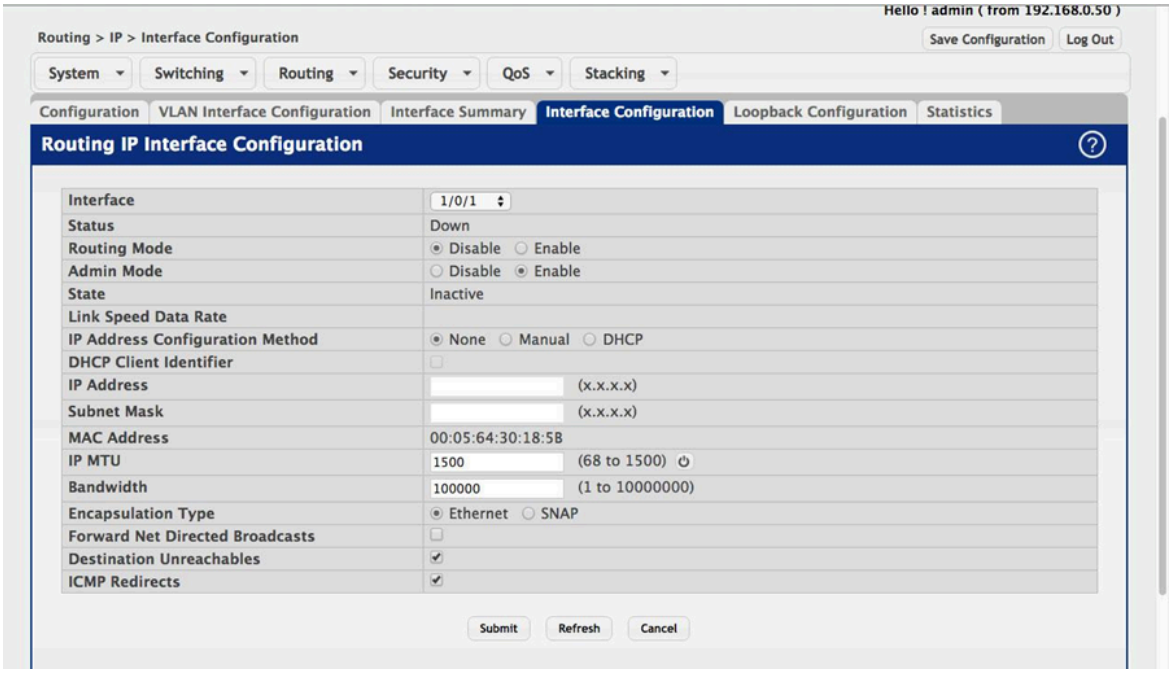
After you click **Edit**, the navigation is redidected to the respective configuration page for the selected interface based on interface type [loopback/non-loopback].

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 Broadcasts	Indicates how the interface handles network-directed broadcast packets. A network-directed broadcast is a broadcast directed to a specific subnet. The possible values are as follows: • Enabled – Network directed broadcasts are forwarded. • Disabled – Network directed broadcasts are dropped.
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.

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

4.2.4. Routing > IP > Interface Configuration



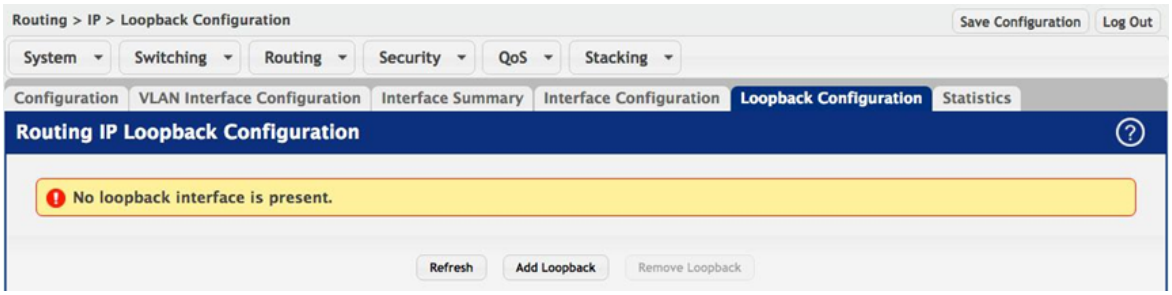
Use this page to configure the IP routing settings for each non-loopback interface.

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.
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.

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

4.2.5. Routing > IP > Loopback Configuration



Use this page to configure the IP routing settings for each loopback interface.

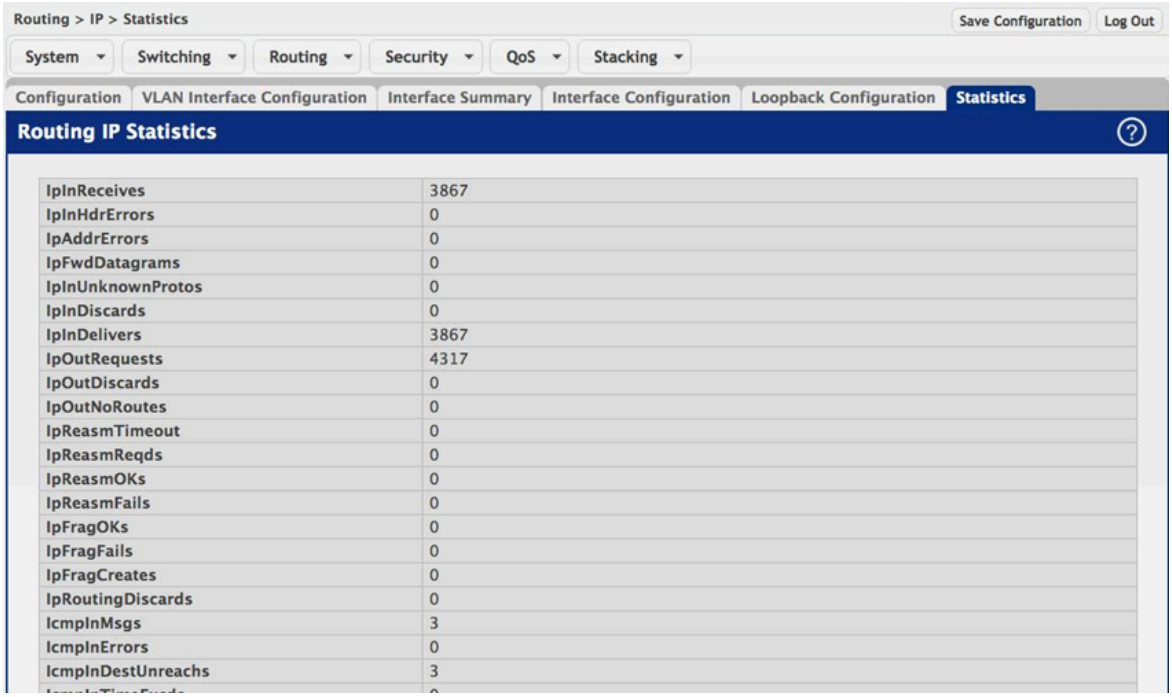
Interface	The menu contains all loopback interfaces that can be configured for routing. To configure routing settings for an interface, select it from the menu and then configure the rest of the settings on the page.
IP Address	The IP address of the loopback interface.
Subnet Mask	The IP subnet mask for the interface (also known as the network mask or netmask).

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.

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

4.2.6. Routing > IP > 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.

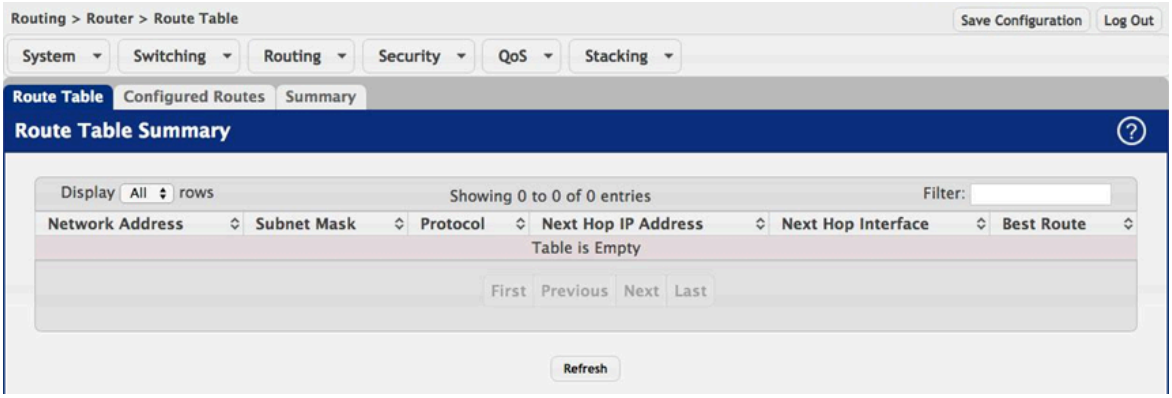
IpInReceives	The total number of input datagrams received from all routing interfaces, including those datagrams received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live 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.

4.3. Routing > Router

4.3.1. Routing > Router > 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	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.
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.

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

4.3.2. Routing > Router > Configured Routes

Use this page to configure the default route and static 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.

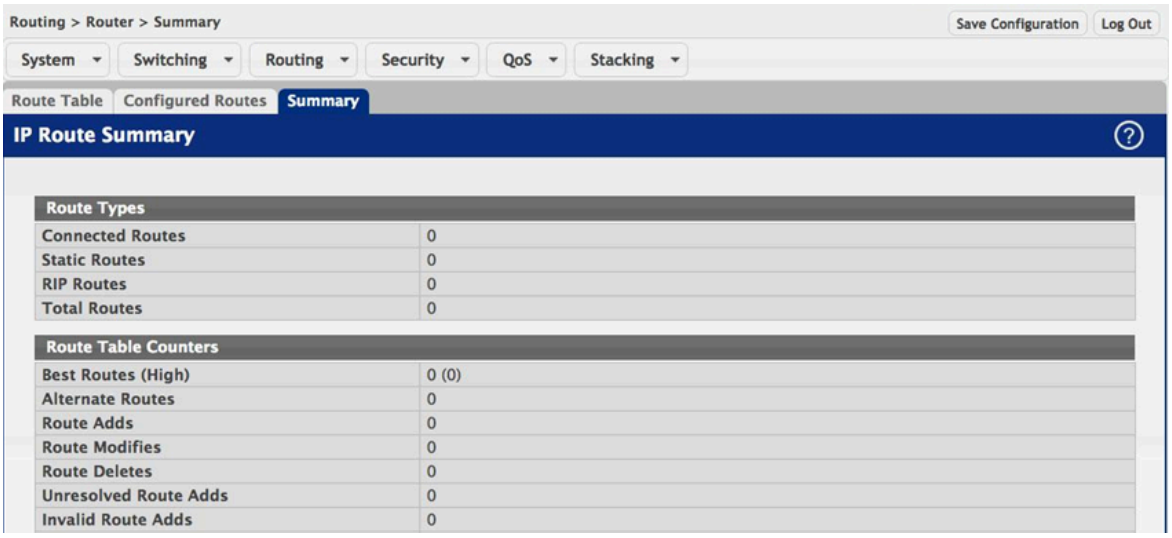
Network Address	The IP route prefix for the destination network. This IP address must contain only the network portion of the address and not the host bits. When adding a default route, this field is not available.
Subnet Mask	The IP subnet mask (also known as the network mask or netmask) associated 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.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination.
Preference	The preference of the route. A lower preference value indicates a more preferred route. When the routing table has more than one route to the same network, the device selects the route with the best (lowest) route preference.

After you click Add, the Add Route window opens and allows you to configure routes. The fields that can be configured depend on the route type. The following information describes the additional field available in the Add Route window.

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.

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

4.3.3. Routing > Router > Summary



This page displays summary information about the entries in the IP routing table.

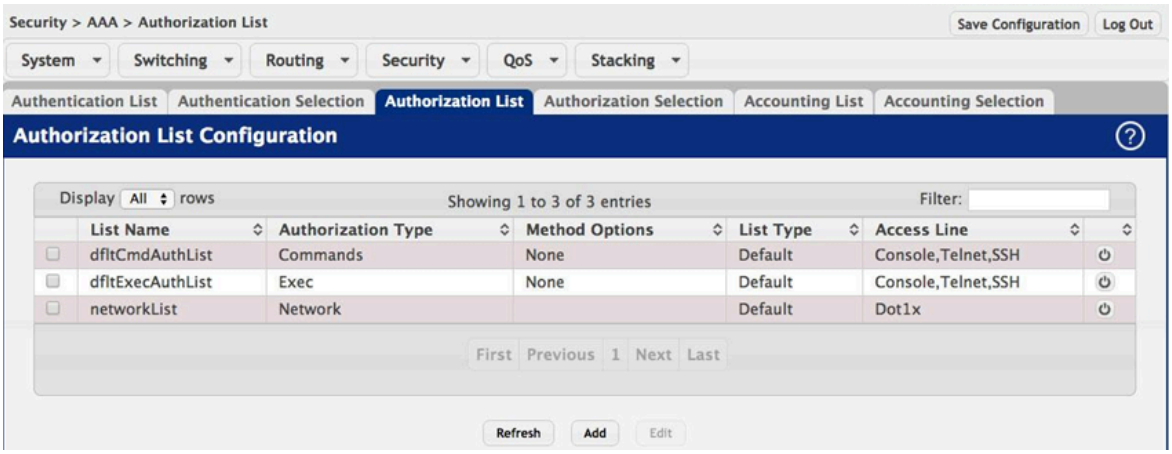
Connected Routes	The total number of connected routes in the IP routing table.
Static Routes	The total number of static routes in the IP routing table.
RIP Routes	The total number of routes installed by the RIP protocol.
Total Routes	The total number of routes in the routing table.
Best Routes (High)	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.
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.

Chapter 5. Security

5.1. Security > AAA

5.1.1. Security > AAA > Authentication List



Use this 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.

Use the buttons to perform the following tasks:

- To configure a new authentication 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 authentication 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 authentication list to the factory default values, click the Reset icon associated with the entry. You must confirm the action before the entry is reset.

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. • IAS – Uses the local Internal Authentication Server (IAS) database for 802.1X port-based authentication. • 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. • None – No authentication is used. • 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 to verify the user's credentials. • Deny – Denies 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.

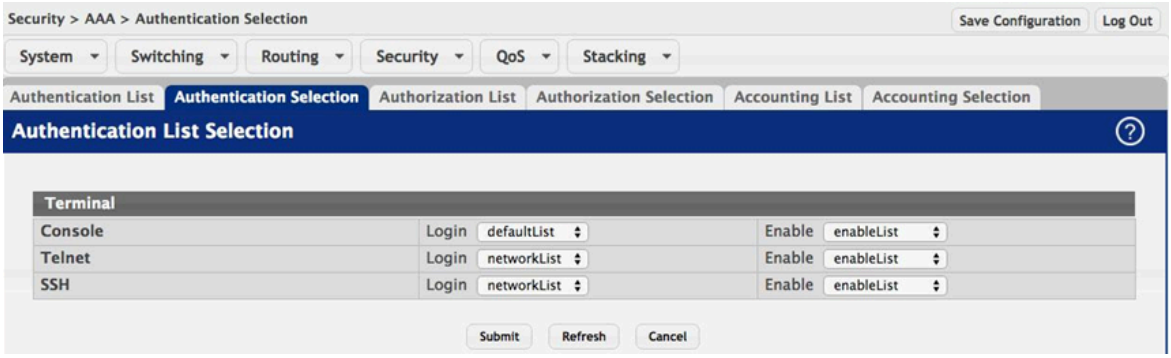
After you click Add or Edit, a window opens and allows you to configure authentication list settings. When adding an authentication list, you can configure the List Name and Access Type fields as well as the Authentication Methods. When editing an existing authentication list, only the Authentication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

Authentication Methods	This area includes the Available Methods and Selected Methods fields. For lists that allow multiple authentication methods, the order in which

	you move the method from the Available Methods field to the Selected Methods field determines the order in which the device attempts to authenticate the user. For example, if the selected methods are Enable, followed by None, a user who fails to authenticate with the enable password is granted access anyway because the final method indicates that no authentication is required.
Available Methods	The authentication methods that can be used for the authentication list. Not all authentication methods are available for all lists. To set the authentication method, select the method in the Available Methods field and click the right arrow to move it into the Selected Methods field.
Selected Methods	The authentication methods currently configured for the list. When multiple methods are in this field, the order in which the methods are listed is the order in which the methods will be used to authenticate a user. If the user fails to be authenticated using the first method, the device attempts to verify the user's credentials by using the next method in the list. No authentication methods can be added after None. To remove a method from this field, select it and click the left arrow to return it to the Available Methods area.

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

5.1.2. Security > AAA > Authentication Selection



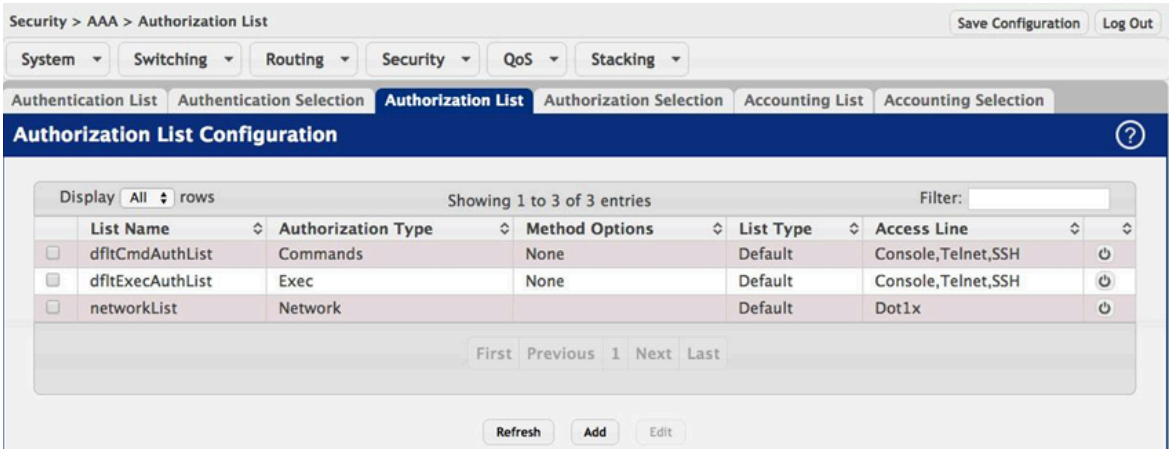
Use this page to associate an authentication list with each CLI-based access method (Console, Telnet, and SSH). Each access method has the following two authentication lists associated with it:

- 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.

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.
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.

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

5.1.3. Security > AAA > 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.

Use the buttons to perform the following tasks:

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

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 applies to port-based access (IEEE 802.1X) rather than access to the CLI.
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.

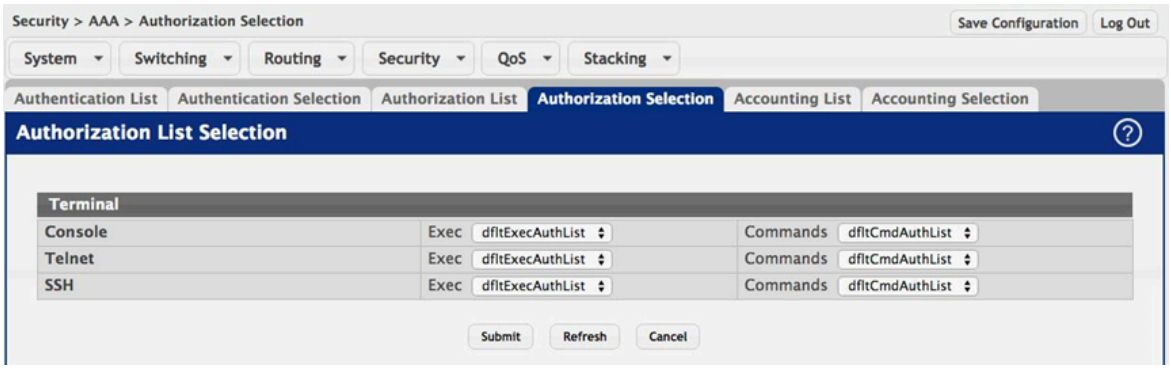
After you click Add or Edit, a window opens and allows you to configure authorization list settings. When adding an authorization list, you can configure the List Name and Authorization Type fields as well as the Authorization Methods. When editing an existing authentication list, only the Authorization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

Authorization Methods	This area includes the Available Methods and Selected Methods fields. For lists that allow multiple authorization methods, the order in which you move the method from the Available Methods field to the Selected

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

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

5.1.4. Security > AAA > Authorization Selection



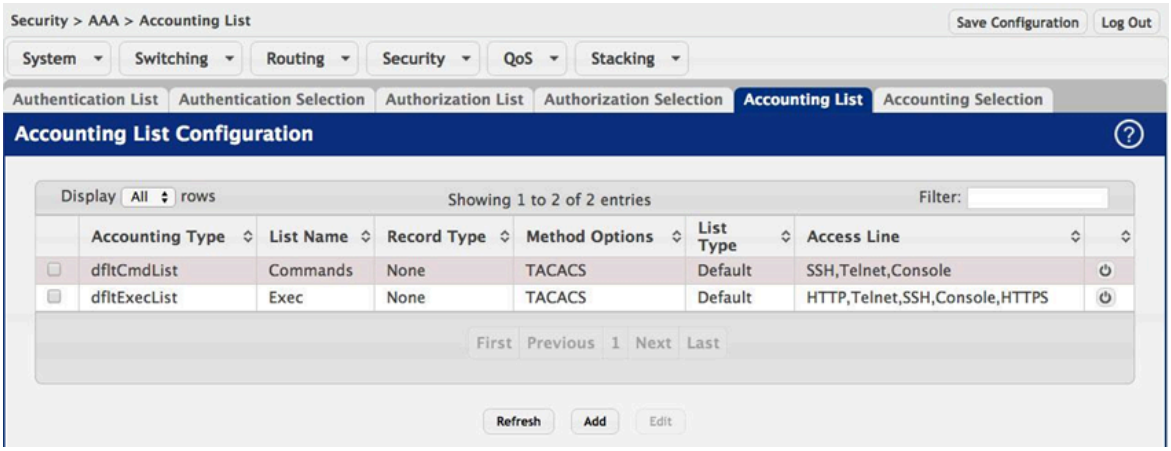
Use this page to associate an authorization list with each CLI-based access method (Console, Telnet, and SSH). Each access method has the following two authorization lists associated with it:

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

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.

