

Web UI Reference Guide

Product Model: DXS-3600 Series

Layer 2/3 Managed 10Gigabit Ethernet Switch

Release 2.00

Information in this document is subject to change without notice. Reproduction of this document in any manner, without the written permission of the D-Link Corporation, is strictly forbidden.

Trademarks used in this text: D-Link and the D-Link logo are trademarks of the D-Link Corporation; Microsoft and Windows are registered trademarks of the Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either as the entities claiming the marks and the names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

© 2013 D-Link Corporation. All rights reserved.

October, 2013. P/N 651XS3632010G

Table of Contents

1. Introduction	1
Audience	1
Other Documentation	1
Conventions	1
Notes, Notices, and Cautions	1
2. Web-based Switch Configuration	3
Management Options	3
Connecting using the Web User Interface	3
Logging onto the Web Manager	3
Web User Interface (Web UI)	4
Areas of the User Interface	4
3. System	6
Device Information	6
Device Information	6
Temperature Status	7
CPU Status	8
System Log Entries	9
Fan Status	11
Flash, SD Card, and Memory Status	12
Port Configuration	13
Port Settings	13
Port Status	14
Port Auto Negotiation	15
Jumbo Frame	16
System Log	16
System Log Settings	16
System Log Discriminator Settings	18
System Log Server Settings	19
System Log	20
System Attack Log	20
Time Profile	20
4. Management	22
User Account Settings	22
5. Layer 2 Features	24
FDB	24
Static FDB	24
MAC Address Table Settings	25
MAC Address Table	26
MAC Notification	27
VLAN	28
802.1Q VLAN	28
802.1v Protocol VLAN	29
GVRP	30
MAC VLAN	34

VLAN Interface	35
Subnet VLAN	39
Private VLAN	40
Spanning Tree	41
STP Global Settings	41
STP Port Settings	43
MST Configuration Identification	45
STP Instance	46
MSTP Port Information	46
Link Aggregation	46
L2 Protocol Tunnel.....	49
L2 Multicast Control	51
Multicast Filtering.....	51
6. Layer 3 Features.....	52
ARP	52
ARP Aging Time	52
Static ARP.....	52
Proxy ARP	53
ARP Table.....	53
Gratuitous ARP	54
IPv4 Interface.....	55
IPv4 Static/Default Route.....	56
IPv4 Route Table	57
IPv6 Interface.....	58
IPv6 Static/Default Route.....	59
IPv6 Route Table	60
7. Quality of Service (QoS).....	62
Basic Settings	62
Port Default CoS.....	62
Port Scheduler Method.....	62
Queue Settings	64
CoS to Queue Mapping	65
Port Rate Limiting	65
Queue Rate Limiting	66
Advanced Settings.....	67
DSCP Mutation Map.....	67
Port Trust State and Mutation Binding.....	68
DSCP CoS Mapping	69
CoS Color Mapping	70
DSCP Color Mapping	70
Class Map.....	71
Aggregate Policer	73
Policy Map	76
Policy Binding	77
8. Access Control List (ACL).....	78
ACL Access List.....	78
Standard IP ACL.....	78

Extend IP ACL	81
Standard IPv6 ACL	101
Extend IPv6 ACL	105
Extend MAC ACL.....	117
Expert ACL.....	120
ACL Interface Access Group	147
ACL VLAN Access Map	148
ACL VLAN Filter.....	149
9. Security	150
Trusted Host.....	150
10. Monitoring.....	151
Mirror Settings.....	151
Traffic	152
Traffic Monitoring by Direction	152
Traffic Monitoring by Type	153
Traffic Monitoring by Size	154
Traffic Monitoring by Error	155
11. Save and Tools.....	156
Save Configuration	156
Firmware Upgrade & Backup.....	156
Firmware Upgrade from HTTP	156
Firmware Upgrade from TFTP.....	157
Firmware Backup to HTTP	157
Firmware Backup to TFTP.....	158
Configuration Restore & Backup	158
Configuration Restore from HTTP	158
Configuration Restore from TFTP	159
Configuration Backup to HTTP	159
Configuration Backup to TFTP	160
Log Backup	160
Log Backup to HTTP	160
Log Backup to TFTP.....	161
Reset.....	161
Reboot System	162
Appendix A - Password Recovery Procedure.....	163
Appendix B - System Log Entries	165
Appendix C - Trap Entries.....	198
Appendix D - RADIUS Attributes Assignment	203
Appendix E - IETF RADIUS Attributes Support.....	206

1. Introduction

This manual's command descriptions are based on the software release 2.00. The commands listed here are the subset of commands that are supported by the DXS-3600 Series switch.

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the DXS-3600 Series switch, which will be generally be referred to simply as the "switch" within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

The documents below are a further source of information in regards to configuring and troubleshooting the switch. All the documents are available either from the CD, bundled with this switch, or from the D-Link website. Other documents related to this switch are:

- *DXS-3600 Series Hardware Installation Guide*
- *DXS-3600 Series CLI Reference Guide*

Conventions

Convention	Description
Boldface Font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the File menu and choose Cancel . Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: You have mail . Bold font is also used to represent filenames, program names and commands. For example: use the copy command.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Menu Name > Menu Option	Indicates the menu structure. Device > Port > Port Properties means the Port Properties menu option under the Port menu option that is located under the Device menu.
<i>Blue Courier Font</i>	This convention is used to represent an example of a screen console display including example entries of CLI command input with the corresponding output.

Notes, Notices, and Cautions

Below are examples of the three types of indicators used in this manual. When administering your switch using the information in this document, you should pay special attention to these indicators. Each example below provides an explanatory remark regarding each type of indicator.



NOTE: A note indicates important information that helps you make better use of your device.



NOTICE: A notice indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



CAUTION: A caution indicates a potential for property damage, personal injury, or death.

2. Web-based Switch Configuration

Management Options

Connecting using the Web User Interface

Logging onto the Web Manager

Web User Interface (Web UI)

Management Options

This switch provides multiple access platforms that can be used to configure, manage and monitor networking features available on this switch. Currently there are three management platforms available and they are described below.

The Command Line Interface (CLI) through the Serial Port or remote Telnet

This switch can be managed, out-of-band, by using the console port on the front panel of the switch. Alternatively, the switch can also be managed, in-band, by using a Telnet connection to any of the LAN ports on this switch. The command line interface provides complete access to all switch management features.

SNMP-based Management

The switch can be managed with an SNMP-compatible console program. The switch supports SNMP version 1.0, version 2.0 and version 3.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Web-based Management Interface

After successfully installing the switch, the user can configure the switch, monitor the LED panel, and display statistics graphically using a Web browser, such as Microsoft® Internet Explorer (version 6 and later), Mozilla Firefox (version 3 and later), Safari (version 5 and later), Google Chrome (version 5 and later), Opera (version 12 and later), or Netscape (version 8 and later).

Connecting using the Web User Interface

Most software functions of the DXS-3600 Series switches can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the switch from remote stations anywhere on the network through a standard web browser. The web browser acts as a universal access tool and can communicate directly with the switch using the HTTP or HTTPS protocol.



NOTE: The Command Line Interface (CLI) provides the functionality of managing, configuring, and monitoring **all** of the software features that are available on this switch.