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

5.1.5. Security > AAA > 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. You must confirm the action before the entry is reset.

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:

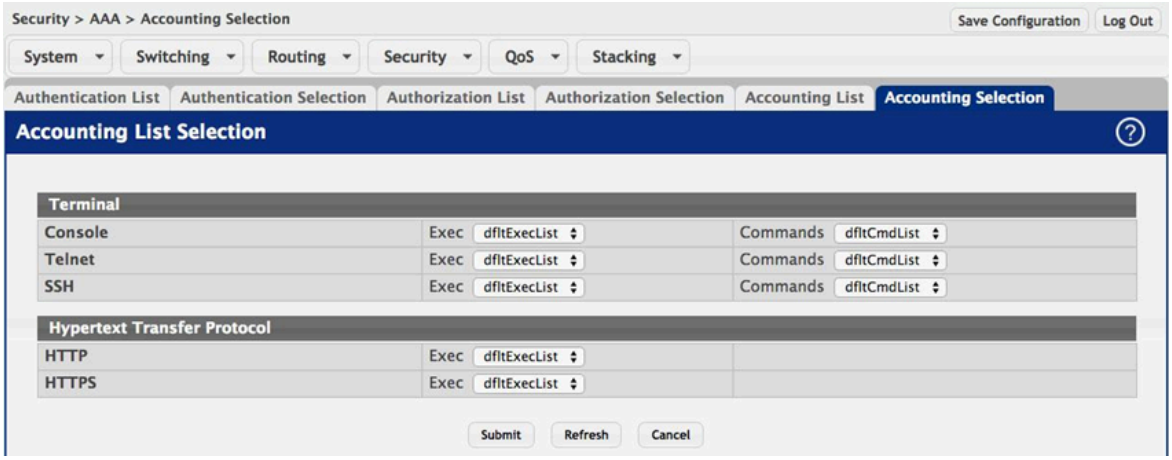
	• StartStop – Accounting notifications are sent at the beginning and at the end of an exec session or a user-executed command. User activity does not wait for the accounting notification to be recorded at the AAA server. • StopOnly – Accounting notifications are sent at the end of an exec session or a user-executed command.
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.

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

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

5.1.6. Security > AAA > Accounting Selection



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

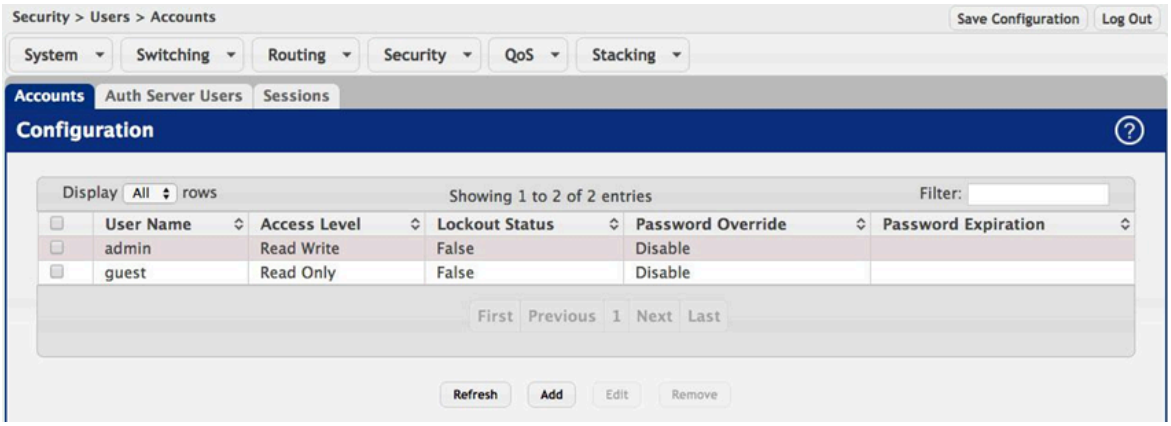
- Exec – The accounting list to record user login and logout times.
- Commands – The accounting list to record which actions a user takes on the system, such as page views or configuration changes. This list also records the time when the action occurred. For Terminal access methods, this list records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

Terminal	The access methods in this section are CLI-based.
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	The access methods in this section are through a web browser.
HTTP	The Exec accounting list and the Commands accounting list to apply to users who access the web-based management interface by using HTTP.
HTTPS	The Exec accounting list and the Commands accounting list to apply to users who access the web-based management interface by using secure HTTP (HTTPS).

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

5.2. Security > Users

5.2.1. Security > Users > 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.

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: • Read Write - The user can view and modify the configuration. • Read Only - The user can view the configuration but cannot modify any fields. • Suspended - 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.

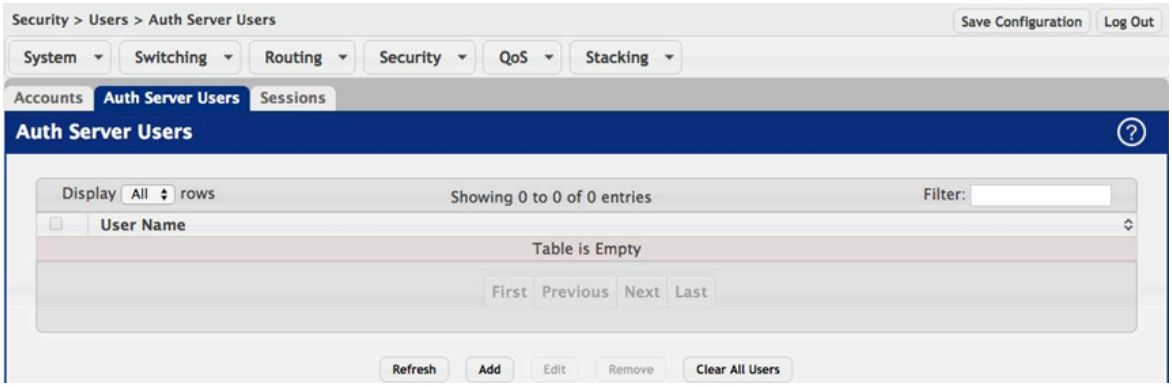
Password Expiration	Indicates the current expiration date (if any) of the password.

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.

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

5.2.2. Security > Users > Auth Server Users



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.

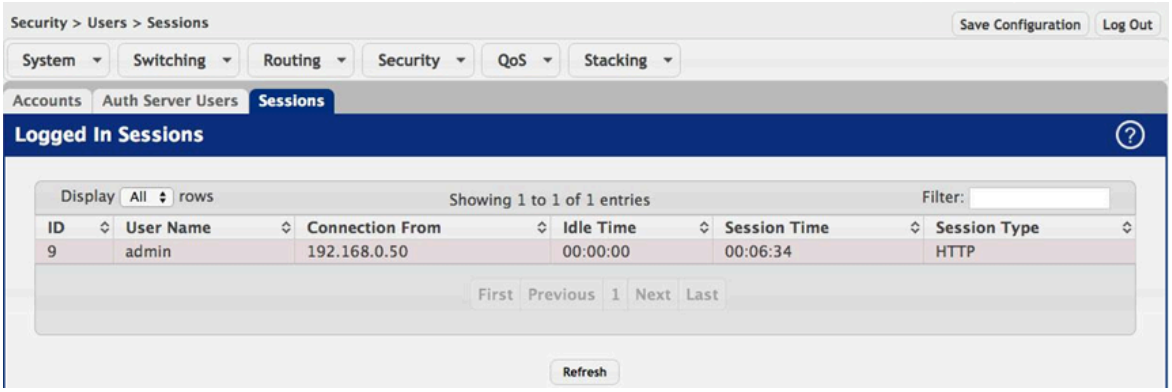
User Name	A unique name used to identify this user account. You configure the User Name when you add a new user.

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.

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.

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

5.2.3. Security > Users > Sessions

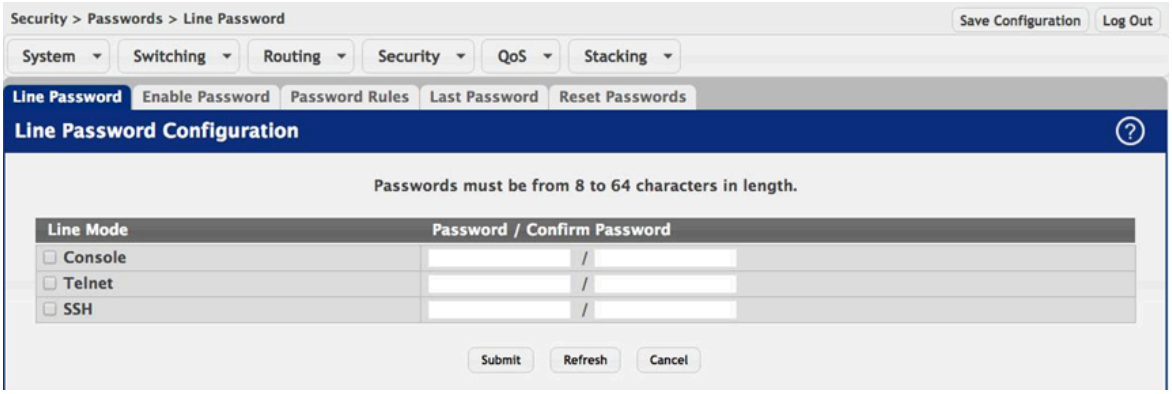


This page identifies the users that are logged in to the management interface of the device. The page also provides information about their connections.

ID	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.

5.3. Security > Passwords

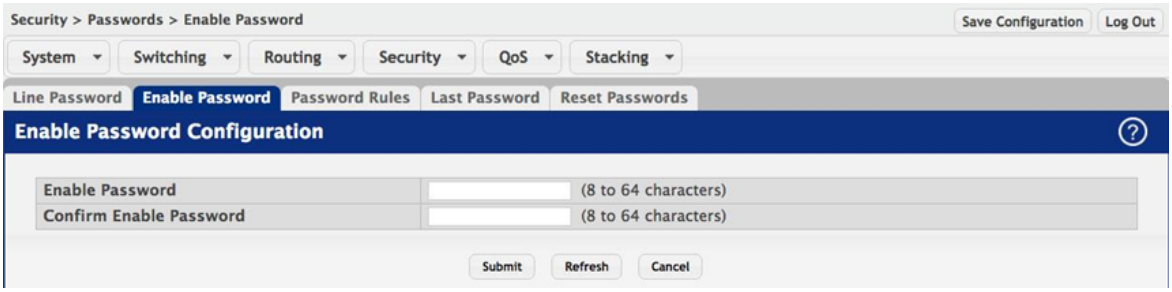
5.3.1. Security > Passwords > Line Password



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.

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

5.3.2. Security > Passwords > Enable Password

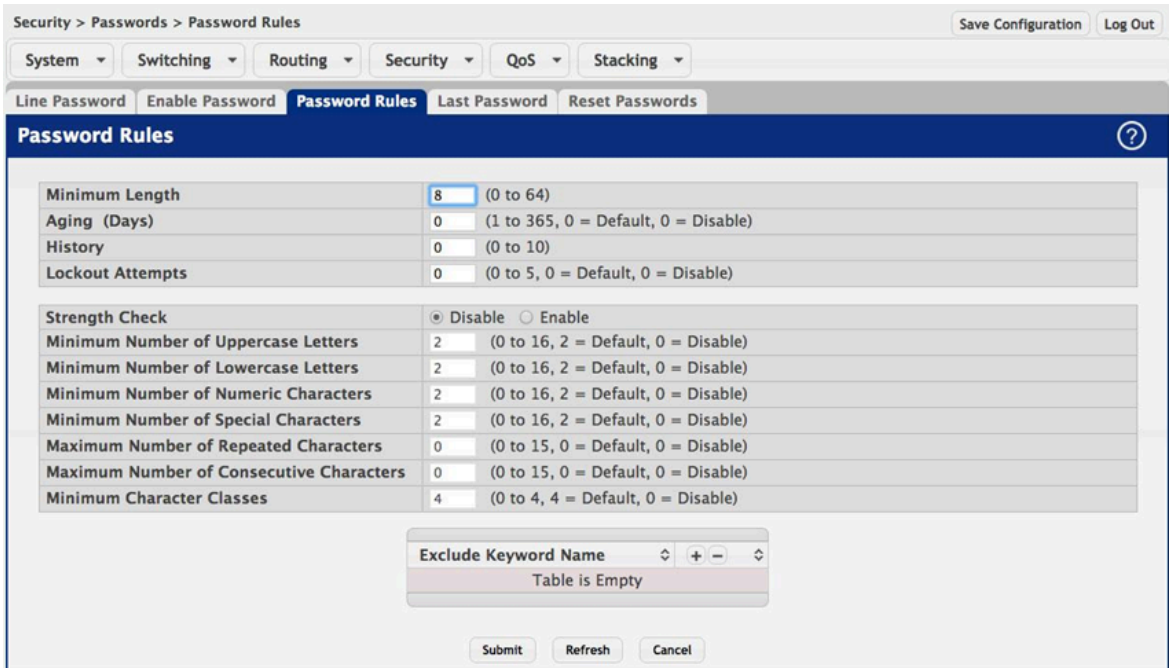


Use this page to set a local password to control CLI access to privileged levels.

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.

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

5.3.3. Security > Passwords > Password Rules



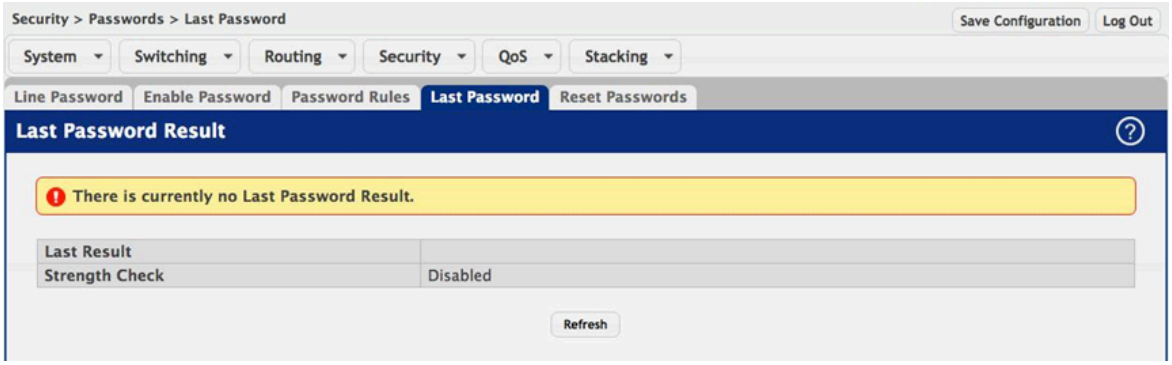
Use this page to configure rules for locally-administered passwords. The rules you set determine the strength of local passwords that device users can associate with their usernames. The strength of a password is a function of length, complexity, and randomness.

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.

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

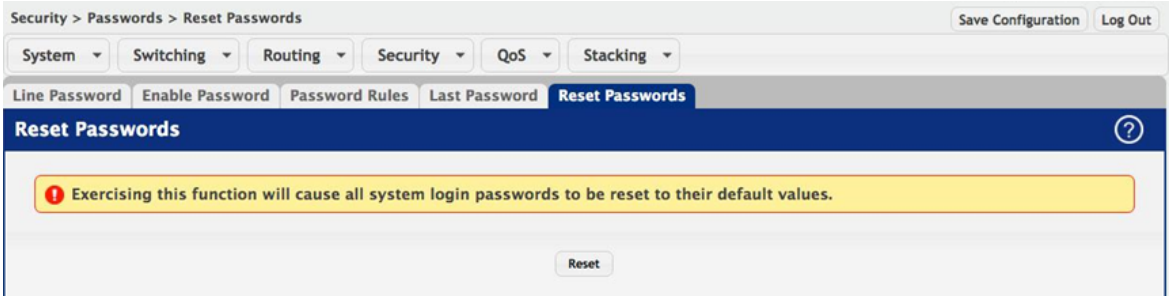
5.3.4. Security > Passwords > Last Password



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 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.

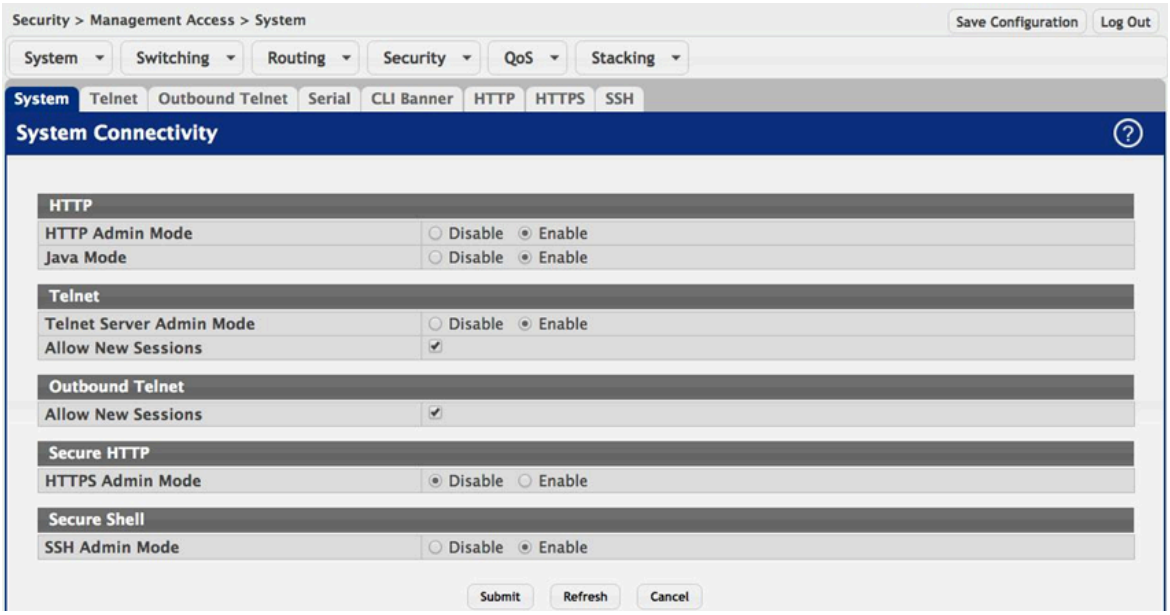
5.3.5. Security > Passwords > Reset Passwords



Reset (Button)	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.

5.4. Security > Management Access

5.4.1. Security > Management Access > System



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

Table 5.1. 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.
Java Mode	Enables or disables the port that Java uses. When this mode is disabled, any feature on the device that uses Java is not available and cannot be viewed by using a web browser.

Table 5.2. 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.

Table 5.3. Outbound Telnet

Allow New Sessions	Enables or disables new telnet sessions. When this option is disabled, the system does not accept any new telnet sessions, but existing telnet sessions are unaffected.

Table 5.4. Secure HTTP

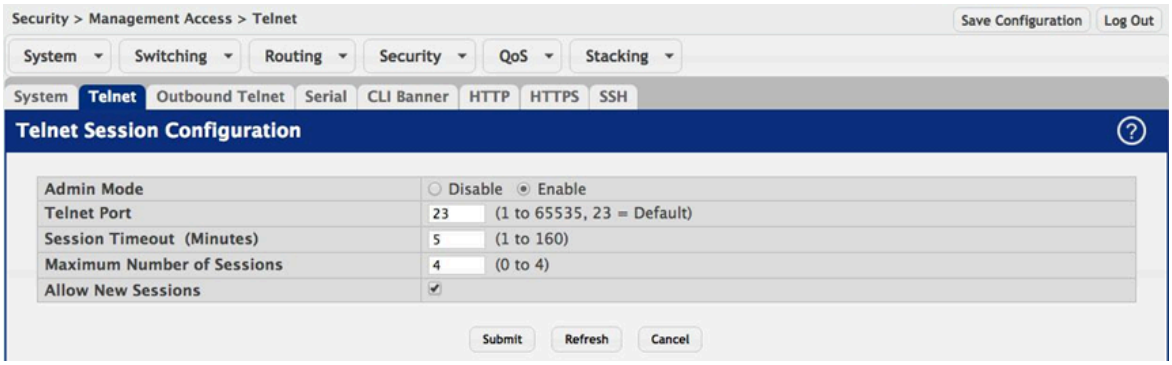
HTTPS Admin Mode	Enables or disables the administrative mode of secure HTTP. When this mode is enabled, the device management interface can be accessed through a web browser using the HTTPS protocol.

Table 5.5. 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.

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

5.4.2. Security > Management Access > Telnet



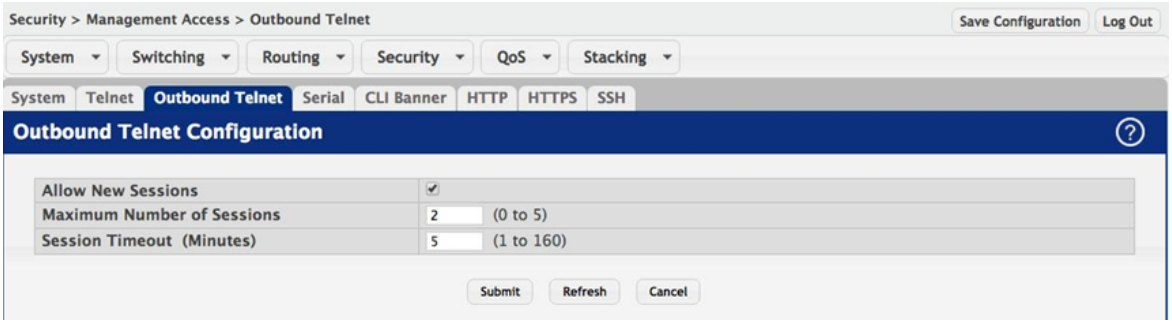
This page displays the current value of the telnet configuration parameters for the device. A user having sufficient privilege level may change the values shown on this page.

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.  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).

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

5.4.3. Security > Management Access > Outbound Telnet

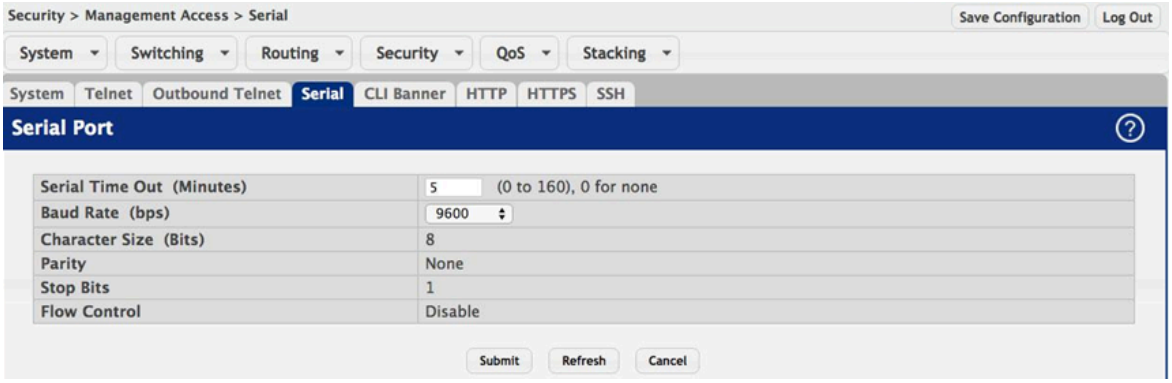


This page displays the current value of the outbound Telnet settings on the device. An outbound Telnet session is a Telnet session initiated from the CLI of the device to the Telnet client on a remote device.

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

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

5.4.4. Security > Management Access > Serial

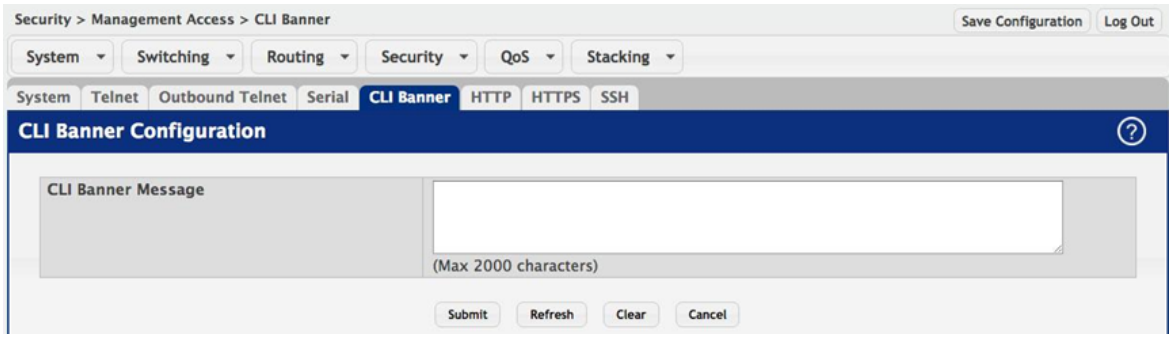


The Serial Port page displays the serial (console) port settings for the device. If you connect a terminal or PC to the device through the serial port, configure the terminal or terminal-emulation software with the settings that are displayed on this page to access the device command-line interface (CLI).

Serial 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.

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

5.4.5. Security > Management Access > CLI Banner

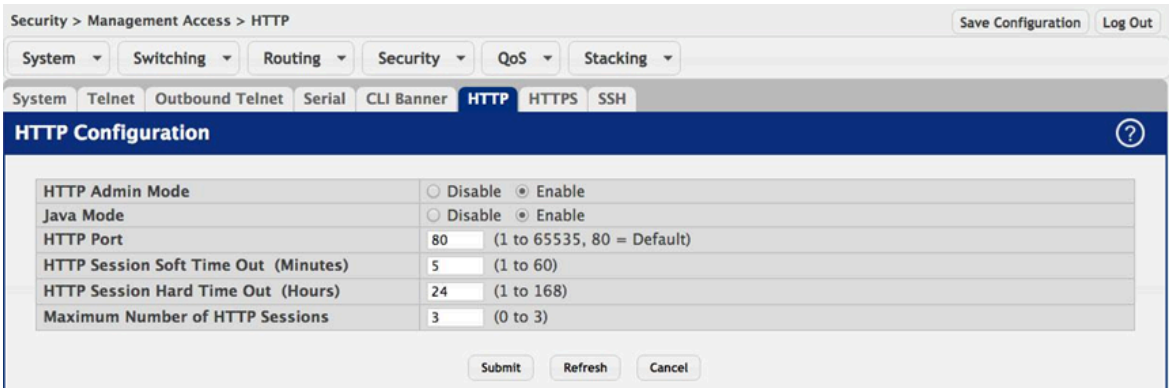


Use this page to configure the command-line interface (CLI) banner message that displays when a user connects to the device using a serial, telnet, or SSH session.

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.

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

5.4.6. Security > Management Access > HTTP



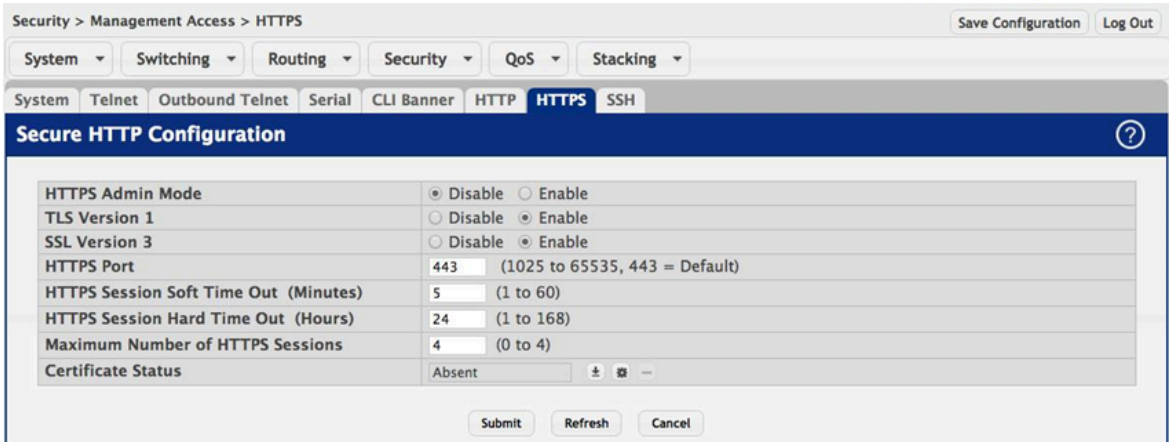
Use this page to view and modify the HTTP settings on the device. HTTP allows web-based management access to the device from an administrative system.

HTTP Admin Mode	Enables or disables the HTTP administrative mode. When enabled, the device can be accessed through a web browser using the HTTP protocol.
Java Mode	Enables or disables the Java mode. When enabled, the Java port (port 4242) is open. Port 4242 is used by certain applications within the system. This field applies to both HTTP and HTTPs connections.
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. 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.

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

5.4.7. Security > Management Access > HTTPS



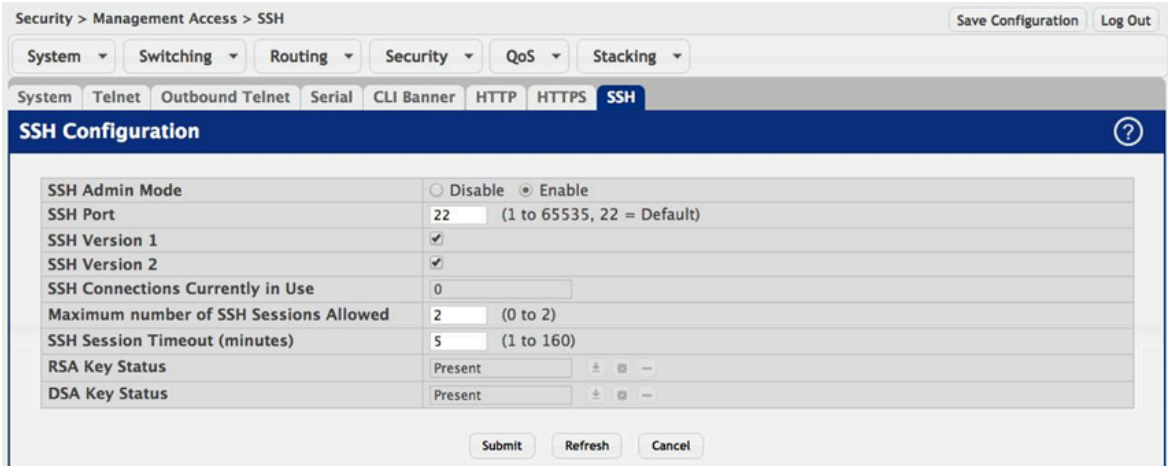
Use this page to view and modify the Secure HTTP (HTTPS) settings on the device. HTTPS increases the security of web-based management by encrypting communication between the administrative system and the device.

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.

	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.

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

5.4.8. Security > Management Access > 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.

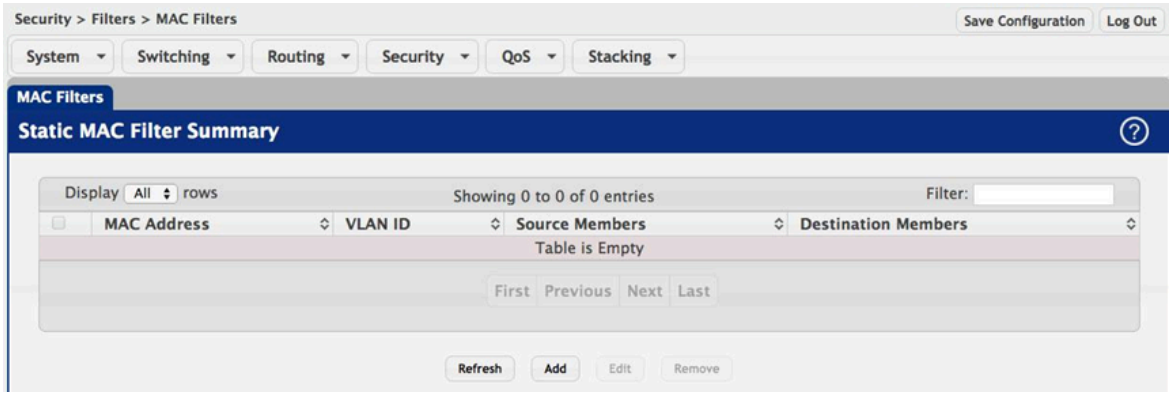
SSH Admin Mode	Enables or disables the SSH server administrative mode. When this mode is enabled, the device can be accessed by using an SSH client on a remote system.
SSH Port	The TCP port number on which the SSH server listens for requests. Existing SSH login sessions are not affected by a change in this value, although establishment of any new SSH sessions must use the new port number.  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.

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

5.5. Security > Filters

5.5.1. Security > Filters > 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.

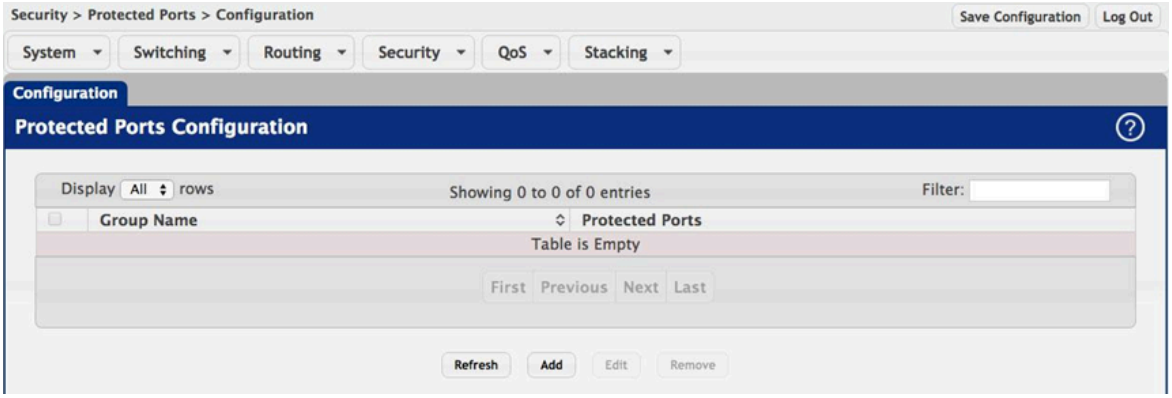
MAC Address	The MAC address of the filter. The destination MAC address of an Ethernet frame must match this value to be considered for the filter. When adding or editing a filter, note that you cannot configure the following MAC addresses in this field: • 00:00:00:00:00:00 • 01:80:C2:00:00:00 to 01:80:C2:FF:FF:FF • 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.

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

5.6. Security > Protected Ports

5.6.1. Security > Protected Ports > 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:

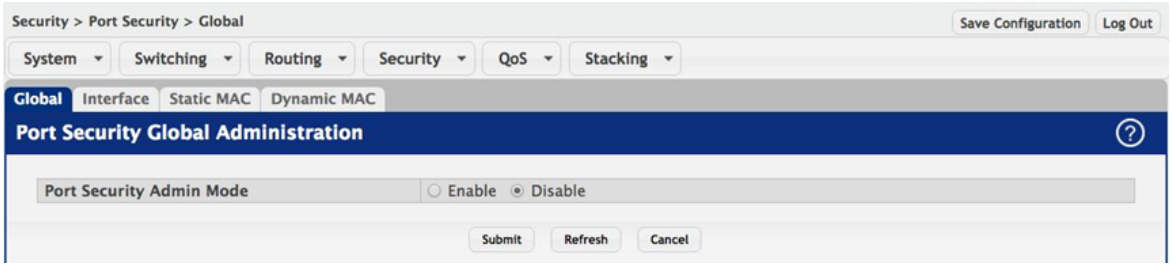
- To create a protected ports group and add ports to the group, click Add and configure the settings in the available fields.
- To change the name or the port members for an existing group, select the group to update and click Edit.
- To remove one or more protected ports groups, select each entry to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

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.

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

5.7. Security > Port Security

5.7.1. Security > Port Security > Global

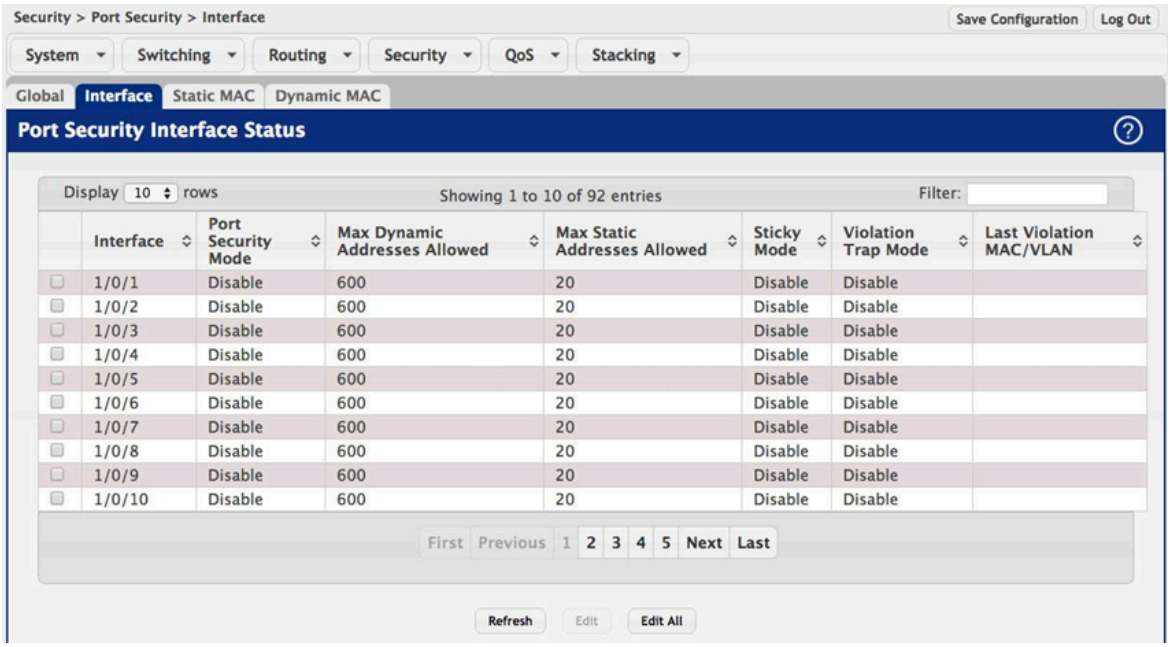


Use this page to configure the global administrative mode for the port security feature. Port security, which is also known as port MAC locking, allows you to limit the number of source MAC address that can be learned on a port. If a port reaches the configured limit, any other addresses beyond that 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 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.

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

5.7.2. Security > Port Security > Interface



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

Use the buttons to perform the following tasks:

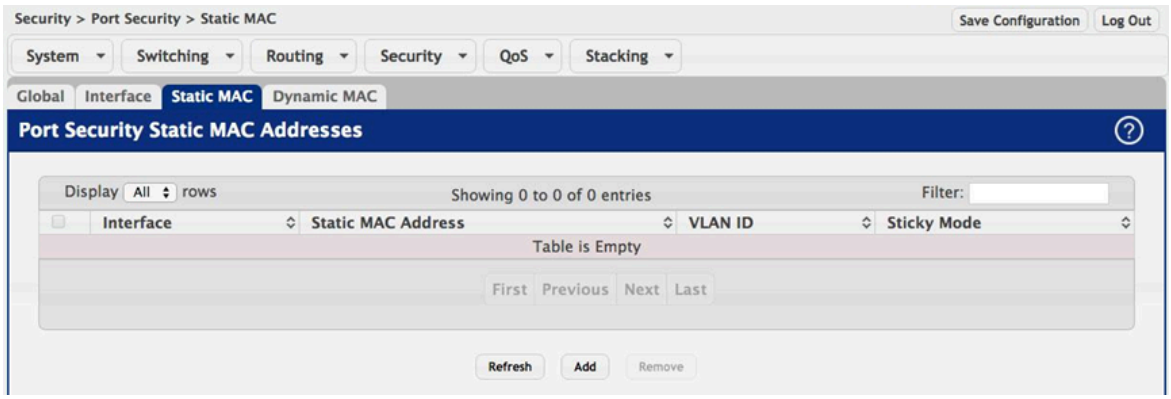
- To configure the settings for one or more interfaces, select each entry to modify and click Edit.
- To apply the same settings to all interfaces, click Edit All.

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.
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.

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

5.7.3. Security > Port Security > 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.

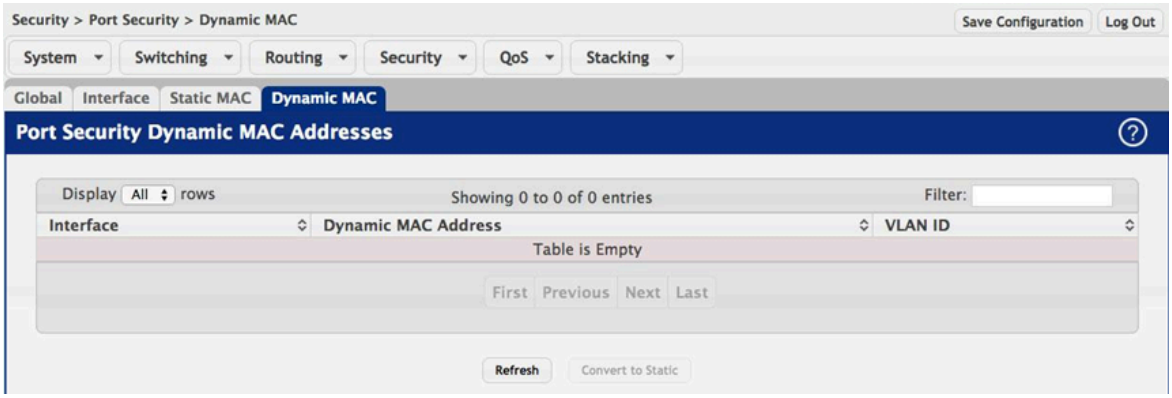
Use the buttons to perform the following tasks:

- 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	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.