Logging onto the Web Manager

To access the Web User Interface, simply open a standard web browser on the management PC and enter the switch's default IP address into the address bar of the browser and press the **Enter** key.



NOTE: The default IP address of this switch is **10.90.90.90**, with a subnet mask of **255.0.0.0**.

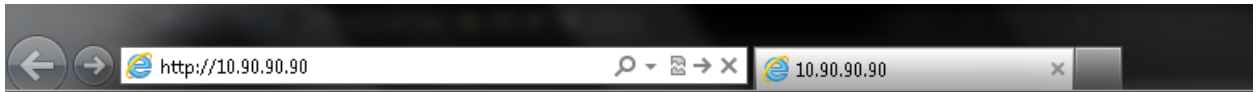


Figure 2-1 Displays entering the IP address in Internet Explorer

This will open the user authentication window, as seen below.



Figure 2-2 User Authentication Window

By default, there is no username or password configured on this switch. When connecting to the Web UI for the first time simply leave the **User Name** and **Password** fields blank and click the **Login** button.

Web User Interface (Web UI)

The user interface provides access to various switch configuration and management windows, to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. Three distinct areas that divide the user interface, as described in the table.

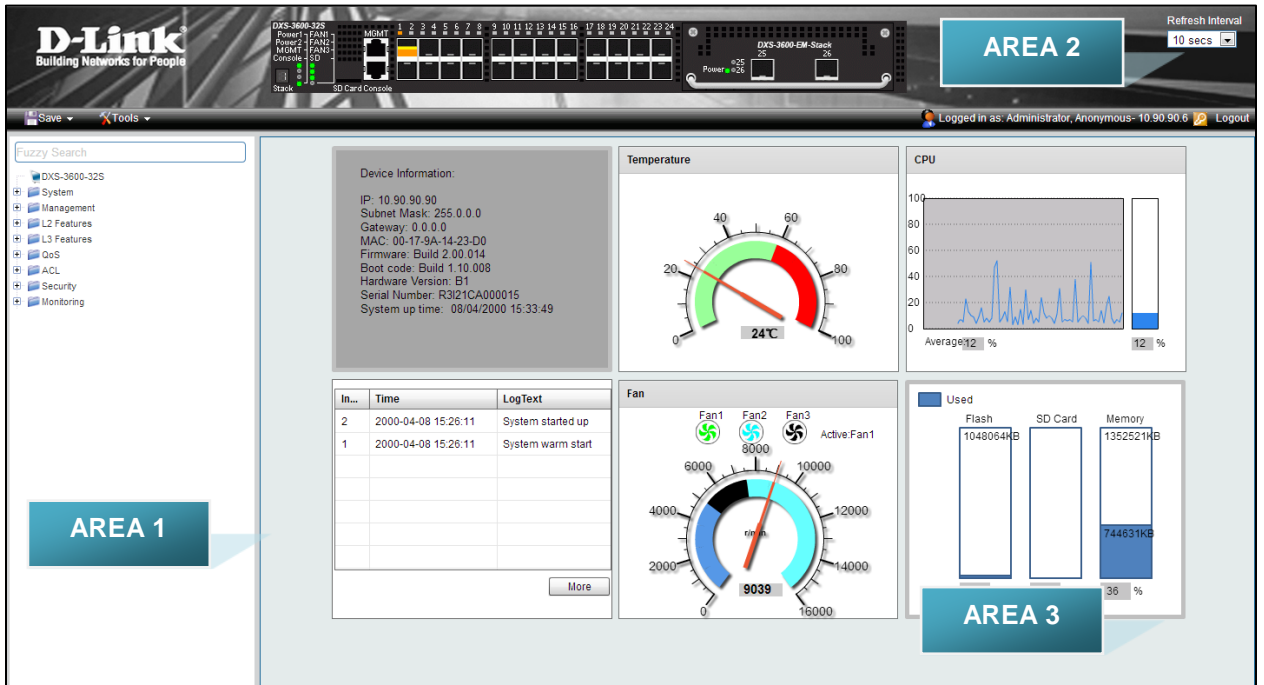


Figure 2-3 Main Web UI Window

Area Number	Description
AREA 1	In this area, a folder tree layout is displayed of functions that can be configured using the Web UI. Open folders and click the hyperlinked menu buttons to access each individual page for configuration. The DXS-3600-32S link is the default page that will display basic monitoring settings for this switch.
AREA 2	In this area, a graphical near real-time image of the front panel of the switch is displayed. Some management functions, like Save and Tools are accessible here.
AREA 3	In this area, the switch's configuration page can be found, based on the selection made in Area 1 .

3. System

Device Information
Port Configuration
System Log
Time Profile

Device Information

On this page, the Device Information, Temperature status, CPU, Usage status, System Log, Fan status, and Memory usage status are displayed. It appears automatically when you log on to the switch. To return to the Device Information window after viewing other windows, click the **DXS-3600-32S** link.

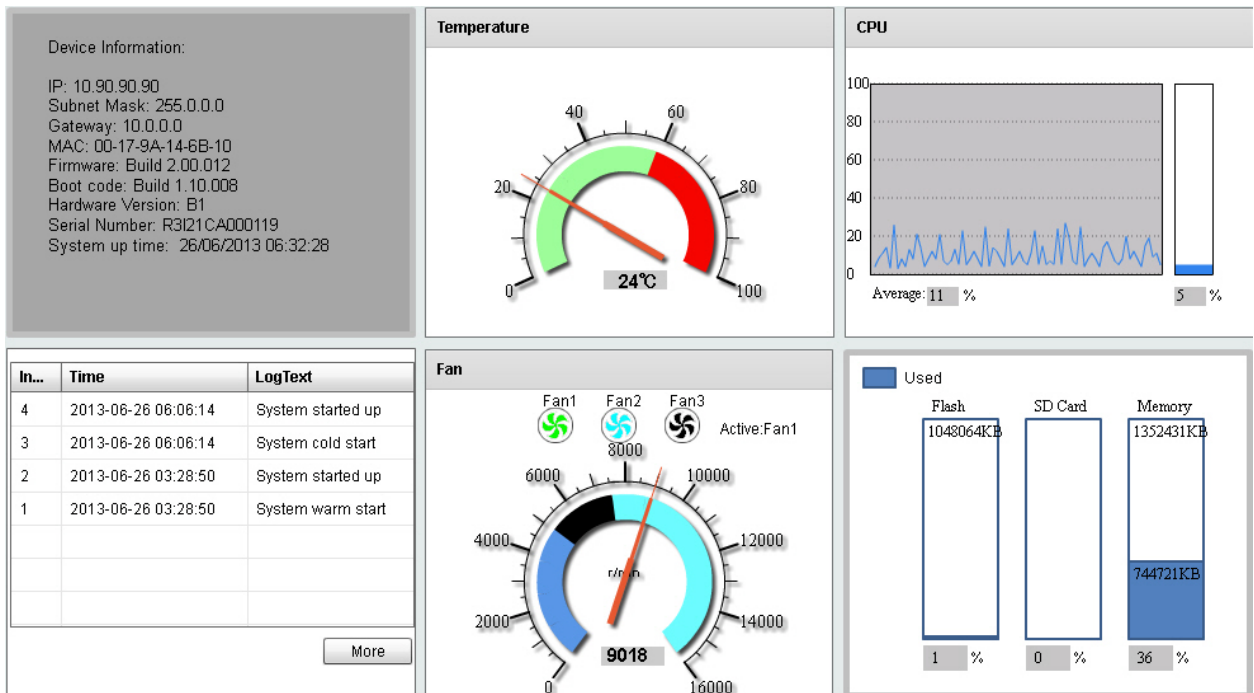


Figure 3-1 Device Information Window

Device Information

In the Device Information section, the user can view a list of basic information regarding the switch.