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

5.7.4. Security > Port Security > 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

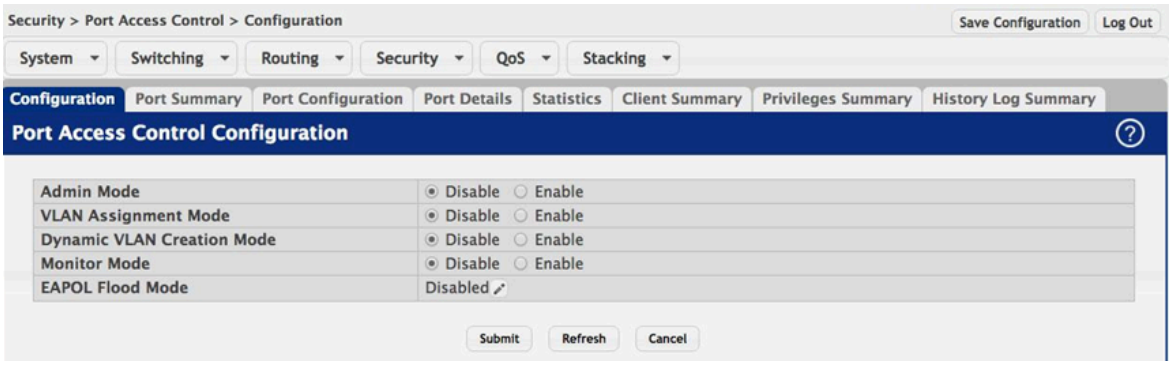
dynamically-locked MAC addresses to convert, then the addresses are converted in the order in which they were learned until the number of allowed static MAC address entries is reached.

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.

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

5.8. Security > Port Access Control

5.8.1. Security > Port Access Control > Configuration



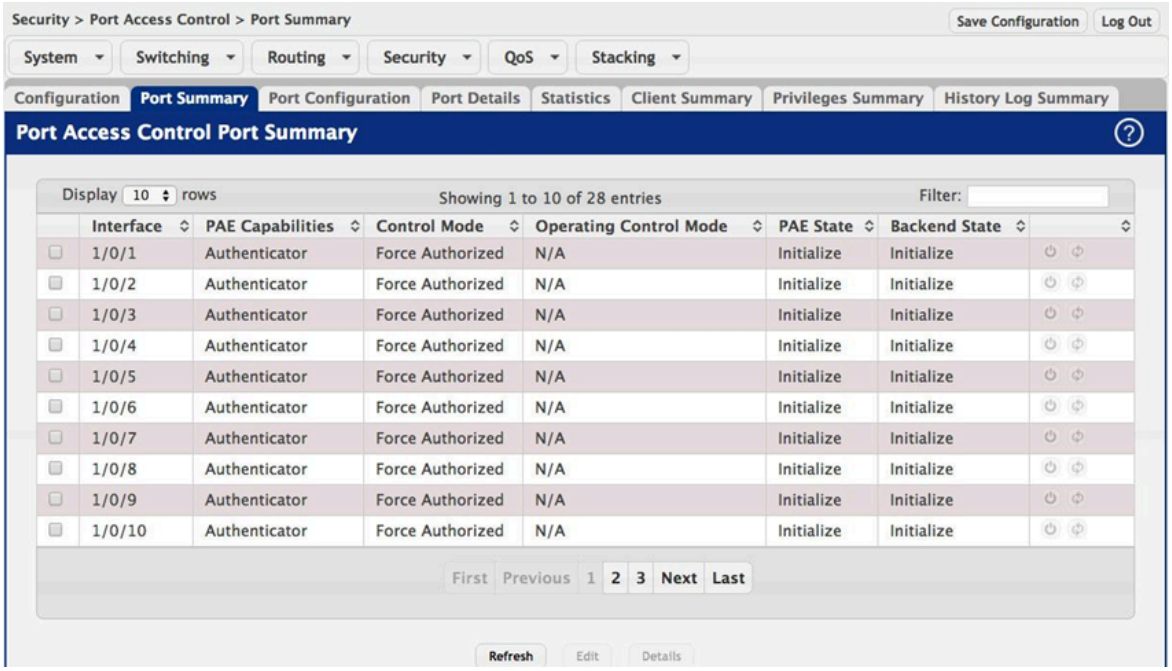
Use this page to configure the global Port Access Control settings on the device. The port-based access control feature uses IEEE 802.1X to enable the authentication of system users through a local internal server or an external server. Only authenticated and approved system users can transmit and receive 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.

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.

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

5.8.2. Security > Port Access Control > 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:

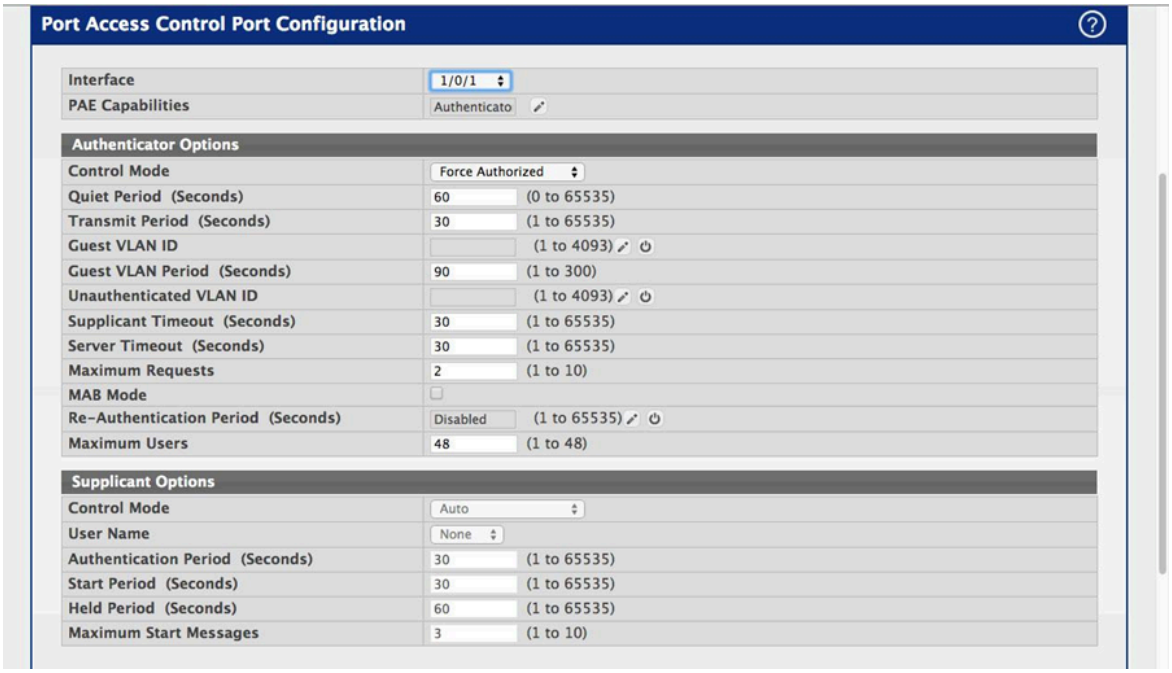
- To change the port-based access control settings for a port, select the port to configure and click Edit. You are automatically redirected to the Port Access Control Port Configuration page for the selected port.
- To view additional information about the port-based access control settings for a port, 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.

Interface	The interface associated with the rest of the data in the row.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following:

	• Authenticator – The port enforces authentication and passes authentication information from a remote supplicant (similar to a client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access. • Supplicant – The port must be granted permission by the authentication server before it can access the remote authenticator port.
Control Mode	The port-based access control mode configured on the port, which is one of the following: • Auto – The port is unauthorized until a successful authentication exchange has taken place. • Force Unauthorized – The port ignores supplicant authentication attempts and does not provide authentication services to the client. • Force Authorized – The port sends and receives normal traffic without client port-based authentication. • MAC-Based – This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses.
Operating Control Mode	The control mode under which the port is actually operating, which is one of the following: • Auto • Force Unauthorized • Force Authorized • MAC-Based • N/A If the mode is N/A, port-based access control is not applicable to the port. If the port is in detached state it cannot participate in port access control. Additionally, if port-based access control is globally disabled, the status for all ports is N/A.
PAE State	The current state of the authenticator PAE state machine, which is the 802.1X process that controls access to the port. The state can be one of the following: • Initialize • Disconnected • Connecting • Authenticating

	• Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized
Backend State	The current state of the 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.

5.8.3. Security > Port Access Control > Port Configuration



Use this page to configure the port-based authentication settings for each port.

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.

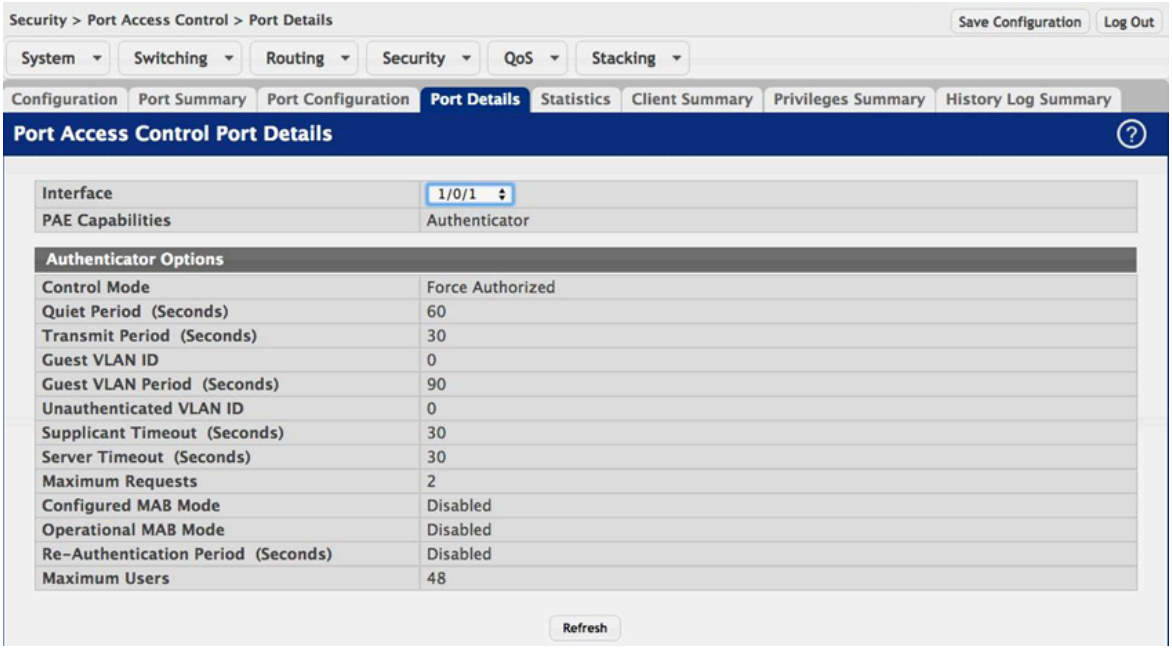
Authenticator Options	The fields in this section can be changed only when the selected port is configured as an authenticator port (that is, the PAE Capabilities field is set to Authenticator).
Control Mode	The port-based access control mode on the port, which is one of the following:

	• Auto – The port is unauthorized until a successful authentication exchange has taken place. • Force Unauthorized – The port ignores supplicant authentication attempts and does not provide authentication services to the client. • Force Authorized – The port sends and receives normal traffic without client port-based authentication. • 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	The fields in this section can be changed only when the selected port is configured as a supplicant port (that is, the PAE Capabilities field is set to Supplicant).
Control Mode	The port-based access control mode on the port, which is one of the following: • Auto – The port is in an unauthorized state until a successful authentication exchange has taken place between the supplicant port, the authenticator port, and the authentication server. • Force Unauthorized – The port is placed into an unauthorized state and is automatically denied system access. • Force Authorized – The port is placed into an authorized state and does not require client port-based authentication to be able to send and receive traffic.
User Name	The name the port uses to identify itself as a supplicant to the authenticator port. The menu includes the users that are configured for system management. When authenticating, the supplicant provides the password associated with the selected User Name.
Authentication Period	The amount of time the supplicant port waits to receive a challenge from the authentication server. If the configured Authentication Period expires, the supplicant retransmits the authentication request until it is authenticated or has sent the number of messages configured in the Maximum Start Messages field.
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.

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

5.8.4. Security > Port Access Control > Port Details



Use this page to view 802.1X information for a specific port.

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.

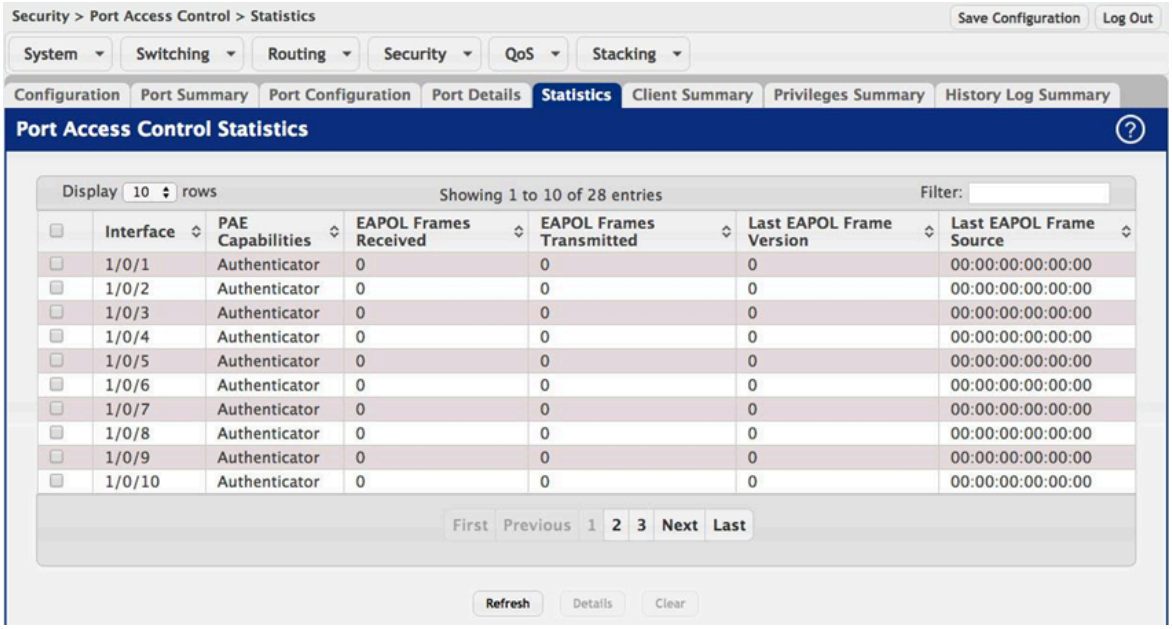
Authenticator Options	The fields in this section provide information about the settings that apply to the port when it is configured as an 802.1X authenticator.
Control Mode	The port-based access control mode on the port, which is one of the following: • Auto – The port is unauthorized until a successful authentication exchange has taken place. • Force Unauthorized – The port ignores supplicant authentication attempts and does not provide authentication services to the client. • Force Authorized – The port sends and receives normal traffic without client port-based authentication.

	• 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.
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	The fields in this section provide information about the settings that apply to the port when it is configured as an 802.1X supplicant.
Control Mode	The port-based access control mode on the port, which is one of the following: • Auto – The port is in an unauthorized state until a successful authentication exchange has taken place between the supplicant port, the authenticator port, and the authentication server.

	• Force Unauthorized – The port is placed into an unauthorized state and is automatically denied system access. • Force Authorized – The port is placed into an authorized state and does not require client port-based authentication to be able to send and receive traffic.
User Name	The name the port uses to identify itself as a supplicant to the authenticator port. The menu includes the users that are configured for system management. When authenticating, the supplicant provides the password associated with the selected User Name.
Authentication Period	The amount of time the supplicant port waits to receive a challenge from the authentication server. If the configured Authentication Period expires, the supplicant retransmits the authentication request until it is authenticated or has sent the number of messages configured in the Maximum Start Messages field.
Start Period	The amount of time the supplicant port waits for a response from the authenticator port after sending a Start packet. If no response is received, the supplicant retransmits the Start packet.
Held Period	The amount of time the supplicant port waits before contacting the authenticator port after an active 802.1X session fails.
Maximum Start Messages	The maximum number of Start packets the supplicant port sends to the authenticator port without receiving a response before it considers the authenticator to be 802.1X-unaware.

5.8.5. Security > Port Access Control > 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.

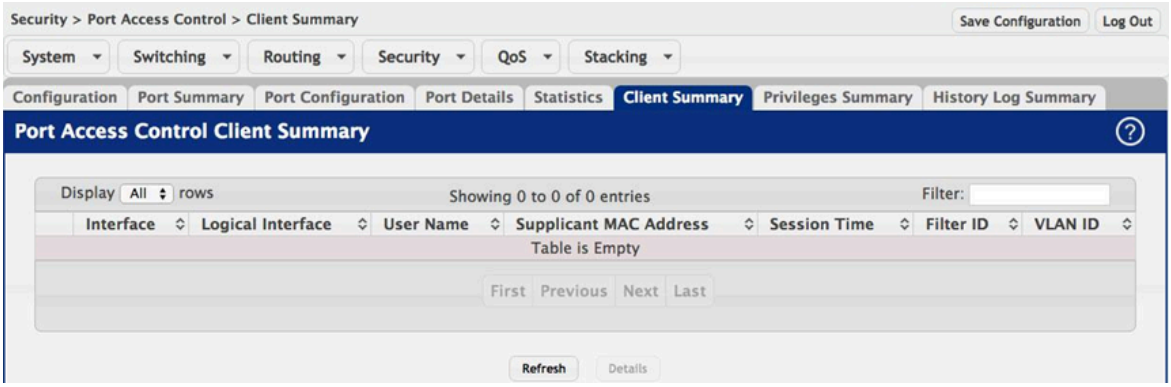
Interface	The interface associated with the rest of the data in the row. When viewing detailed information for an interface, this field identifies the interface being viewed.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: • Authenticator – The port enforces authentication 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.

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 Error Frames Received	The number of EAPOL frames with an invalid packet body length received on the interface.
Clear (Button)	Resets all statistics counters to 0 for the selected interface or interfaces.

5.8.6. Security > Port Access Control > Client Summary



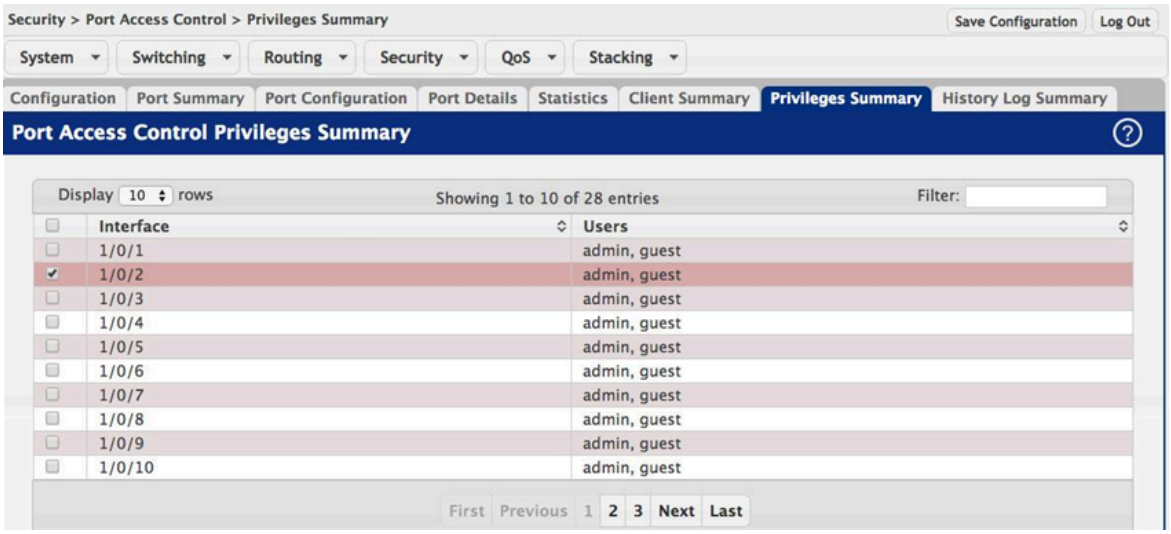
This page displays information about supplicant devices that are connected to the local authenticator ports. If there are no active 802.1X sessions, the table is empty. To view additional information about a supplicant, select the interface it is connected to and click Details.

Interface	The local interface associated with the rest of the data in the row. When viewing detailed information for an interface, this field identifies the interface being viewed.
Logical Interface	The logical port number associated with the supplicant that is connected to the port.
User Name	The name the client uses to identify itself as a supplicant to the authentication server.
Supp MAC Address	The MAC address of the supplicant that is connected to the port.
Session Time	The amount of time that has passed since the connected supplicant was granted access to the network through the authenticator port.
Filter ID	The policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID	The ID of the VLAN the supplicant was placed in as a result of the authentication process.

After you click Details, a window opens and displays additional information about the client. The following information describes the additional fields that appear in the window.

Session Timeout	The reauthentication timeout period set by the RADIUS server to the supplicant device.
Session Termination Action	The termination action set by the RADIUS server that indicates the action that will take place once the supplicant reaches the session timeout value.