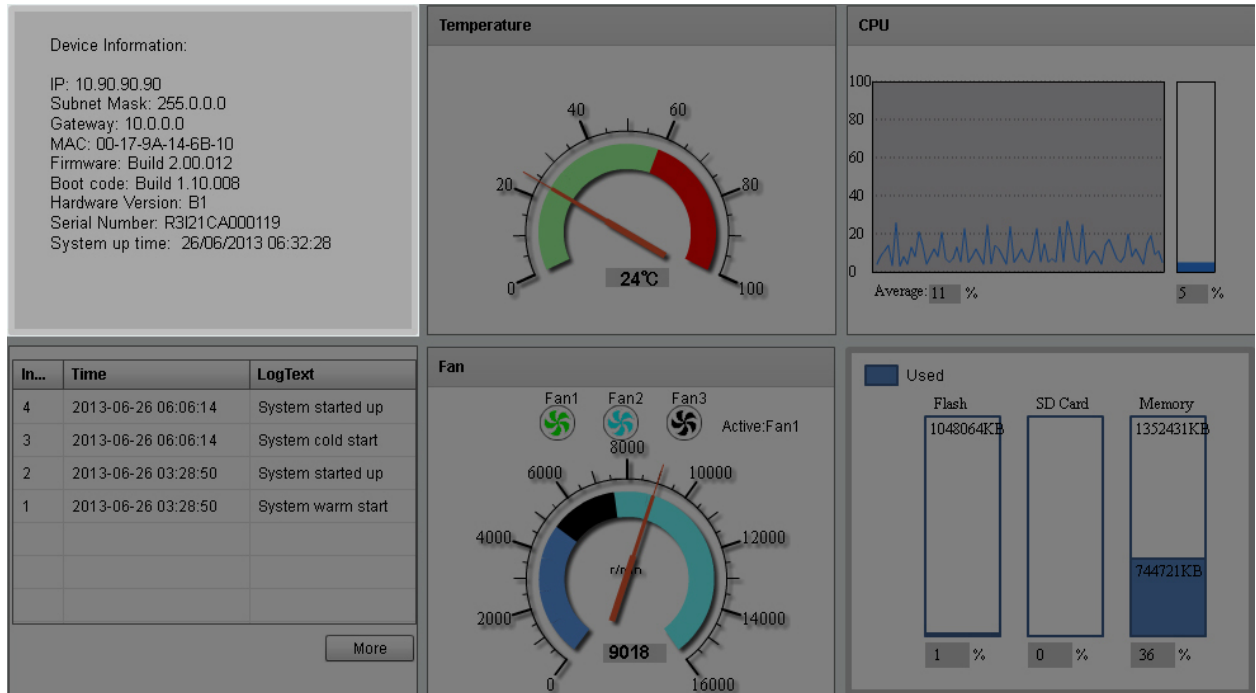


Figure 3-2 Device Information (Highlight) Window

In the **Device Information** section, the following display parameters are available:

Parameter	Description
IP Address	Here the IP address of the switch's main interface is displayed.
Subnet Mask	Here the Subnet Mask of the switch's main interface is displayed.
Gateway	Here the Gateway IP address of the switch's main interface is displayed.
MAC Address	Here the MAC address of the switch is displayed.
Firmware Version	Here the Firmware version of the switch is displayed.
Boot Code Version	Here the Boot Code of the switch is displayed.
Hardware Version	Here the Hardware version of the switch is displayed.
Serial Number	Here the Serial number of the switch is displayed.
System Up Time	Here the System's up time is displayed.

Temperature Status

In the **Temperature** section, the user can view a real-time display of the switch's internal temperature. The temperature of the switch is mainly influenced by two factors: (1) the environment, and (2) the internal air-flow of the switch. In the *DXS-3600 Series Hardware Installation Guide*, there are some guidelines that can assist the user with the installation of this switch in a temperature friendly environment. The fan modules, installed in this switch, have temperature sensors built-in that automatically controls the air-flow inside the switch.

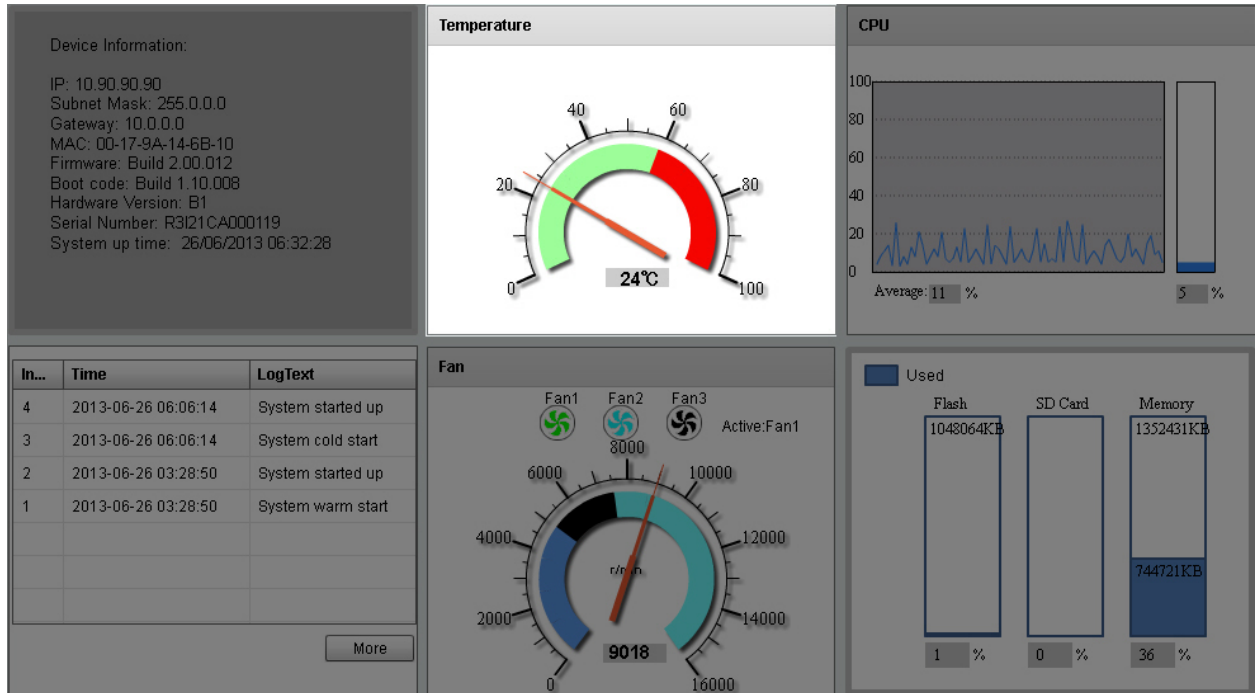


Figure 3-3 Temperature Status Window

In the **Temperature** section, the following display parameters are available:

Parameter	Description
Percentage Display	In this graphic, the reading is divided into percentage sections. The green area is known as the 'safe' area. This area ranges from 0% to 60%. This is the optimum temperature range recommended for this switch.
Temperature	Below the percentage gauge needle, the accurate temperature reading, for this switch, is displayed in degrees Celsius.
Warning Section	In this graphic, the reading is divided into percentage sections. The red area is known as the 'warning' area. This area ranges from 60% to 100%. It is recommended not to allow the switch to run this hot, to avoid component damage.

CPU Status

In the CPU section, the user can view a real-time display of the switch's CPU usage. There are a number of factors that can influence a depleted CPU usage. One of those factors is network broadcasts. In the *DXS-3600 Series CLI Reference Guide* there is an abundance of features that can be enabled to prevent this problem from occurring.

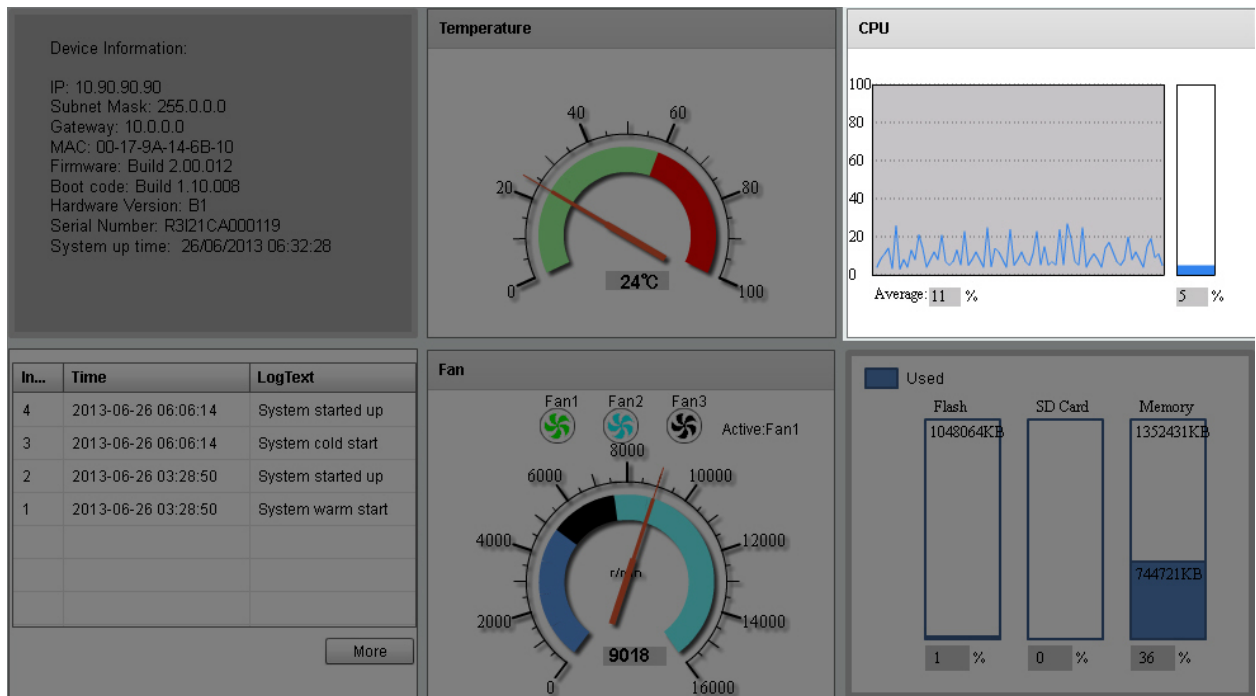


Figure 3-4 CPU Status Window

In the **CPU** section, the following display parameters are available:

Parameter	Description
Percentage Display	In this graphic, the reading is divided into percentage sections. This area ranges from 0% to 100%.
Average	Below the CPU percentage line chart, we find an accurate display of the average CPU usage percentage.
Percentage Bar	In this graphic, an accurate reading of the real-time CPU usage percentage is displayed.

System Log Entries

In the System Log section, the user can view a list of System log entries, generated by the switch, when certain events have occurred.

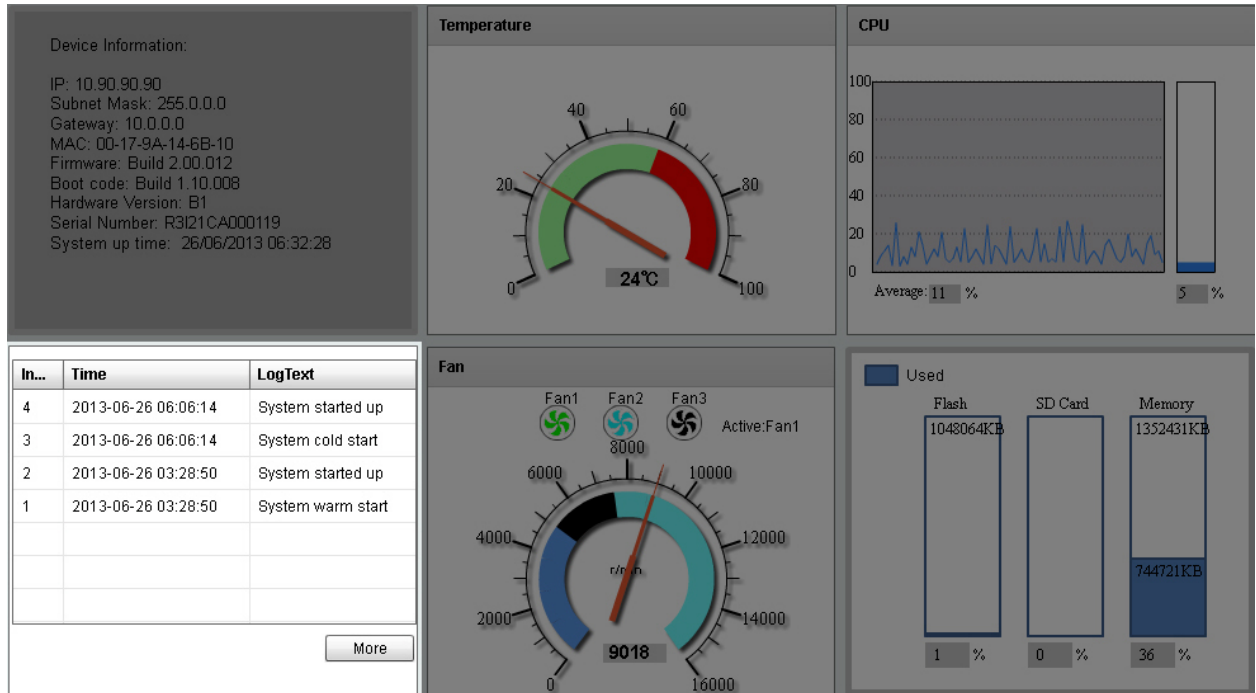


Figure 3-5 System Log Window

In the **System Log** section, the following display parameters are available:

Parameter	Description
Entry Number	Every log entry has a specific entry number, generated when the log entry was added to the System log entry display. Here the System log entry number is displayed in reverse order.
Time	Here the specific date and time of the log entry is displayed.
Log Text	Here the log entry description is displayed.