5.8.7. Security > Port Access Control > Privileges Summary

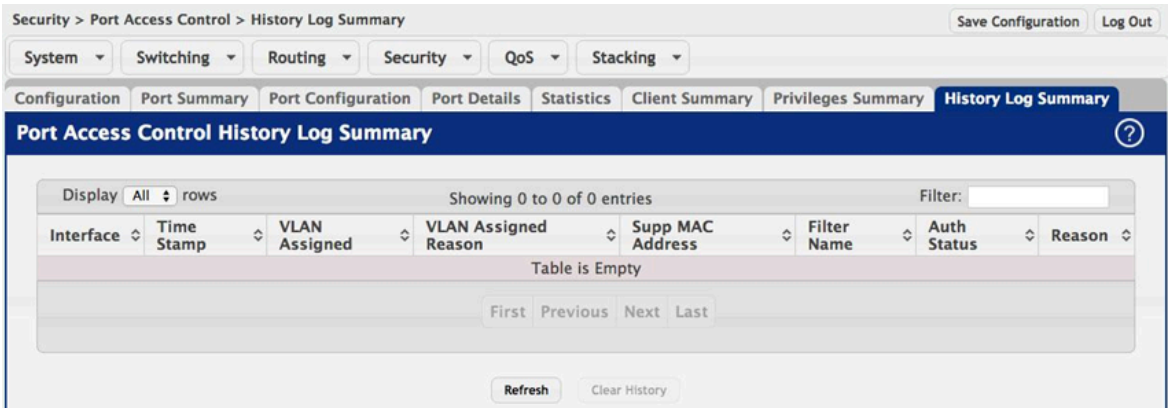


Use this page to grant or deny port access to users configured on the system. To change the access control privileges for one or more ports, select each interface to configure and click Edit. The same settings are applied to all selected interfaces.

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.

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

5.8.8. Security > Port Access Control > History Log Summary

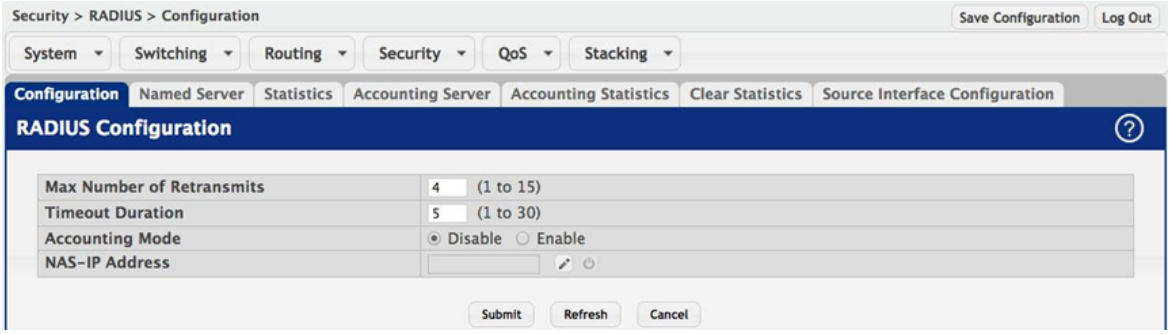


This page displays information about the 802.1X entries in the history log table.

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.

5.9. Security > RADIUS

5.9.1. Security > RADIUS > Configuration

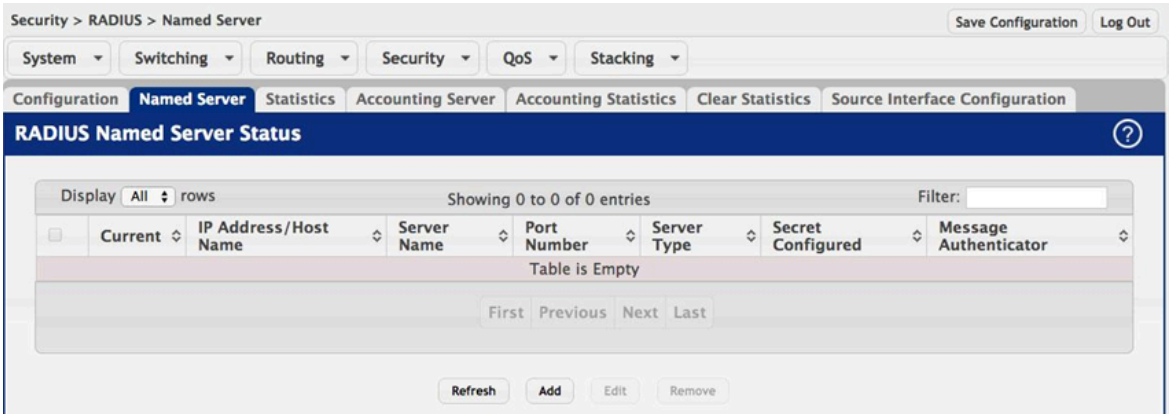


Use this page to configure global settings for the Remote Authentication Dial-In User Service (RADIUS) feature. The device includes a RADIUS client that can contact one or more RADIUS servers for various Authentication, Authorization, and Accounting (AAA) services. The RADIUS server maintains a centralized database that contains per-user information.

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.

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

5.9.2. Security > RADIUS > 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.

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

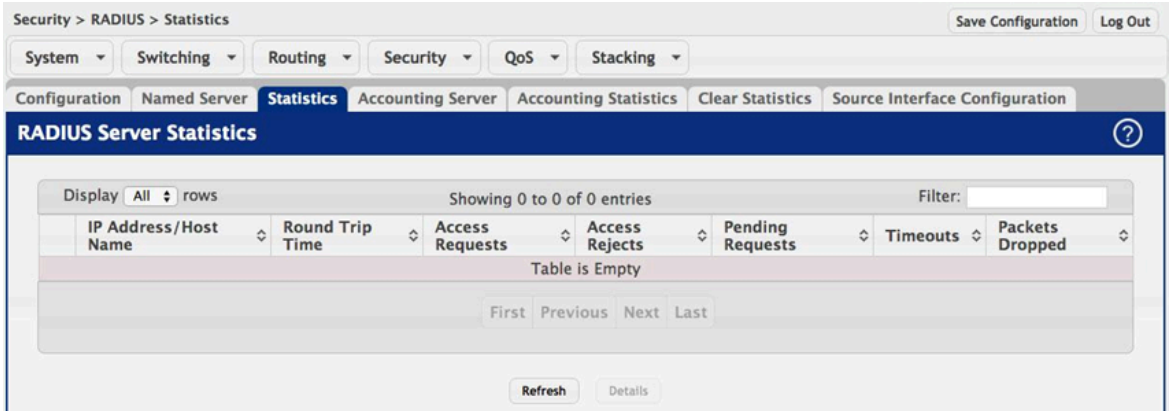
	Server Name value, the RADIUS client attempts to use the primary server first. If the primary server does not respond, the RADIUS client attempts to use one of the backup servers within the same named server group.
Secret Configured	Indicates whether the shared secret for this server has been configured.
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.

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.

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

5.9.3. Security > RADIUS > 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.

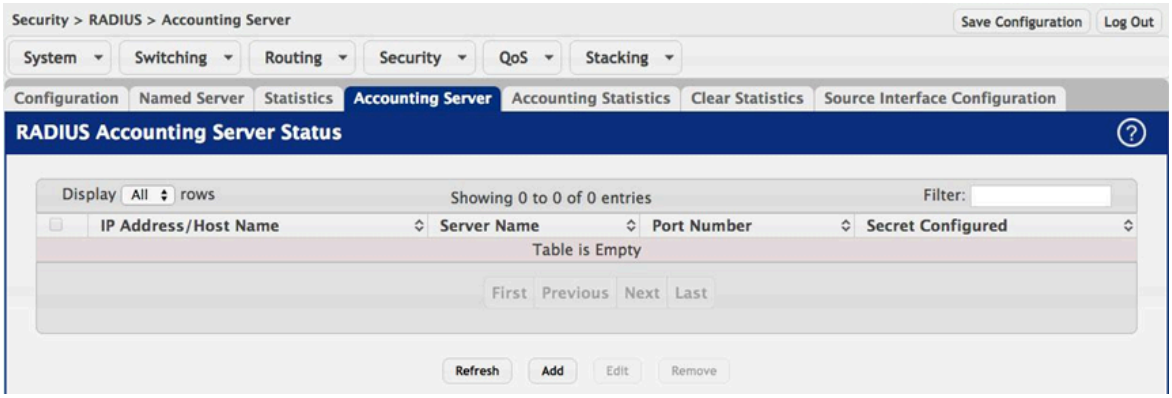
IP Address/Host Name	The IP address or host name of the RADIUS server associated with the rest of the data in the row. When viewing the detailed statistics for a RADIUS server, this field identifies the RADIUS server.
Round Trip Time	The time interval, in hundredths of a second, between the most recent 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.

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.

5.9.4. Security > RADIUS > 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.

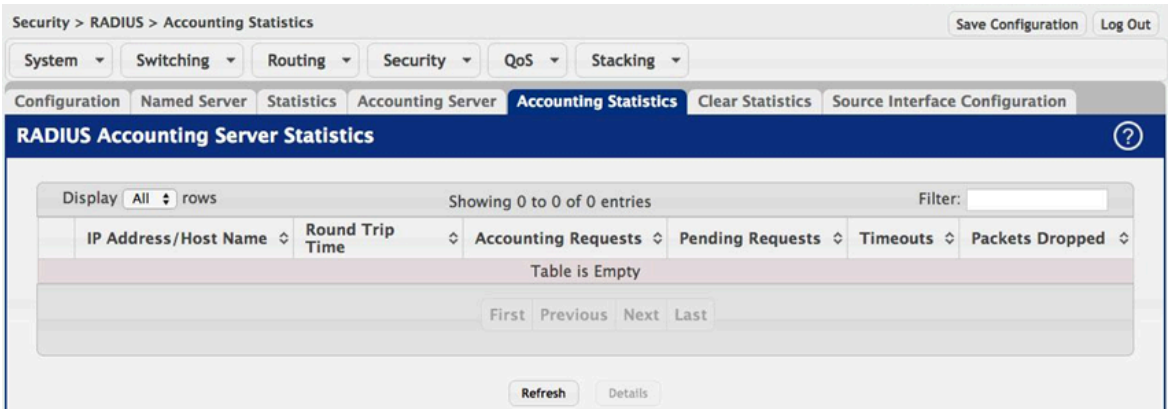
IP Address/Host Name	The IP address or host name of the RADIUS accounting server. Host names must be resolvable by DNS and are composed of a series of labels separated by dots.
Server Name	The name of the RADIUS accounting server. The server name must be unique among all configured RADIUS accounting 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.

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.

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

5.9.5. Security > RADIUS > 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.

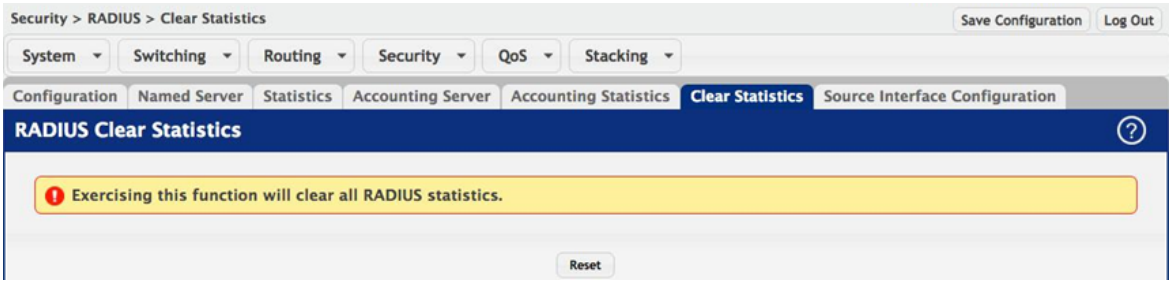
IP Address/Host Name	The IP address or host name of the RADIUS accounting server associated with the rest of the data in the row. When viewing the detailed statistics for a RADIUS accounting server, this field identifies the server.
Round Trip Time	The time interval, in hundredths of a second, between 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.

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 Responses	The number of malformed RADIUS Accounting-Response packets received from the server. Malformed packets include packets with an

	invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets that contained invalid authenticators received from the accounting server.
Unknown Types	The number of RADIUS packets of unknown type which were received from the server on the accounting port.

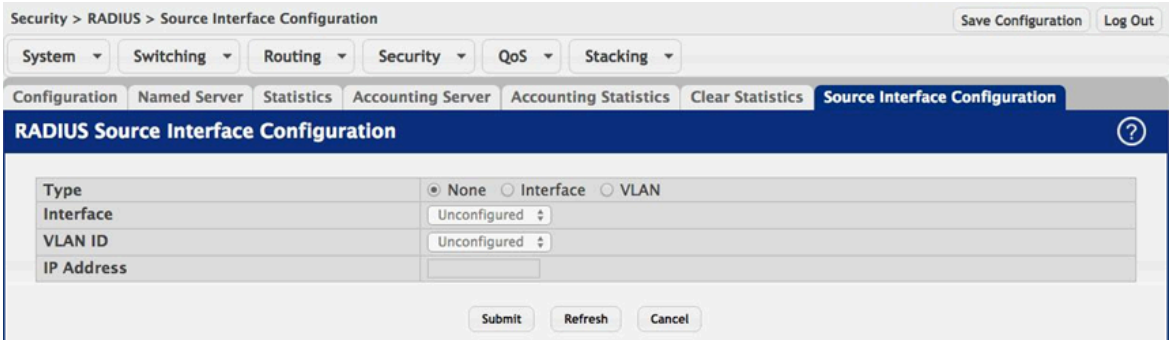
5.9.6. Security > RADIUS > Clear Statistics



Use this page to reset all RADIUS authentication and accounting statistics to zero.

Reset (Button)	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.

5.9.7. Security > RADIUS > 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.

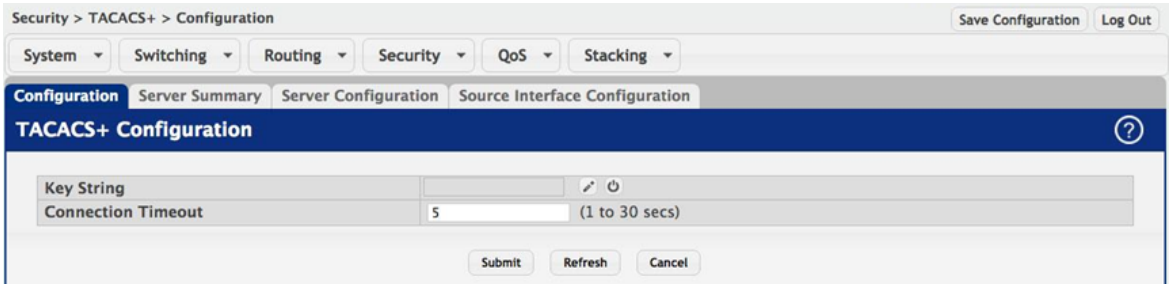
Type	The type of interface to use as the source interface:

	• 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.
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.
IP Address	The IP address associated with the configured Source Interface.

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

5.10. Security > TACACS+

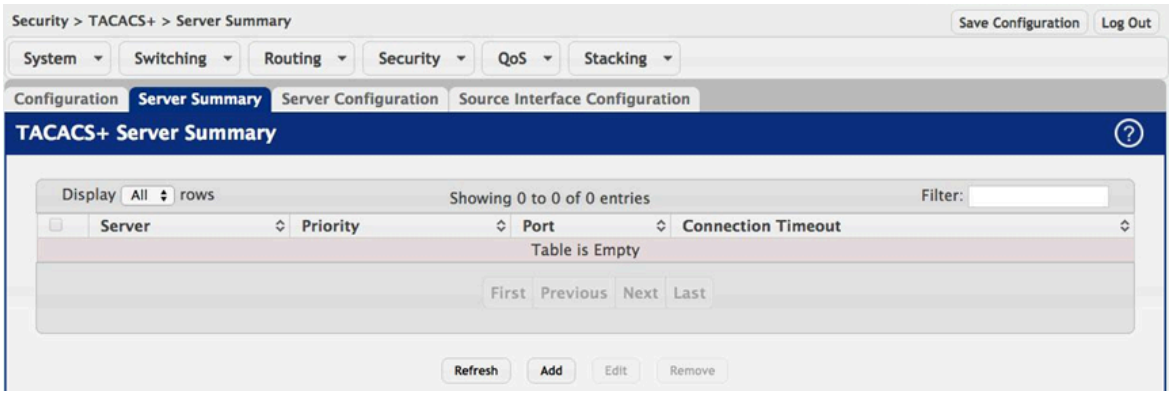
5.10.1. Security > TACACS+ > Configuration



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.

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

5.10.2. Security > TACACS+ > Server Summary



Use this page to view and configure information about the TACACS+ Server(s).

Use the buttons to perform the following tasks:

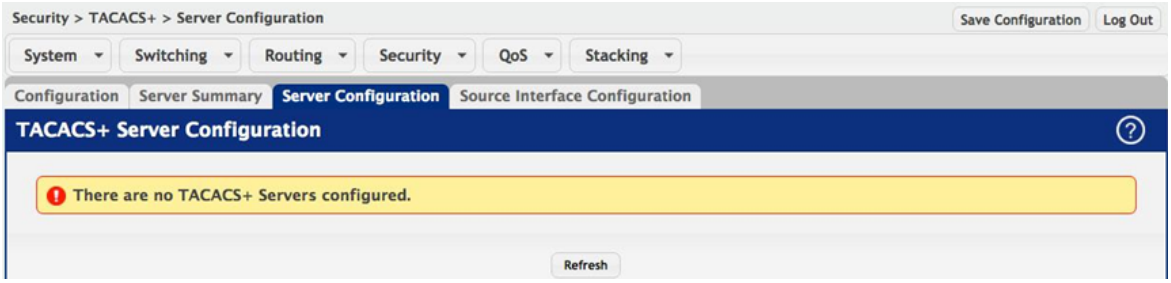
- To add a TACACS+ Server to the list of servers the TACACS+ client can contact, click Add. If maximum number of server is added, the button will be disabled
- To edit a configured TACACS+ server from the list, select the entry and click Edit.

- 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.

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.

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

5.10.3. Security > TACACS+ > Server Configuration

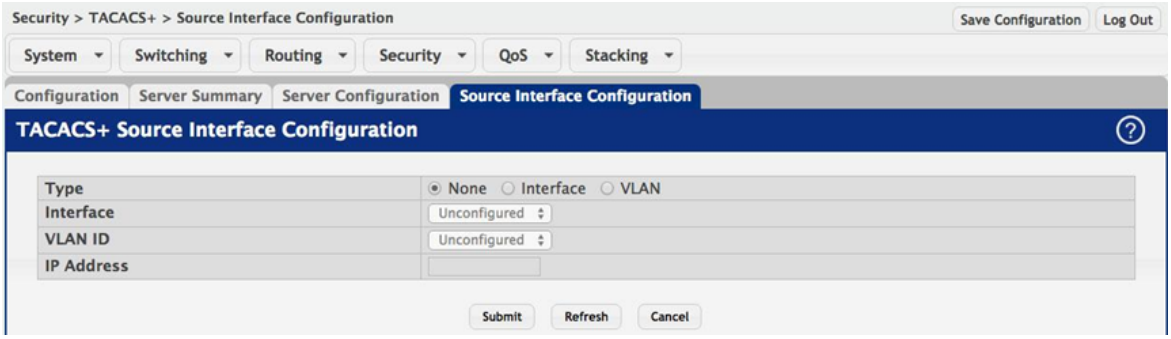


Use this page to view and configure information about the TACACS+ Server(s).

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.

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

5.10.4. Security > TACACS+ > Source Interface Configuration



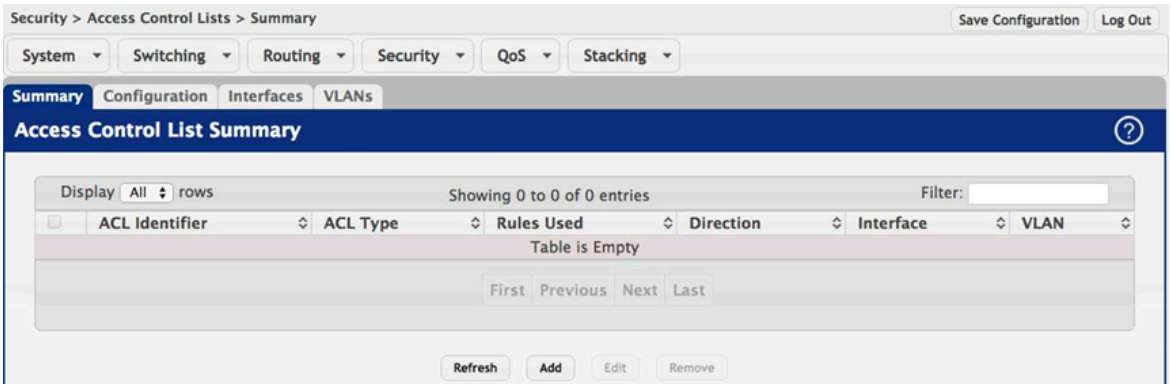
Use this page to specify the physical or logical interface to use as the TACACS+ client source interface. When an IP address is configured on the source interface, this address is used for all TACACS+ communications between the local TACACS+ client and the remote TACACS+ server. The IP address of the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

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.
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.
IP Address	The IP address associated with the configured Source Interface.