Click the **More** button to view a larger display of the complete System Log section.

After clicking the **More** button, the following window will appear:

In the **Fan** section, the following display parameters are available:

Parameter	Description
Fan Number	At the top of this graphic, the list of installed fans is displayed. After clicking on any specific fan icon, the real-time RPM gauge of that fan will be displayed. Also after clicking on a fan icon, the Active Fan display parameter will change accordingly.
RPM Graph	In this graph (gauge display), we observe the RPM speed at which the selected fan is working at.
RPM Reading	At the bottom of the graphics, we observe the accurate real-time display of the RPM value for a specific fan.

Flash, SD Card, and Memory Status

In this section, the user can view a real-time graphic that represents the memory usage for the **Flash**, **SD Card**, and **RAM Memory**.

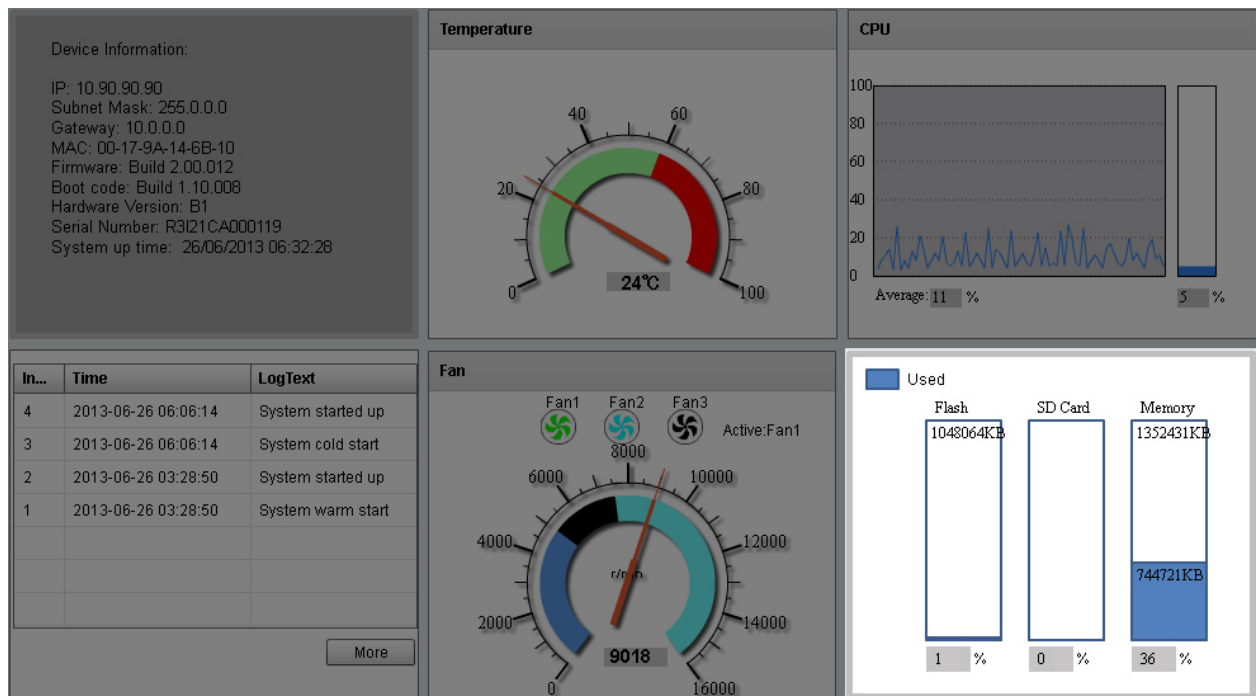


Figure 3-8 Flash, SD Card, and Memory Status Window

In this section, the following display parameters are available:

Parameter	Description
Used	This displays the color that represents the used memory allocation.
Flash	This displays the used and unused space of the Flash. The more accurate percentage display can be found below the graphic.
SD Card	This displays the used and unused space of the SD Card. The more accurate percentage display can be found below the graphic.
Memory	This displays the used and unused space of the Memory. The more accurate percentage display can be found below the graphic.

Port Configuration

Port Settings

On this page, users can view and configure the switch's port settings. To view the following window, click **System > Port Configuration > Port Settings**, as shown below:

Port	Link Status	State	MDIX	Flow Control		Duplex	Speed	Description
				Send	Receive			
eth1/0/1	Up	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/2	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/3	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/4	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/5	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/6	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/7	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/8	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/9	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/10	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/11	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/12	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/13	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/14	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/15	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/16	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/17	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	
eth1/0/18	Down	Enabled	Auto-mdix	Off	Off	Auto-duplex	Auto-speed	

Figure 3-9 Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the appropriate port range used for the configuration here.
Medium Type	Select the port medium type here. Options to choose from are RJ45 and SFP . Note: Selecting the SFP option, includes the use of SFP+ transceivers for 10G connectivity.
State	Select this option to enable or disabled the physical port here.
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are Auto, Normal, and Cross. Auto - Select this option for auto-sensing of the optimal type of cabling. Normal - Select this option for normal cabling. If this option is selected, the port is in the MDI mode and can be connected to a PC's NIC using a straight-through cable or a port (in the MDI mode) on another switch through a cross-over cable. Cross - Select this option for cross cabling. If this option is selected, the port is in the MDIX mode and can be connected to a port (in the MDI mode) on another switch through a straight cable.

Flow Control	Select to either turn flow control On or Off here. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use back-pressure flow control, and Auto ports use an automatic selection of the two.
Duplex	Select the duplex mode used here. Options to choose from are Auto , Half , and Full .
Speed	Select the port speed option here. This option will manually force the connected on the selected port to only connect at the speed specified here. Options to choose from are Auto , 10M , 100M , 1000M , 1000M Master , 1000M Slave , 10G , 10G Master , 10G Slave , and 40G . The switch allows users to configure two types of gigabit connections; 1000M Master and 1000M Slave which refer to connections running a 1000BASE-T cable for connection between the switch port and another device capable of a gigabit connection. The master setting (1000M Master) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (1000M Slave) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for 1000M Master, the other side of the connection must be set for 1000M Slave. Any other configuration will result in a link down status for both ports. Note: The 10M and 100M speed options are only applicable when the DXS-3600-EM-8T expansion module is used.
Capability Advertised	When the Speed is set to Auto , these capabilities are advertised during auto-negotiation.
Description	Enter a 64 characters description for the corresponding port here.

Click the **Apply** button to accept the changes made.