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

5.11. Security > Access Control Lists

5.11.1. Security > Access Control Lists > 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:

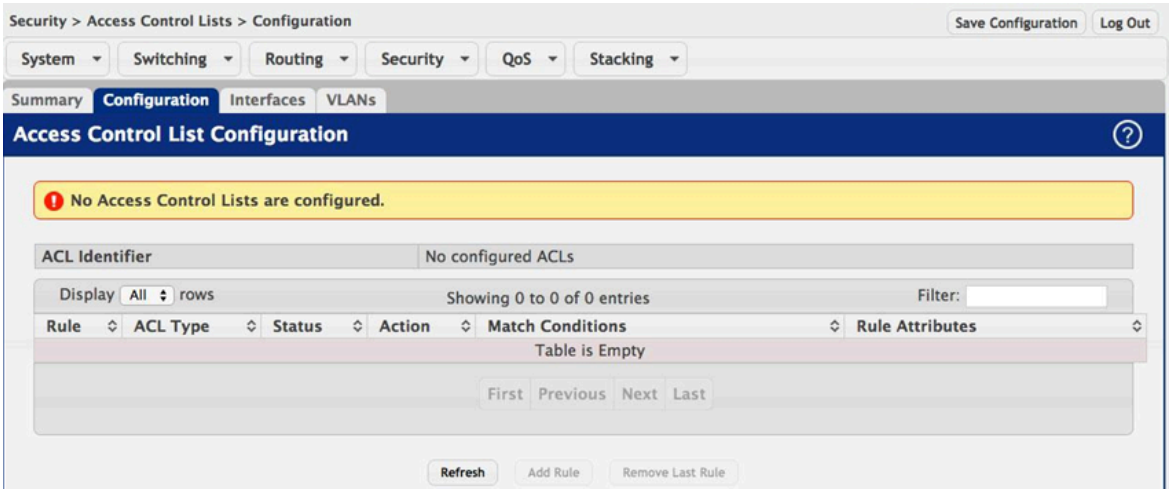
- To add an ACL, click Add and configure the ACL type and ID.
- To remove one or more configured ACLs, select each entry to delete and click Remove. You must confirm the action before the entry is deleted.
- To configure rules for an ACL, select the ACL to configure and click Edit. You are redirected to the Access Control List Configuration page for the selected ACL.

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.

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

5.11.2. Security > Access Control Lists > 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 the most recently configured rule for an ACL, select the ID of the appropriate ACL from the ACL Identifier menu and click Remove Last Rule. You must confirm the action before the entry is deleted.

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.
Rule	The number that identifies the rule. A number is automatically assigned to a rule when it is created. Rules are added in the order that they are created and cannot 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.

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.

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.
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

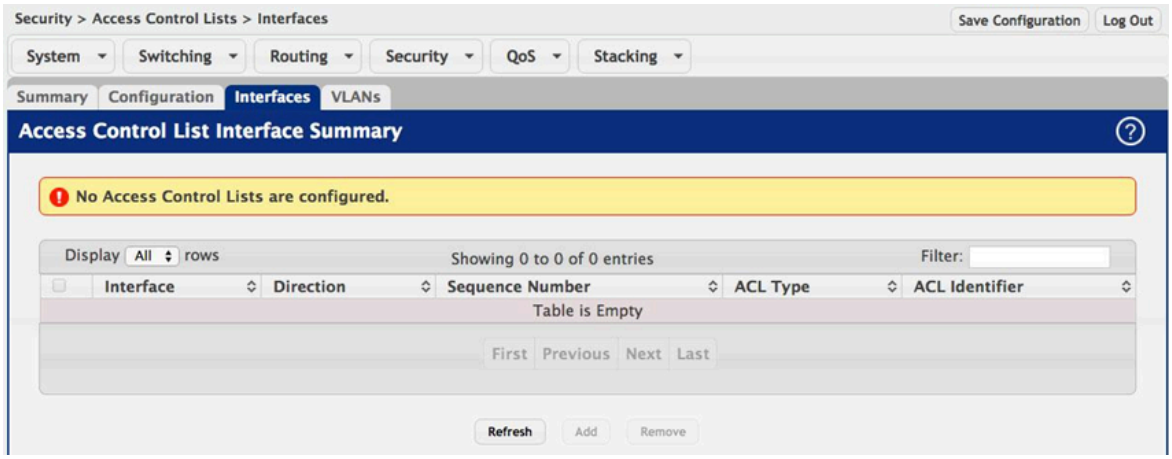
	include BGP, Domain, Echo, FTP, FTP Data, HTTP, SMTP, Telnet, WWW, POP2, and POP3. UDP port keywords include Domain, Echo, NTP, RIP, SNMP, TFTP, TIME, and WHO.
Destination Prefix / Prefix Length	The IPv6 prefix combined with the IPv6 prefix length to be compared to a packet's destination IPv6 address 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.
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.
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.
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).

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

5.11.3. Security > Access Control Lists > Interfaces



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:

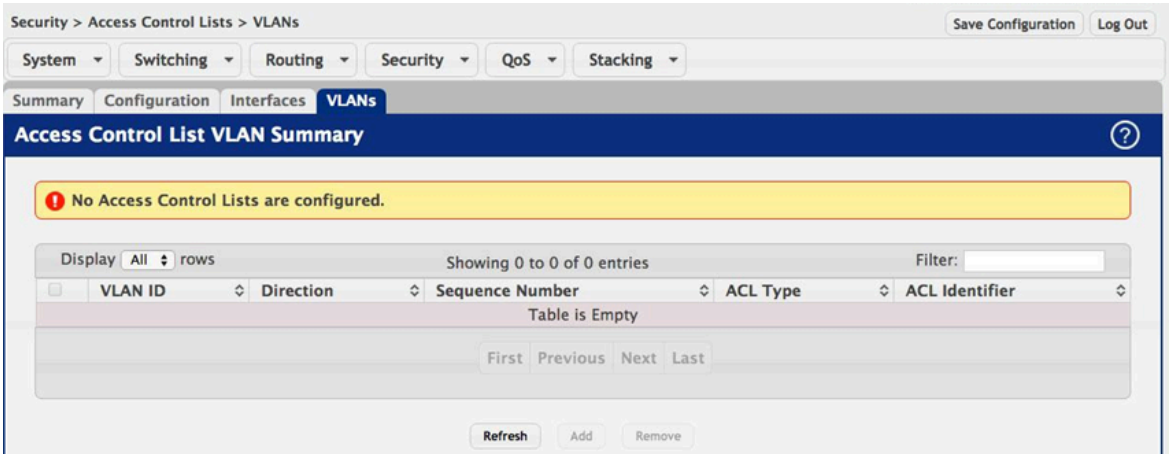
- To apply an ACL to an interface, click Add and configure the settings in the available fields.
- To remove the association between an interface and an ACL, select each entry to delete and click Remove. You must confirm the action before the entry is deleted.

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.

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

5.11.4. Security > Access Control Lists > 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.

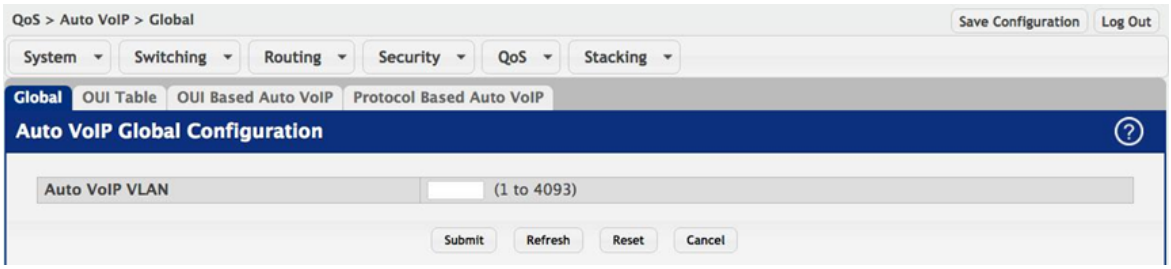
VLAN ID	The ID of the VLAN associated with the rest of the data in the row. When associating a VLAN with an ACL, use this field to select the desired VLAN.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on a VLAN (Inbound) or after it has been received, 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	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.

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

Chapter 6. Quality of Service

6.1. QoS > Auto VoIP

6.1.1. QoS > Auto VoIP > Global

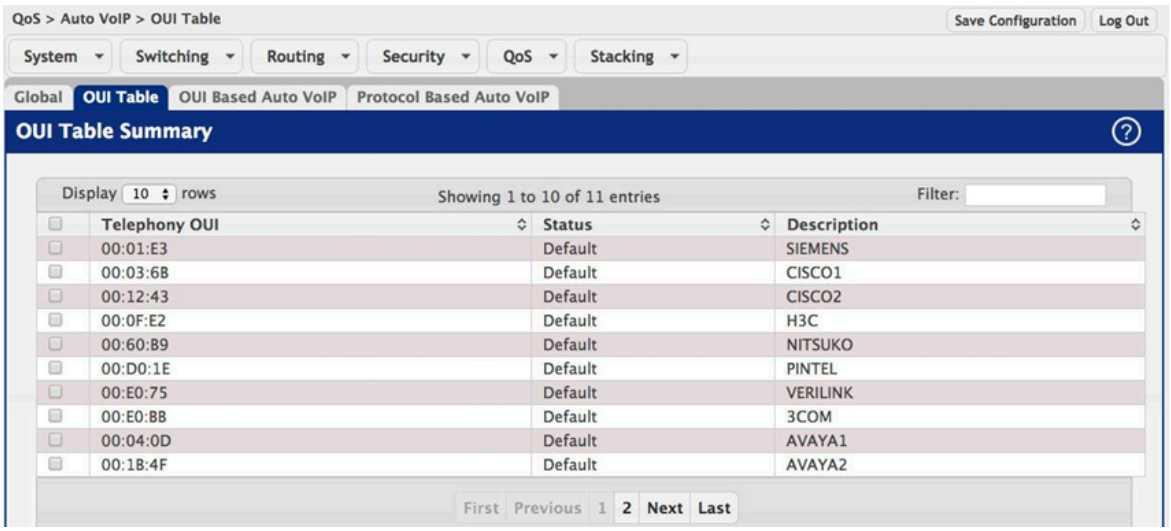


Use this page to configure the VLAN ID for the Auto VoIP VLAN or to reset the current Auto VoIP VLAN ID to the default value. Voice over Internet Protocol (VoIP) enables telephone calls over a data network. Because voice traffic is typically more time-sensitive than data traffic, the Auto VoIP feature 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.

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.

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

6.1.2. QoS > Auto VoIP > 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.

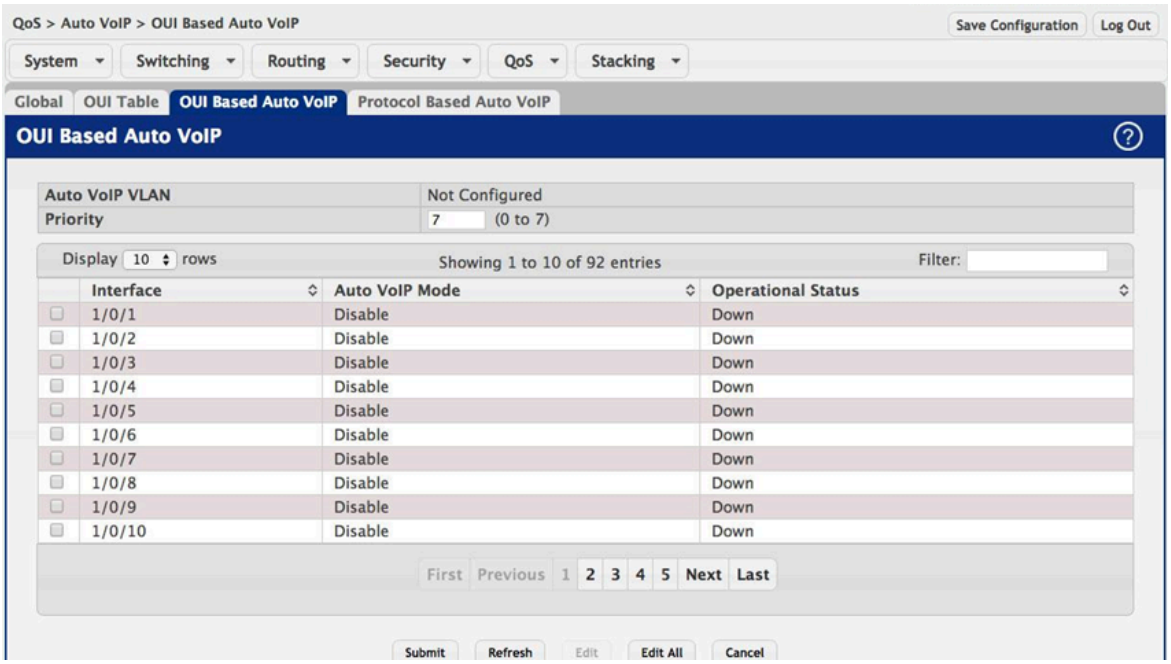
Use the buttons to perform the following tasks:

- 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.

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.

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

6.1.3. QoS > Auto VoIP > 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.

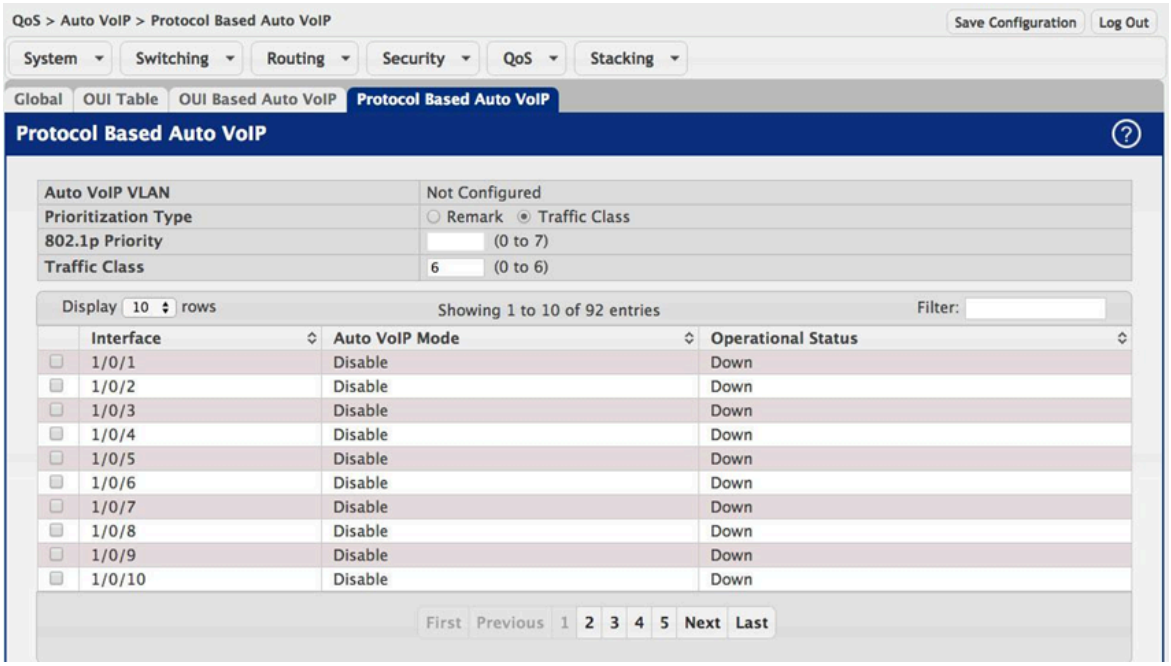
Use the buttons to perform the following tasks:

- 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.

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 Status	The operational status of an interface. To be up, an interface must be administratively enabled and have a link.

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

6.1.4. QoS > Auto VoIP > 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.

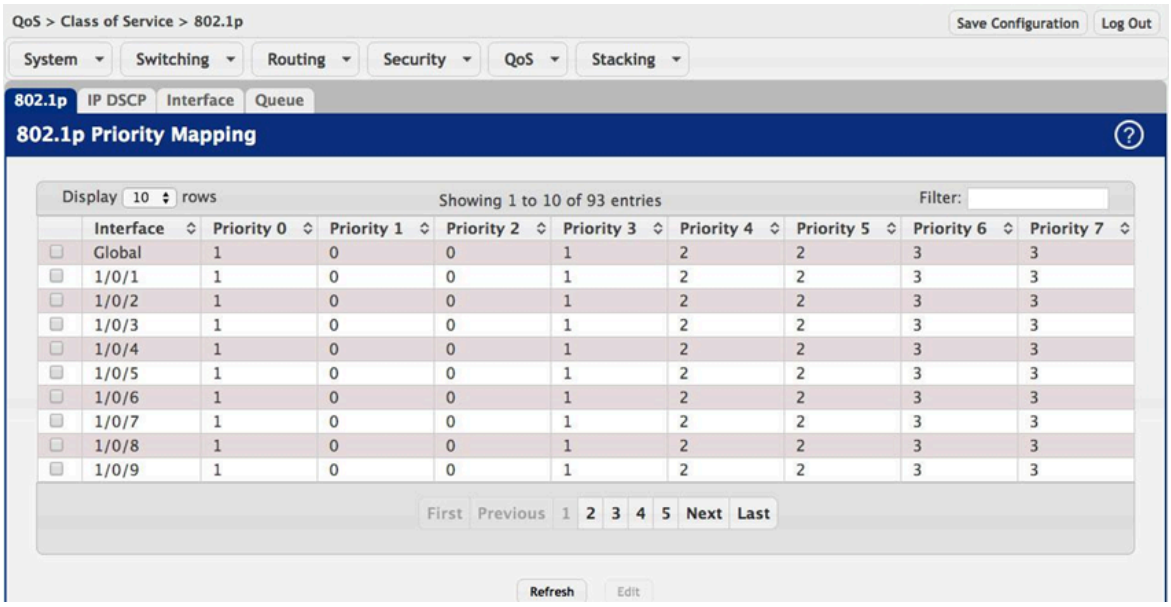
Auto VoIP VLAN	The VLAN used to segregate VoIP traffic from other non-voice traffic. All VoIP traffic in a session identified by the call-control protocol gets assigned to this VoIP VLAN.
Prioritization Type	The method used to prioritize VoIP traffic when a call-control protocol is detected, which is 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.

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

6.2. QoS > Class of Service

6.2.1. QoS > Class of Service > 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.

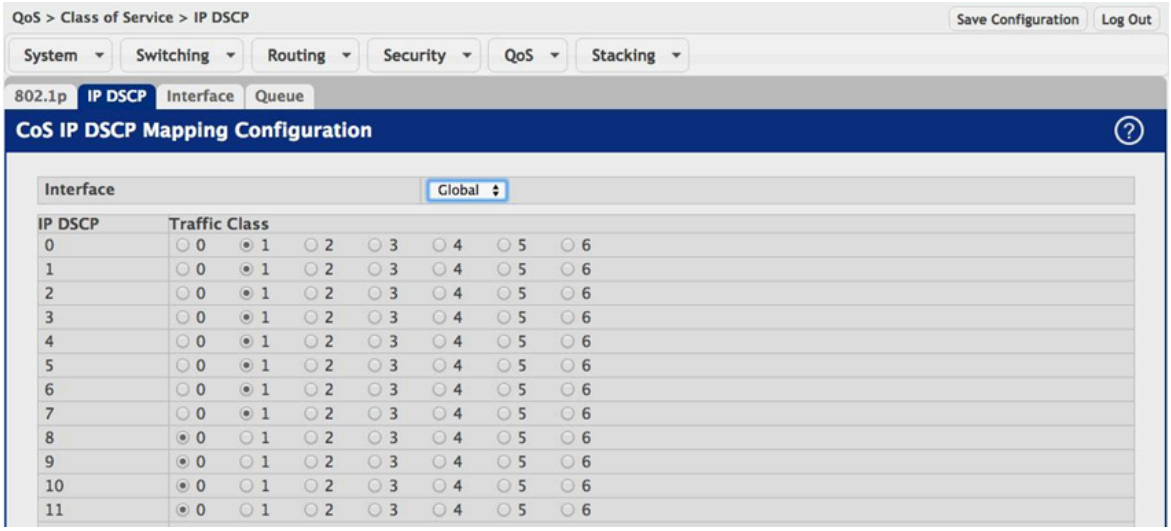
Interface	The interface associated with the rest of the data in the row. The Global entry represents the common settings for all interfaces, unless specifically overridden individually.
Priority	The heading row lists each 802.1p priority value (0–7), and the data in the table shows which traffic class 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:

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.

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

6.2.2. QoS > Class of Service > IP DSCP

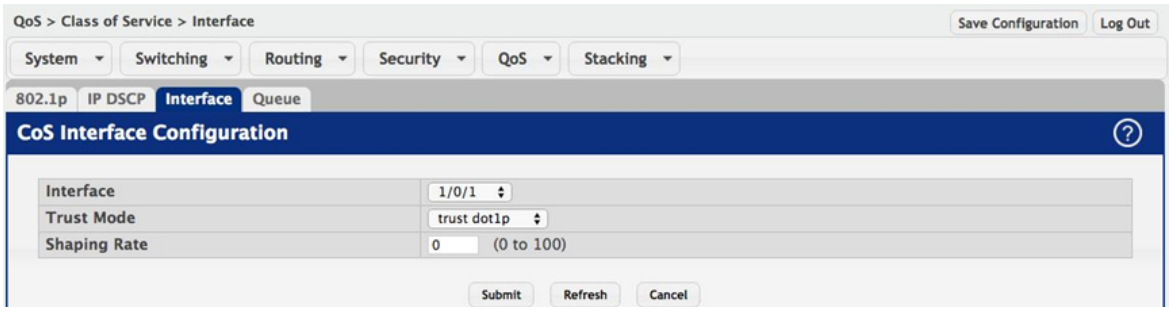


Use this page to configure the per-interface mapping between the IP DiffServ Code Point (DSCP) value and the traffic class. A DSCP value can be included in the Service Type field of an IP header. When traffic is queued for transmission on the interface, the DSCP value in the IP header is mapped to the traffic class specified on this page. A traffic class with a higher value has priority over a traffic class with a lower value.