Port Status

On this page, users can view the switch's physical port status and settings. To view the following window, click **System > Port Configuration > Port Status**, as shown below:

Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
eth1/0/1	connected	00-17-9A-14-6C-10	1	Off	Off	A-full	A-1000	10GBASE-R
eth1/0/2	not-connected	00-17-9A-14-6C-11	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/3	not-connected	00-17-9A-14-6C-12	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/4	not-connected	00-17-9A-14-6C-13	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/5	not-connected	00-17-9A-14-6C-14	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/6	not-connected	00-17-9A-14-6C-15	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/7	not-connected	00-17-9A-14-6C-16	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/8	not-connected	00-17-9A-14-6C-17	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/9	not-connected	00-17-9A-14-6C-18	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/10	not-connected	00-17-9A-14-6C-19	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/11	not-connected	00-17-9A-14-6C-1A	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/12	not-connected	00-17-9A-14-6C-1B	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/13	not-connected	00-17-9A-14-6C-1C	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/14	not-connected	00-17-9A-14-6C-1D	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/15	not-connected	00-17-9A-14-6C-1E	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/16	not-connected	00-17-9A-14-6C-1F	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/17	not-connected	00-17-9A-14-6C-20	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/18	not-connected	00-17-9A-14-6C-21	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/19	not-connected	00-17-9A-14-6C-22	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/20	not-connected	00-17-9A-14-6C-23	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/21	not-connected	00-17-9A-14-6C-24	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/22	not-connected	00-17-9A-14-6C-25	1	Off	Off	Auto	Auto	10GBASE-R

Figure 3-10 Port Status Window

Port Auto Negotiation

On this page, users can view detailed port auto-negotiation information. To view the following window, click **System > Port Configuration > Port Auto Negotiation**, as shown below:

Port	AN	RS	CS	CB	CAB	CRB	RFA	RFR
eth1/0/1	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/2	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/3	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/4	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/5	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/6	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/7	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/8	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/9	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/10	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/11	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/12	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/13	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/14	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/15	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/16	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/17	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/18	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/19	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/20	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/21	Enabled	Not detected	-	-	-	-	Disabled	NoError
eth1/0/22	Enabled	Not detected	-	-	-	-	Disabled	NoError

Figure 3-11 Port Auto Negotiation Window

Jumbo Frame

On this page, users can view and configure the Jumbo Frame size and settings. The switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1,518 bytes of payload. The switch supports jumbo frames with a maximum frame size of up to 12288 bytes. To view the following window, click **System > Port Configuration > Jumbo Frame**, as shown below:

Port	Maximum Receive Frame Size (bytes)
eth1/0/1	1536
eth1/0/2	1536
eth1/0/3	1536
eth1/0/4	1536
eth1/0/5	1536
eth1/0/6	1536
eth1/0/7	1536
eth1/0/8	1536
eth1/0/9	1536
eth1/0/10	1536
eth1/0/11	1536
eth1/0/12	1536
eth1/0/13	1536
eth1/0/14	1536
eth1/0/15	1536
eth1/0/16	1536
eth1/0/17	1536
eth1/0/18	1536
eth1/0/19	1536
eth1/0/20	1536
eth1/0/21	1536

Figure 3-12 Jumbo Frame Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the appropriate port range used for the configuration here.
Maximum Receive Frame Size	Enter the maximum receive frame size value here. This value must be between 64 and 12288 bytes. By default, this value is 1536 bytes.

Click the **Apply** button to accept the changes made.

System Log

System Log Settings

On this page, users can view and configure the system's log settings.

To view the following window, click **System > System Log > System Log Settings**, as shown below:

The screenshot shows the 'System Log Settings' window. It is organized into four main sections, each with an 'Apply' button:

- Global State:** Source Interface State (Enabled), Type (VLAN), Interface ID (1-4094) (1).
- Buffer Log Settings:** Buffer Log State (Enabled), Severity (4(Warnings)), Discriminator Name (15 chars), Write Delay (0-65535) (300) sec Infinite.
- Console Log Settings:** Console Log State (Disabled), Severity (4(Warnings)), Discriminator Name (15 chars).
- SMTP Log Settings:** SMTP Log State (Disabled), Severity (4(Warnings)), Discriminator Name (15 chars).

Figure 3-13 System Log Settings Window

The fields that can be configured for **Global State** are described below:

Parameter	Description
Source Interface State	Select this option to enable or disable the source interface's global state.
Type	Select the type of interface that will be used. Options to choose from are Loopback , Mgmt , and VLAN .
Interface ID	Enter the interface's ID used here. When selecting the Loopback option as the Type , enter the interface's ID used here. This value must be between 1 and 8 . When selecting the Mgmt option as the Type , enter the interface's ID used here. This value can only be 0 as there is only one management interface. When selecting the VLAN option as the Type , enter the interface's ID used here. This value must be between 1 and 4094 .

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Buffer Log Settings** are described below:

Parameter	Description
Buffer Log State	Select whether the enable or disable the buffer log's global state here. Options to choose from are Enable , Disabled , and Default . When selecting the Default option, the buffer log's global state will follow the default behavior.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) .
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long.
Write Delay	Enter the log's write delay value here. This value must be between 0 and 65535 seconds. By default, this value is 300 seconds. Tick the

Infinite option, to disable the write delay feature.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Console Log Settings** are described below:

Parameter	Description
Console Log State	Select whether the enable or disable the console log's global state here.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) .
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **SMTP Log Settings** are described below:

Parameter	Description
SMTP Log State	Select whether the enable or disable the SMTP log's global state here.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) .
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long.

Click the **Apply** button to accept the changes made.

System Log Discriminator Settings

On this page, users can view and configure the system log's discriminator settings.

To view the following window, click **System > System Log > System Log Discriminator Settings**, as shown below:

Name	Facility	Facility List	Severity	Severity List	
Discriminato...	includes	SYS,WEB,CFG,FIRMWARE...	drops	7	Delete

Figure 3-14 System Log Discriminator Settings Window

The fields that can be configured are described below:

Parameter	Description
Discriminator	Enter the discriminator name here. This name can be up to 15 characters long.
Facility	Select the facility's behavior option and the type of facility that will be associated with the selected behavior here. Behavior options to choose from are Drops and Includes .
Severity	Select the severity behavior option and the value of the type of information that will be logged. Behavior options to choose from are Drops and Includes . Severity value options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) .

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

System Log Server Settings

On this page, users can view and configure system log's server settings.

To view the following window, click **System > System Log > System Log Server Settings**, as shown below:

Figure 3-15 System Log Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the system log server's IPv4 address here.
Host IPv6 Address	Enter the system log server's IPv6 address here.
UDP Port	Enter the system log server's UDP port number here. This value must be between 1024 and 65535. By default, this value is 514.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) .
Facility	Select the facility value here. Options to choose from are 0 to 23.
Discriminator Name	Enter the discriminator name here. This name can be up to 15

	characters long.
VRF Name	Enter the VRF name, that will be associated with this configuration, here.

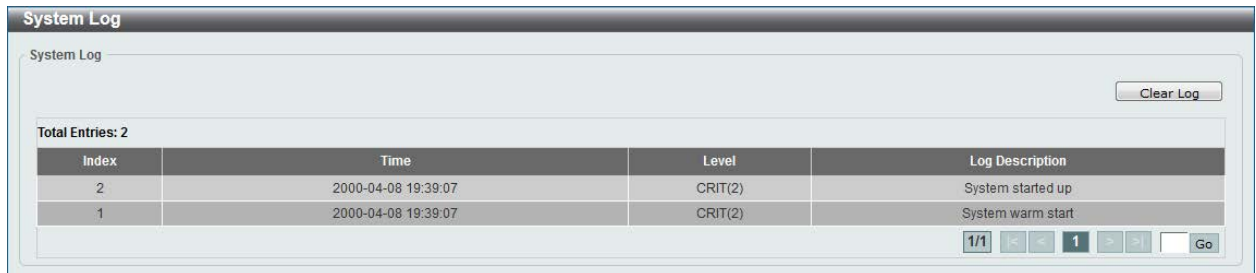
Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

System Log

On this page, users can view and clear the system log.

To view the following window, click **System > System Log > System Log**, as shown below:



The screenshot shows the 'System Log' window with a 'Clear Log' button in the top right. Below the button, it indicates 'Total Entries: 2'. A table displays the log entries:

Index	Time	Level	Log Description
2	2000-04-08 19:39:07	CRIT(2)	System started up
1	2000-04-08 19:39:07	CRIT(2)	System warm start

At the bottom right of the table, there is a pagination control showing '1/1' and a 'Go' button.


Figure 3-16 System Log Window

Click the **Clear Log** button to clear the system log entries displayed in the table.

System Attack Log

On this page, users can view and clear the system attack log.

To view the following window, click **System > System Log > System Attack Log**, as shown below:



The screenshot shows the 'System Attack Log' window with a 'Clear Attack Log' button in the top right. Below the button, it indicates 'Total Entries: 0'. A table header is visible with the following columns:

Index	Time	Level	Log Description
-------	------	-------	-----------------

Figure 3-17 System Attack Log Window

Click the **Clear Attack Log** button to clear the system attack log entries displayed in the table.

Time Profile

On this page, users can view and configure the time profile settings.

To view the following window, click **System > Time Profile**, as shown below:

Figure 3-18 Time Profile Window

The fields that can be configured are described below:

Parameter	Description
Range Name	Enter the time profile's range name here. This name can be up to 32 characters long.
From Week ~ To Week	Select the starting and ending days of the week that will be used for this time profile. Tick the Daily option to use this time profile for every day of the week. Tick the End Week Day option to use this time profile from the starting day of the week until the end of the week, which is Sunday.
From Time ~ To Time	Select the starting and ending time of the day that will be used for this time profile. The first drop-down menu selects the hour and the second drop-down menu selects the minute.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete Periodic** button to delete the periodic entry.

Click the **Delete** button to delete the specified entry.

4. Management

User Account Settings

User Account Settings

On this page, user accounts can be created and configured. Also on this page active user account sessions can be viewed.

There are several configuration options available in the Web User Interface (Web UI). The set of configuration options available to the user depends on the account's **Privilege Level**.



NOTE: By default, there is no user account created on this switch.

To view the following window, click **Management > User Account Settings**, as shown below:

After selecting the **User Management Settings** tab, the following page will appear.

Figure 4-1 User Management Settings Window

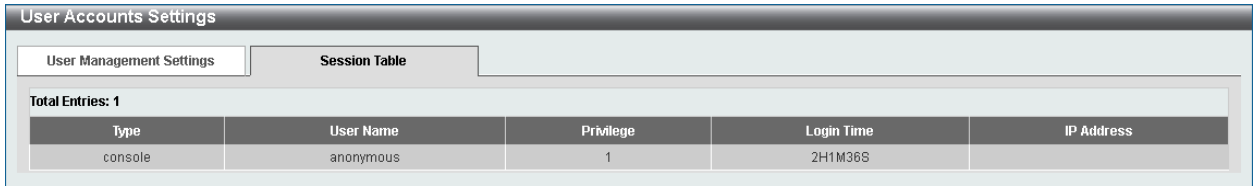
The fields that can be configured are described below:

Parameter	Description
User Name	Enter the user account name here. This name can be up to 32 characters long.
Privilege	Enter the privilege level for this account here. This value must be between 1 and 15.
Password Type	Select the password type for this user account here. Options to choose from are None , Simple , and Cipher .
Password	After selecting either Simple or Cipher as the password type, enter the password for this user account here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified user account entry.

After selecting the **Session Table** tab, the following page will appear.



The screenshot shows the 'User Accounts Settings' web interface. It features two tabs: 'User Management Settings' and 'Session Table'. The 'Session Table' tab is active, displaying a table with the following data:

Type	User Name	Privilege	Login Time	IP Address
console	anonymous	1	2H1M36S	

Figure 4-2 Session Table Window

On this page, a list of active user account session will be displayed.

5. Layer 2 Features

FDB
VLAN
Spanning Tree
Link Aggregation
L2 Protocol Tunnel
L2 Multicast Control

FDB

Static FDB

Unicast Static FDB

On this page, users can view and configure the static unicast forwarding settings on the switch. To view the following window, click **L2 Features > FDB > Static FDB > Unicast Static FDB**, as shown below:

Figure 5-1 Unicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description
Port/Drop	Allows the selection of the port number on which the MAC address entered resides. This option could also drop the MAC address from the unicast static FDB. When selecting Port , select the port number.
Port Number	After selecting the Port option, select the port number used here.
VLAN ID	Enter the VLAN ID on which the associated unicast MAC address resides.
MAC Address	Enter the MAC address to which packets will be statically forwarded. This must be a unicast MAC address.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to delete all the entries found in the display table.

Click the **Delete** button to delete the specified entry.

Multicast Static FDB

On this page, users can view and configure the multicast static FDB settings. To view the following window, click **L2 Features > FDB > Static FDB > Multicast Static FDB**, as shown below:

Figure 5-2 Multicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
VLAN ID	Enter the VLAN ID of the VLAN the corresponding MAC address belongs to.
MAC Address	Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address. The format of the destination MAC address is 01-XX-XX-XX-XX-XX.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries.

Click the **Delete** button to remove the specific entry.

MAC Address Table Settings

On this page, users can view and configure the MAC address table's global settings. To view the following window, click **L2 Features > FDB > MAC Address Table Settings**, as shown below:

Figure 5-3 MAC Address Table Settings (Global Settings) Window

The fields that can be configured are described below:

Parameter	Description
Aging Time	Enter the MAC address table's aging time value here. This value must be between 10 and 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.
Aging Destination Hit	Select to enable or disable the aging destination hit function.

Click the **Apply** button to accept the changes made.

After selecting the **MAC Address Learning** tab option, at the top of the page, the following page will be available.

Port	State
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Enabled
eth1/0/7	Enabled
eth1/0/8	Enabled
eth1/0/9	Enabled
eth1/0/10	Enabled
eth1/0/11	Enabled
eth1/0/12	Enabled
eth1/0/13	Enabled
eth1/0/14	Enabled
eth1/0/15	Enabled
eth1/0/16	Enabled
eth1/0/17	Enabled
eth1/0/18	Enabled
eth1/0/19	Enabled
eth1/0/20	Enabled

Figure 5-4 MAC Address Table Settings (MAC Address Learning) Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the MAC address learning function on the ports specified here.