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.

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

6.2.3. QoS > Class of Service > Interface

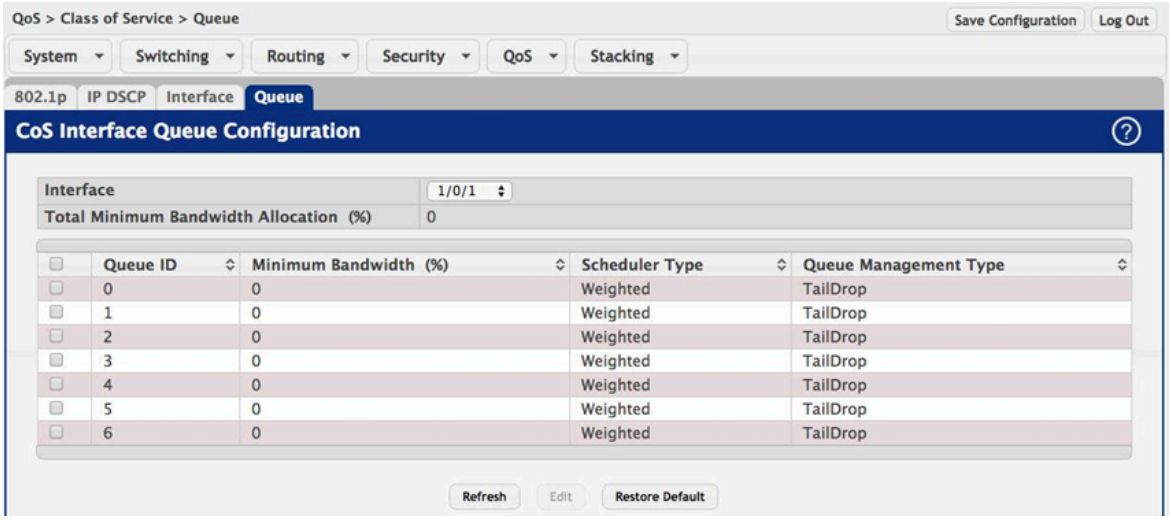


Use this page to configure the per-interface Class of Service (CoS) settings. The CoS feature allows preferential treatment for certain types of traffic over others. To set up this preferential treatment, you can configure the CoS interface settings and individual queues on the egress ports to provide 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.

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.

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

6.2.4. QoS > Class of Service > Queue



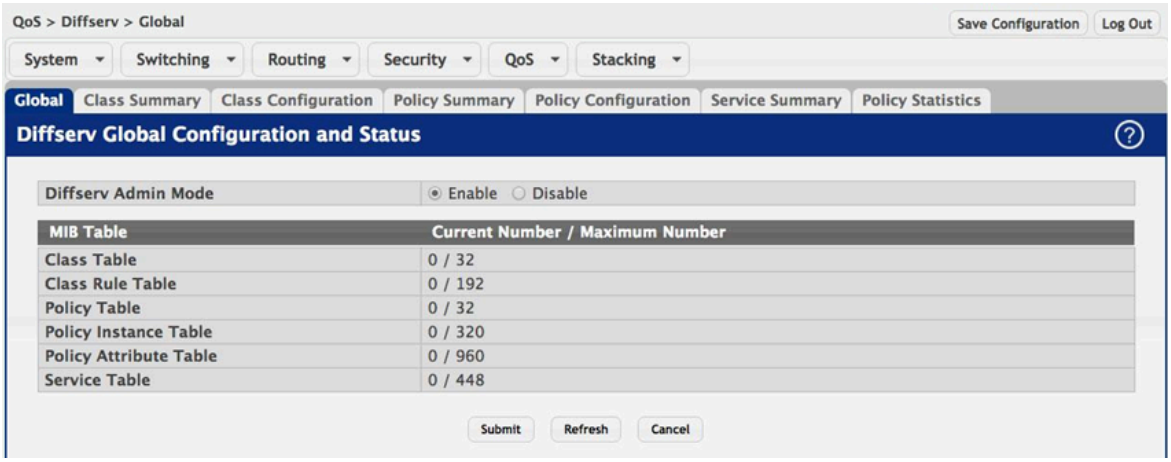
Use this page to define the behavior of the egress CoS queues on each interface. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on an interface. Each interface 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.

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.
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.

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

6.3. QoS > Diffserv

6.3.1. QoS > Diffserv > 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.

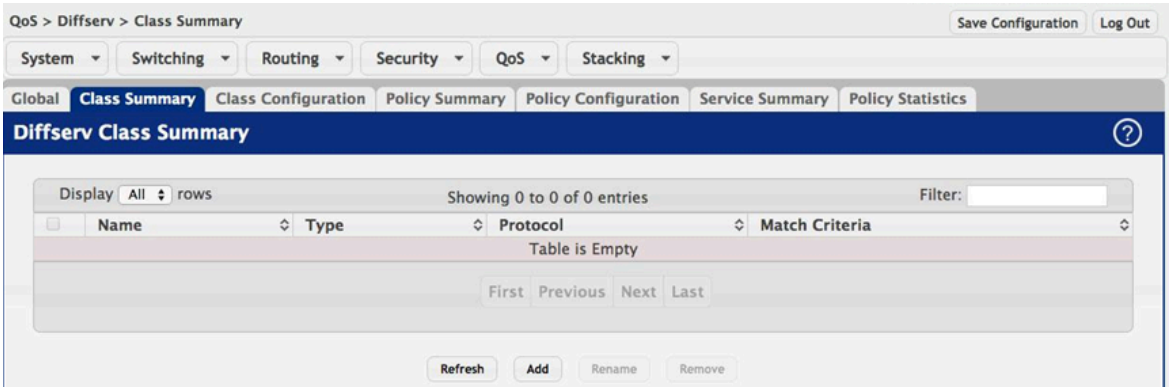
Packets are classified and processed based on defined criteria. The classification criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

Diffserv 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.

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

6.3.2. QoS > Diffserv > Class Summary



Use this page to create or remove DiffServ classes and to view summary information about the classes that exist on the device. Creating a class is the first step in using DiffServ to provide Quality of Service. After a class is created, you can define the match criteria for the class.

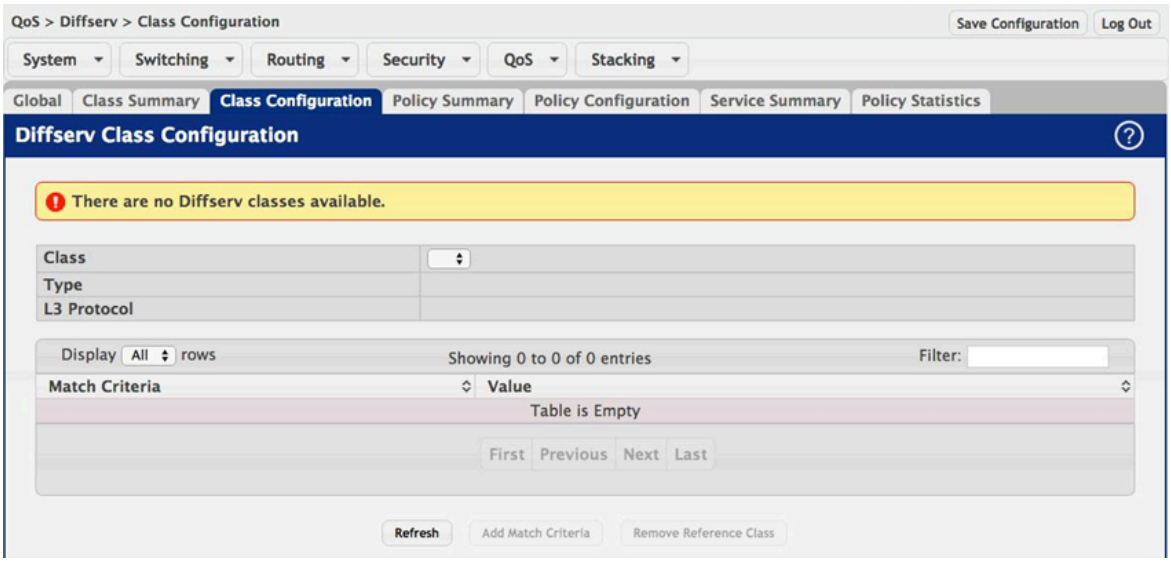
Use the buttons to perform the following tasks:

- 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.

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.

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

6.3.3. QoS > Diffserv > Class Configuration



Use this page to define the criteria to associate with a DiffServ class. As packets are received or transmitted, these DiffServ classes are used to classify and prioritize packets. Each class can contain multiple match criteria.

After you select the class to configure from the Class menu, use the buttons to perform the following tasks:

- To define criteria for matching packets within a class, click Add Match Criteria. Once you add a match criteria entry to a class, you cannot edit or remove the entry. However, you can add more match criteria entries to a class until the maximum number of entries has been reached for the class.
- To remove the associated reference class from the selected class, click Remove Reference Class. 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.

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.

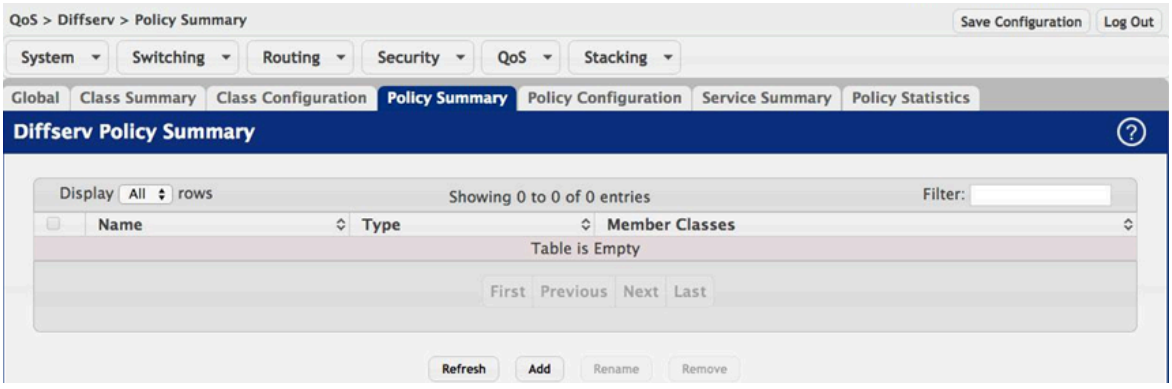
Source MAC Address	Select this option to require a packet's source MAC address to match the specified MAC address. After you select this option, use the following fields to configure the source MAC address match criteria: • MAC Address – The source MAC address to match. • MAC Mask – The MAC mask, which 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.

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

6.3.4. QoS > Diffserv > Policy Summary



Use this page to create or remove DiffServ policies and to view summary information about the policies that exist on the device. A policy defines the QoS attributes for one or more traffic classes. A policy attribute identifies the action taken when a packet matches a class rule. A policy is applied to a packet when a class match within that policy is found.

Use the buttons to perform the following tasks:

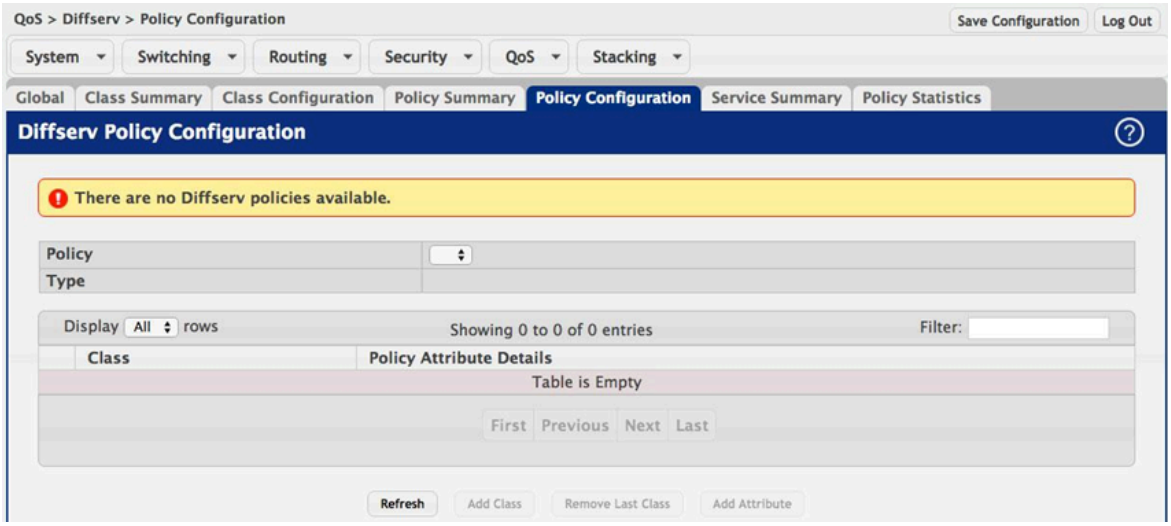
- To add a DiffServ policy, click Add.

- 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.

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.
Member Classes	The DiffServ class or classes that have been added to the policy.

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

6.3.5. QoS > Diffserv > Policy Configuration



Use this page to add or remove a DiffServ policy-class association and to configure the policy attributes. The policy attributes identify the action or actions taken when a packet matches a class rule.

After you select the policy to configure from the Policy menu, use the buttons to perform the following tasks:

- To add a class to the policy, click Add Class.
- To add attributes to a policy or to change the policy attributes, select the policy with the attributes to configure and click Add Attribute.
- To remove the most recently associated class from the selected policy, click Remove Last Class.

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 Secondary CoS	Select this option to mark the priority field of the 802.1p header in the 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

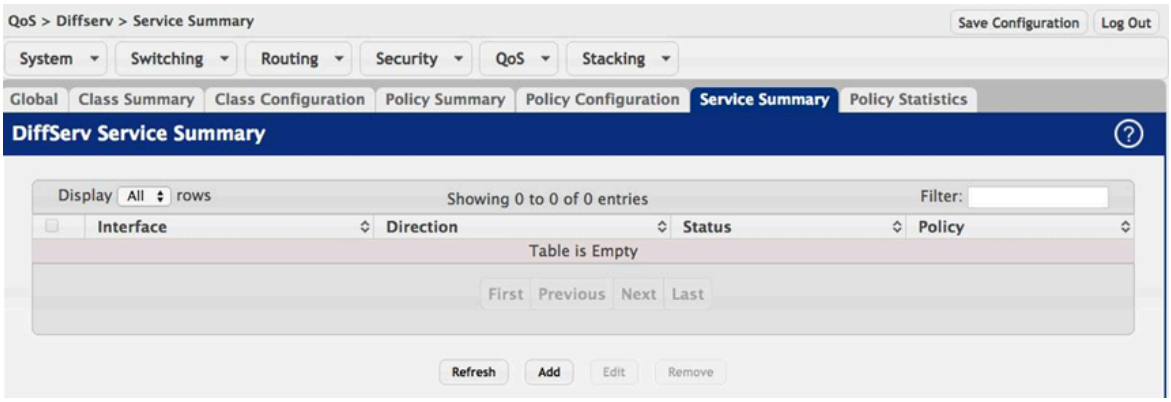
	burst size, resulting in two outcomes (conform and violate). After you select this option, configure the following policing criteria: • Color Mode – The type of color policing used in DiffServ traffic conditioning. • Color Conform Class – For color-aware policing, packets in this class are metered against 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.

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

6.3.6. QoS > Diffserv > 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.

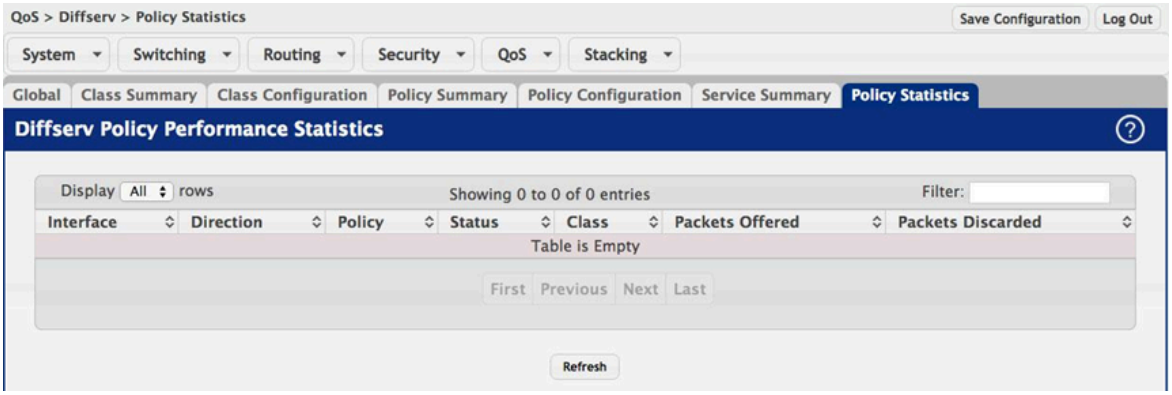
Interface	The interface associated with the rest of the data in the row. Only interfaces that have an associated policy are listed in the table.
Direction	The traffic flow direction to which the policy is applied: • Inbound – The policy is applied to traffic as it enters the interface.
Status	The status 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.

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

6.3.7. QoS > Diffserv > Policy Statistics



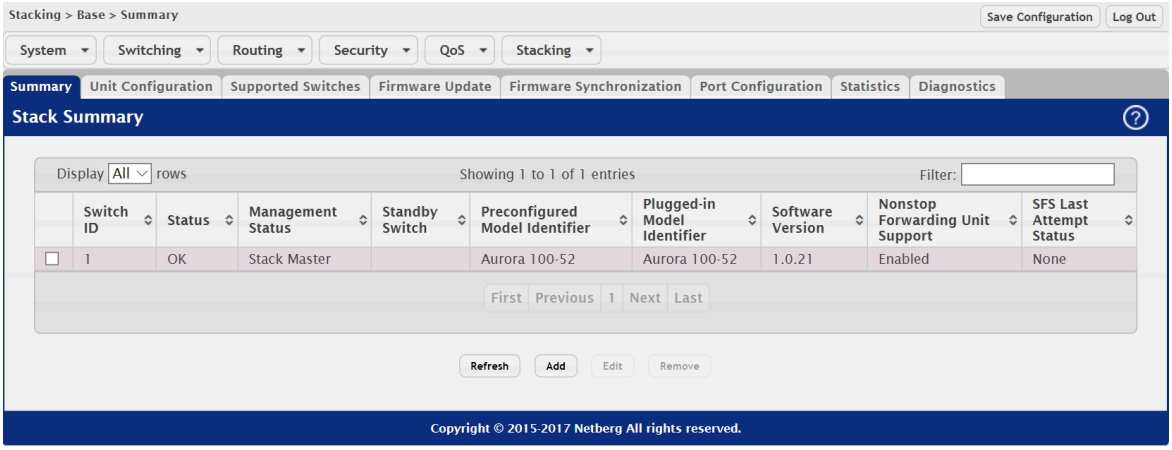
This page displays class-oriented statistical information for the policy, which is specified by the interface and direction.

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.
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.

Chapter 7. Stacking commands

7.1. Stacking > Base

7.1.1. Stacking > Base > Summary



Use this page to view summary information about each unit in the stack and to add or remove stack units. A stack is a set of multiple devices that are connected through their stacking ports. One of the devices controls the operation of the stack and is called the stack master. All other devices in the stack are stack members. The stack members use stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire stack as a single entity to the network.

Use the buttons to perform the following tasks:

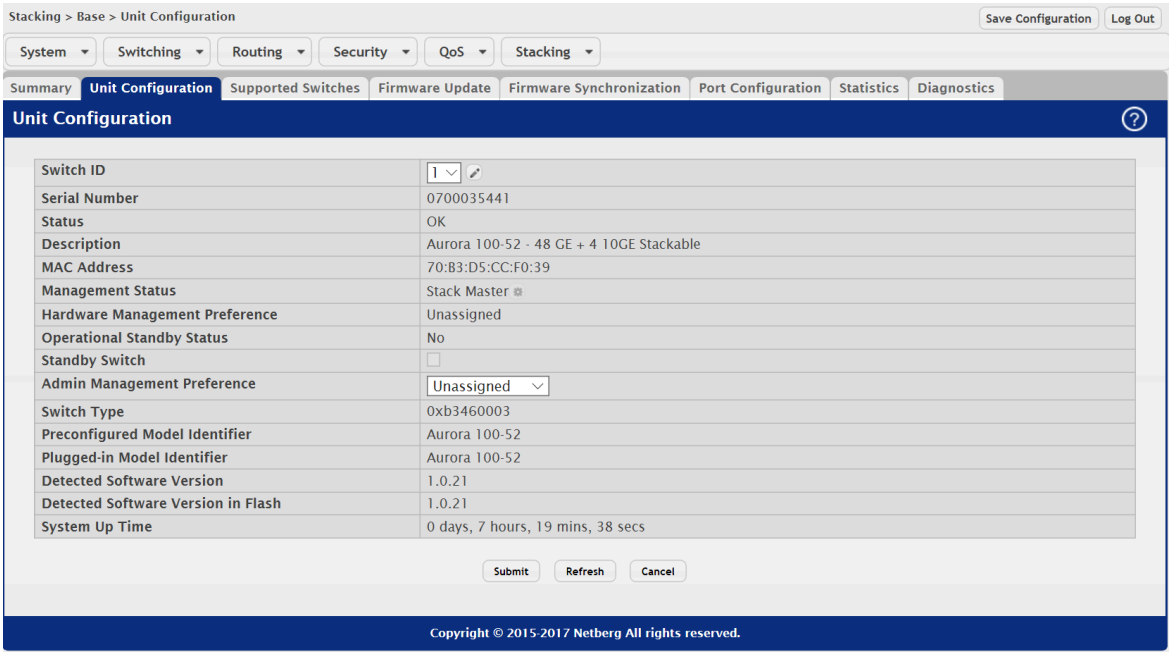
- To preconfigure a unit before physically adding it to the stack, click Add. When a unit is physically connected to the stack and powered on, it is automatically added to the stack and its entry will appear in the table. A preconfigured unit allows for the adjustment of certain settings which will be applied to the unit when it is physically connected and powered on.
- To change the settings for a unit, select the entry to update and click Edit.
- To remove one or more preconfigured units from the stack before it is connected, select each preconfigured entry to remove and click Remove. A unit that is physically connected to the stack and powered on cannot be manually removed from the table.

Switch ID	The ID of the unit in the stack. The Switch ID does not impact whether the unit is the stack master or a stack member. The maximum number of units allowed in the stack is 6. A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a switch stack, its default stack member number changes to the lowest available member number in the stack. The stack master cannot be removed.
Status	The unit status: • OK – The unit is operating within the stack. It is physically connected to the stack and is powered on.

	• Not Present – The unit is not operating within the stack. • Code Mismatch – The firmware version of this unit is mismatched with stack master. • Updating Code – The firmware version of stack master is synchronizing to this unit.
Management Status	The role of the unit within the stack: • Stack Master – The unit is performing the stack master functions for the stack and is the single point of stack-wide management. The stack master maintains the saved and running configuration files for the switch stack. • Stack Member – The unit is not a stack master, but it has connectivity to the stack master. • Unassigned – The management status of the unit has not been assigned. This status might occur because the maximum number of units already exist in the stack or the unit is not present.
Standby Switch	The standby status of the unit. The standby unit in the stack takes over as the stack master if the current stack master fails. • Operational Standby – The unit has connectivity to the stack master and has been nominated to take over as master should the current master fail. • Configured Standby – The unit has been manually configured to take over as master should the current master fail. The unit does not need to be connected to the stack to be configured as the standby unit. • If the field is blank, the unit has not been auto-selected or configured as the standby unit for the stack.
Preconfigured Model Identifier	The value assigned by the device manufacturer to identify the device.
Plugged-in Model Identifier	The value assigned by the device manufacturer to identify the plugged-in device.
Software Version	The detected software version of code on this unit.
Nonstop Forwarding Unit Support	The nonstop forwarding (NSF) support status of the unit. NSF allows the forwarding plane of stack units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the stack master and allows the standby unit to quickly take over as the stack master.
SFS Last Attempt Status	The status of the last attempt to synchronize the firmware of the unit. Stack Firmware Synchronization (SFS) is performed when the feature is enabled and the unit added to the stack has a firmware version different from the master.

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

7.1.2. Stacking > Base > Unit Configuration



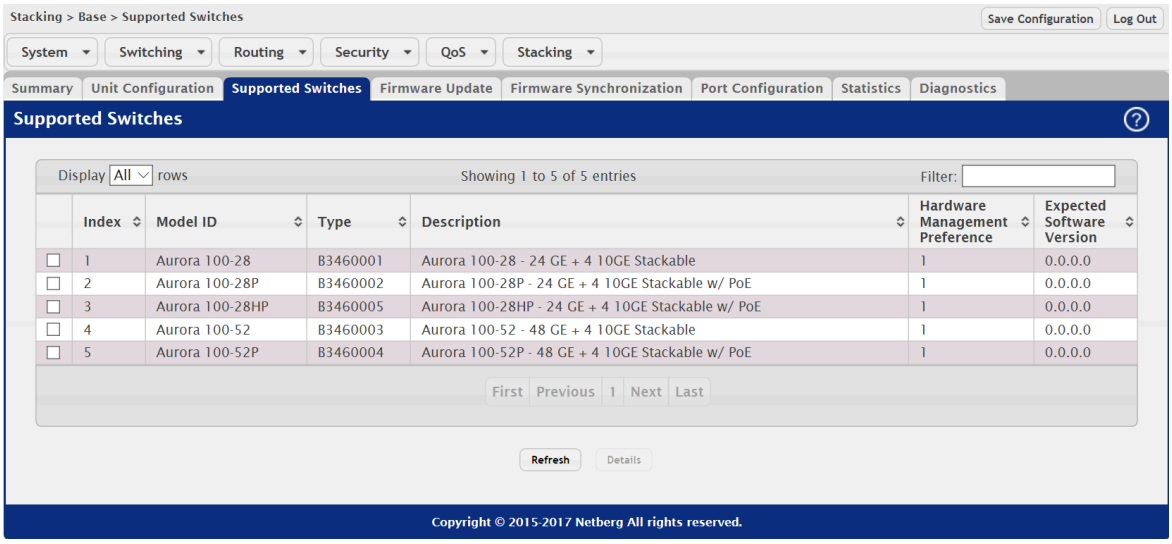
Use this page to view information about each stack unit, renumber a unit, change which unit is the stack master, configure the standby switch, or select the administrative management preference of a unit.

Switch ID	The ID of the unit in the stack. Use the drop-down menu to select the unit with the information to view or configure. A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a switch stack, its default stack member number changes to the lowest available member number in the stack. To change the Switch ID of a unit, click the Edit icon. In the Edit Switch ID window, use the Change Switch ID To field to select the new Switch ID. Renumbering a non-master unit requires a unit reset for the renumbering to take effect. Renumbering a master unit requires a reset of all the switches in the stack for the renumbering to take effect.
Serial Number	The unique device serial number assigned by the device manufacturer.
Status	The unit status: • OK – The unit is operating within the stack. It is physically connected to the stack and is powered on. • Not Present – The unit is not operating within the stack.

Description	The product name of this device.
Management Status	The role of the unit within the stack: • Stack Master – The unit is performing the stack master functions for the stack and is the single point of stack-wide management. The stack master maintains the saved and running configuration files for the switch stack. • Stack Member – The unit is not a stack master, but it has connectivity to the stack master. • Unassigned – The management status of the unit has not been assigned. This status might occur because the maximum number of units already exist in the stack or the unit is not present. To change which unit is the stack master, click the Move Switch Management icon in the Management Status field. In the Move Switch Management window, use the Move Switch Management To field to select the Switch ID of the unit that should take over the stack master role. The operation may take three minutes or longer depending on the stack size and configuration.
Hardware Management Preference	A two-byte value set by the device manufacturer that indicates whether this unit is capable of becoming the stack master. If the value is set to zero then the unit cannot support the stack master function. A higher value means that the unit is more desirable than another unit with a lower value for running the management function.
Operational Standby Status	The operational standby status of the unit. If the status is Yes, the unit has connectivity to the stack master and has been nominated to take over as master should the current master fail.
Standby Switch	Select the check box to configure the unit as the standby unit. The unit does not need to be connected to the stack to be configured as the standby unit. Only one unit can be configured as the standby unit.
Admin Management Preference	The administrative management preference of the unit. When stack master election or re-election occurs, the unit with the highest administrative preference value becomes the stack master. Setting the preference to Disabled makes it ineligible for master selection.
Switch Type	The hardware type value of this supported device.
Preconfigured Model Identifier	The value assigned by the device manufacturer to identify the device.
Plugged-in Model Identifier	The value assigned by the device manufacturer to identify the plugged-in device.
Detected Software Version	The release number and version number of the code detected on the unit.
Detected Software Version in Flash	The release number and version number of the code detected on flash for the unit.
System Up Time	The time in days, hours, minutes and seconds since the system was last reset.

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

7.1.3. Stacking > Base > Supported Switches



Use this page to view information about the devices that can be combined to form a stack. To view additional information about a supported device, select the entry and click **Details**.

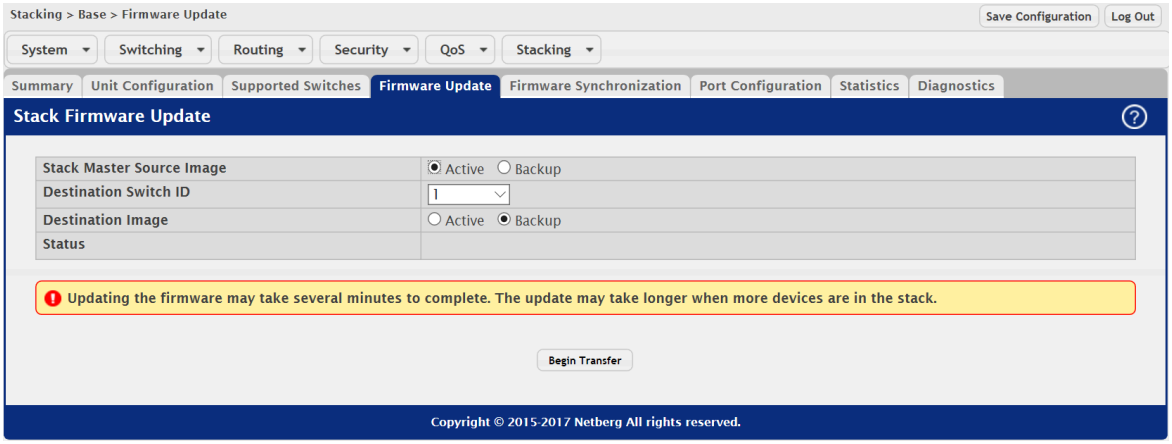
Index	The index assigned to the device type. The Index is used when preconfiguring a stack member by using the CLI or SNMP.
Model ID	The string that identifies the model of the supported switch or card.
Type	The hardware type value of the supported device.
Description	The product name of the device.
Hardware Management Preference	A two-byte value set by the device manufacturer that indicates whether this unit is capable of becoming the stack master. If the value is set to zero, the unit cannot support the stack master function. A higher value means that the unit is more desirable than another unit with a lower value for running the management function.
Expected Software Version	The release number and version number of the code that is expected to be loaded on this device.

After you select an entry in the table and click Details, the Supported Switch Details window opens. The following information describes the additional fields that appear in this window.

Slot Index	A possible slot index for the supported switch. Support for changing the slot configuration is platform dependent. This value is helpful when configuring the system by using SNMP or the CLI.
Card Index	A possible card index that can be inserted into the associated slot. Support for adding cards to a slot is platform dependent. This value is helpful when configuring the system by using SNMP or the CLI.

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

7.1.4. Stacking > Base > Firmware Update

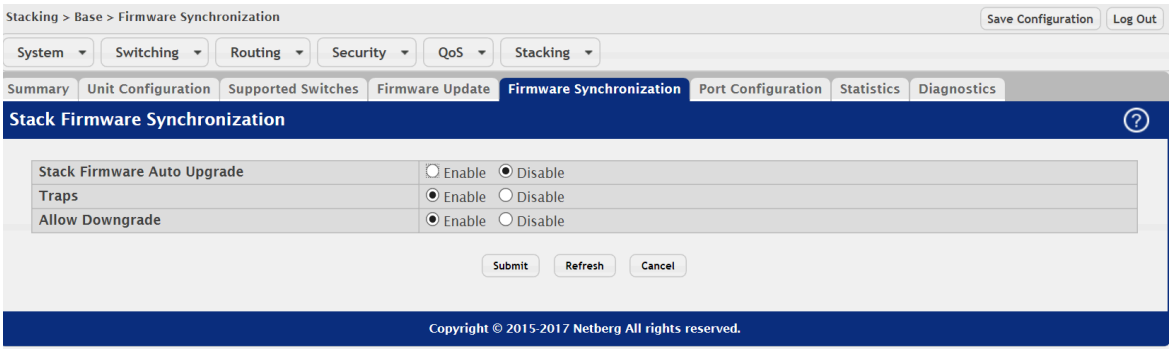


Use this page to update the firmware on one or more units in the stack. The image from the stack master is copied to the selected stack member as either the active or backup image on the stack member.

Stack Master Source Image	The list of available images on the stack master that can be transferred to other units.
Destination Switch ID	Select the unit to which to transfer the stack master firmware image. The menu lists all units of the stack, including the stack master.
Destination Image	Select the image on the destination unit to overwrite.
Status	The firmware update status after initiating the update. The status is one of the following: • Transfer in progress. Please wait… • Transfer completed • Transfer failed • If the field is blank, a firmware update has not been initiated on the selected unit.
Begin Transfer (Button)	Click this button to initiate the transfer. Updating the firmware may take several minutes to complete. The update may take longer when more devices are in the stack.

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

7.1.5. Stacking > Base > Firmware Synchronization

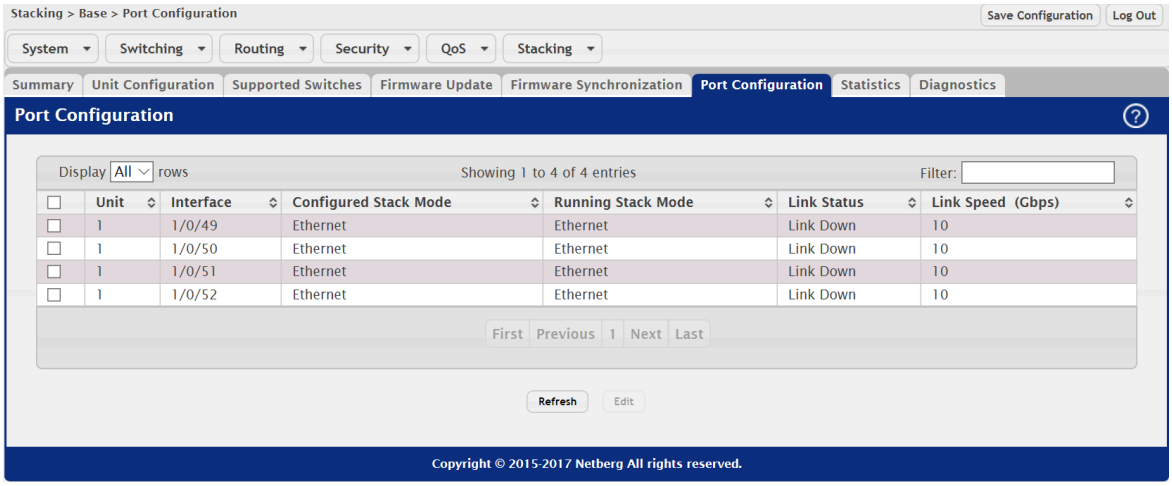


Use this page to configure the Stack firmware Synchronization (SFS) settings on the stack. SFS provides the ability to automatically synchronize firmware for all stack members. If a unit joins the stack and its firmware version is different from the version running on the stack master, the SFS feature can either upgrade or downgrade the firmware on the mismatched stack member. There is no attempt to synchronize the stack to the latest firmware of a member that joins the stack.

Stack Firmware Auto Upgrade	Enable or disable the Stack Firmware Synchronization feature on the stack. Enabling the feature allows the stack master to automatically upgrade the firmware version of a unit that joins the stack if the firmware version on the new stack member is older than the firmware version on the stack master.
Traps	Enable or disable the sending of SNMP traps during SFS start, failure, or finish.
Allow Downgrade	Enable or disable the ability of the stack master to downgrade the image on a new stack member if the firmware version on the stack master is older than the firmware version on the new stack member.

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

7.1.6. Stacking > Base > Port Configuration



Use this page to view and configure stacking functionality on ports that support stacking. For these ports, you can administratively enable stacking mode or Ethernet mode. In Ethernet mode, the port functions like other non-stacking ports. To change the stack mode on a port, select the port to configure and click **Edit**.

Unit	The number that identifies the unit within the stack (also called Switch ID).
Interface	The stackable interfaces on the unit. The table displays only the ports that can be used for physically connecting multiple devices to form a stack.
Configured Stack Mode	The manually-configured mode for the interface, which is either Stack or Ethernet. If you change the stack mode on a port, the configuration is immediately saved in the NVRAM on the unit on which the port is located. However, the run-time mode is not changed until the unit resets.
Running Stack Mode	The mode in which the interface is currently operating.
Link Status	The link status of the port, which is either Up or Down.
Link Speed	The maximum speed of the stacking port.

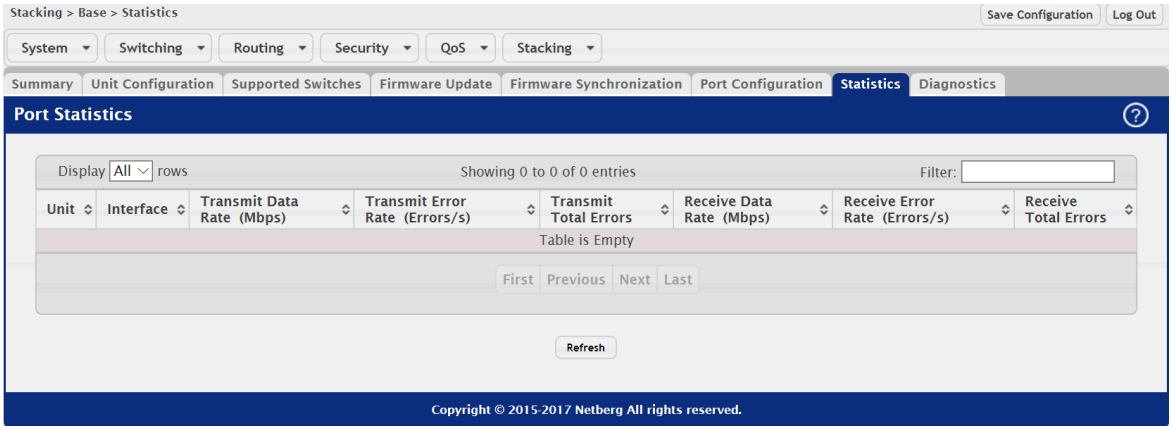
After you select a port and click **Edit**, a window opens and allows you to configure the stack port mode. The additional field available in the window is described below.

Interface Mode	The stack mode to configure on the port. The options are: • Ethernet – Configure the port to operate as an Ethernet port that connects to other network devices, such as servers or end-user hosts. • Stack – Configure the port to operate as a stacking port that connects to other units within the stack.

If you change the stack mode on a port, the configuration is immediately saved in the NVRAM on the unit on which the port is located. However, the run-time mode is not changed until the unit resets.

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

7.1.7. Stacking > Base > Statistics

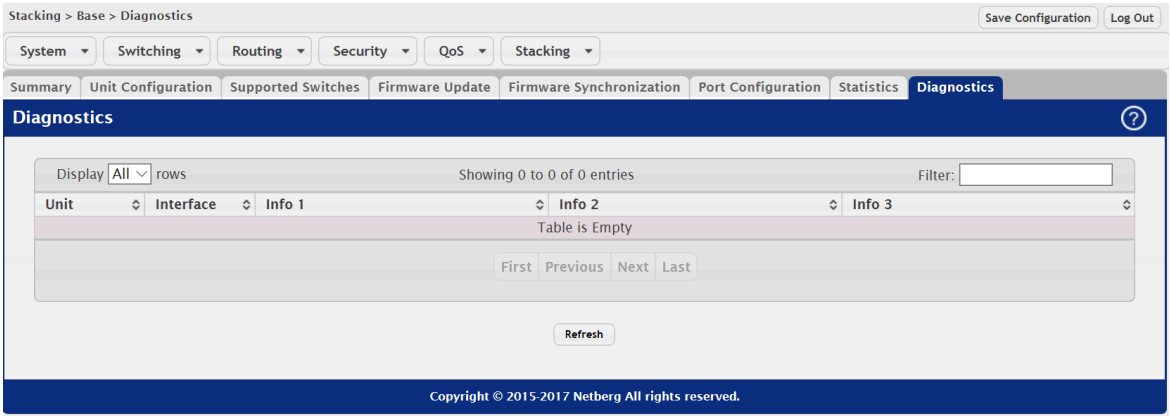


Use this page to view data transmission information for the stacking ports on each stack unit.

Unit	The number that identifies the unit within the stack (also called Switch ID).
Interface	The interface ID of the stackable interface on the unit.
Transmit Data Rate (Mbps)	The approximate rate at which the stack port transmits data.
Transmit Error Rate (Errors/s)	The approximate rate at which the stack port encounters errors when attempting to transmit data.
Transmit Total Errors	The total number of errors the stack port has encountered during data transmission since the unit booted. The counter might wrap if the number of errors exceeds the number the page can display.
Receive Data Rate (Mbps)	The approximate rate at which the stack port receives data.
Receive Error Rate (Errors/s)	The approximate rate at which the stack port encounters errors when attempting to receive data.
Receive Total Errors	The total number of errors the stack port has encountered while attempting to receive data since the unit booted. The counter might wrap if the number of errors exceeds the number the page can display.

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

7.1.8. Stacking > Base > Diagnostics



Use this page to view diagnostic information about stack ports. The page displays three text fields that are populated by the driver and contain debug and status information. Each text field supports a string of up to 80 characters. The following abbreviations are used in the information messages:

- RBYT: Received bytes (including CRC)
- RPKT: Received packets
- TBYT: Transmit bytes
- TPKT: Transmit packets
- RFCS: Receive FCS (CRC) error packet counter
- RFRG: Fragmented packets received (undersized packets with invalid CRC)
- RJBR: Oversized packets with invalid CRC
- RUND: Undersized packets (contains a valid CRC)
- ROVR: Oversized packets with no errors
- RUNT: Frames that are less than the IEEE 802.3 minimum length of 64 octets
- TFCS: Frames transmitted with an FCS error (CRC checks failed)
- TERR: Frames transmitted with any error

Unit	The number that identifies the unit within the stack (also called Switch ID).
Interface	The stackable interface on the unit.
Info 1	Debug and status driver information.
Info 2	Debug and status driver information.
Info 3	Debug and status driver information.

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