Click the **Apply** button to accept the changes made.

MAC Address Table

On this page, users can view the entries listed in the MAC address table. To view the following window, click **L2 Features > FDB > MAC Address Table**, as shown below:

VLAN ID	MAC Address	Type	Port
1	00-11-22-33-44-55	Static	eth1/0/1
1	00-17-9A-14-23-D0	Static	CPU
1	10-BF-48-D6-E2-E2	Dynamic	eth1/0/1
1	F0-BF-97-15-45-60	Dynamic	eth1/0/1
1	01-00-00-00-00-02	Static	eth1/0/1

Figure 5-5 MAC Address Table Window

The fields that can be configured are described below:

Parameter	Description
-----------	-------------

Port	Select the port that will be used for this configuration here.
VLAN ID	Enter the VLAN ID that will be used for this configuration here.
MAC Address	Enter the MAC address that will be used for this configuration here.

Click the **Apply** button to accept the changes made.

Click the **Clear Dynamic by Port** button to clear the dynamic MAC address listed on the corresponding port.

Click the **Clear Dynamic by VLAN** button to clear the dynamic MAC address listed on the corresponding VLAN.

Click the **Clear Dynamic by MAC** button to clear the dynamic MAC address entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear All** button to clear all dynamic MAC addresses.

Click the **View All** button to display all the MAC addresses recorded in the MAC address table.

MAC Notification

On this page, users can view and configure MAC notification. To view the following window, click **L2 Features > FDB > MAC Notification**, as shown below:

Port	Added Trap	Removed Trap
eth1/0/1	Disabled	Disabled
eth1/0/2	Disabled	Disabled
eth1/0/3	Disabled	Disabled
eth1/0/4	Disabled	Disabled
eth1/0/5	Disabled	Disabled
eth1/0/6	Disabled	Disabled
eth1/0/7	Disabled	Disabled
eth1/0/8	Disabled	Disabled
eth1/0/9	Disabled	Disabled
eth1/0/10	Disabled	Disabled
eth1/0/11	Disabled	Disabled
eth1/0/12	Disabled	Disabled
eth1/0/13	Disabled	Disabled

Figure 5-6 MAC Notification (MAC Notification Settings) Window

The fields that can be configured are described below:

Parameter	Description
MAC Address Notification	Select to enable or disable MAC notification globally on the switch
Interval	Enter the time value between notifications. This value must be between 1 and 2147483647 seconds. By default, this value is 1 second.
History Size	Enter the maximum number of entries listed in the history log used for notification. This value must be between 0 and 500. By default, this

	value is 1.
MAC Notification Trap State	Select to enable or disable the MAC notification trap state.
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Added Trap	Select to enable or disable the added trap for the port(s) selected.
Removed Trap	Select to enable or disable the removed trap for the port(s) selected.

Click the **Apply** button to accept the changes made for each individual section.

After selecting the **MAC Notification History** tab, at the top of the page, the following page will be available.



Figure 5-7 MAC Notification (MAC Notification History) Window

On this page, a list of MAC notification messages will be displayed.

VLAN

802.1Q VLAN

On this page, users can view and configure the VLAN settings on this switch. To view the following window, click **L2 Features > VLAN > 802.1Q VLAN**, as shown below:

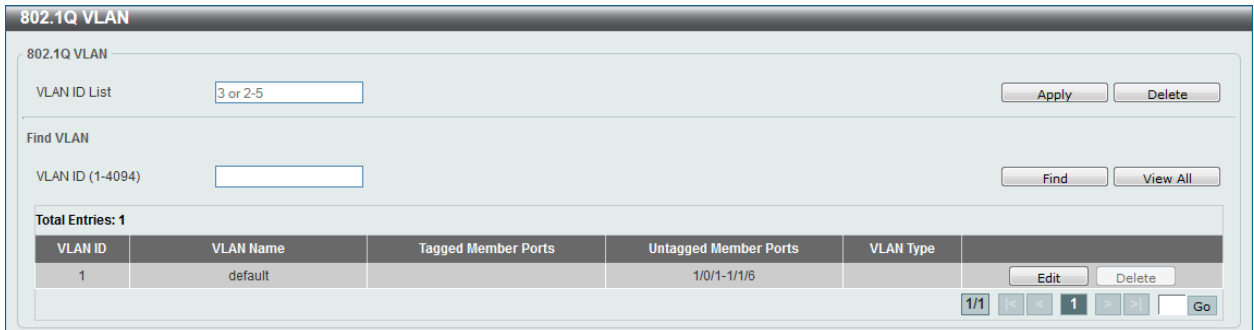


Figure 5-8 802.1Q VLAN Window

The fields that can be configured are described below:

Parameter	Description
VLAN ID List	Enter the VLAN ID list that will be created here.
VLAN ID	Enter the VLAN ID that will be displayed here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to locate all the entries.

Click the **Edit** button to re-configure the specific entry.

802.1v Protocol VLAN

Protocol VLAN Profile

On this page, users can view and configure 802.1v protocol VLAN profiles. The 802.1v Protocol VLAN Group Settings support multiple VLANs for each protocol and allows the user to configure the untagged ports of different protocols on the same physical port. For example, it allows the user to configure an 802.1Q and 802.1v untagged port on the same physical port. To view the following window, click **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile**, as shown below:

Figure 5-9 Protocol VLAN Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter the 802.1v protocol VLAN profile ID here. This value must be between 1 and 16.
Frame Type	Select the frame type option here. This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Options to choose from are Ethernet 2 , SNAP , and LLC .
Ether Type	Enter the Ethernet type value for the group here. The protocol value is used to identify a protocol of the frame type specified. The form of the input is 0x0 to 0xFFFF. Depending on the frame type, the octet string will have one of the following values: <ul style="list-style-type: none"> For Ethernet 2, this is a 16-bit (2-octet) hex value. For example, IPv4 is 0800, IPv6 is 86DD, ARP is 0806, etc... For IEEE802.3 SNAP, this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is a 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Protocol VLAN Profile Interface

On this page, users can view and configure the protocol VLAN profile's interface settings. To view the following window, click **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface**, as shown below:

Figure 5-10 Protocol VLAN Profile Interface Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port that will be used for this configuration here.
Profile ID	Select the 802.1v protocol VLAN profile ID here.
VLAN ID	Enter the VLAN ID used here.
Priority	Select the priority value used here. This value is between 0 and 7. This parameter is specified to re-write the 802.1p default priority previously set in the switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the switch that match this priority are forwarded to the CoS queue specified previously by the user.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

GVRP

GVRP Global

On this page, users can view and configure the GARP VLAN Registration Protocol (GVRP) global settings. To view the following window, click **L2 Features > VLAN > GVRP > GVRP Global**, as shown below:

Figure 5-11 GVRP Global Window

The fields that can be configured are described below:

Parameter	Description
Global GVRP State	Select to enable or disable the global GVRP state here.
Dynamic VLAN Creation	Select to enable or disable the dynamic VLAN creation function here.
NNI BPDU Address	Select the NNI BPDU address option here. This option is used to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address or 802.1ad service provider GVRP address. Options to choose from are Dot1d and Dot1ad .

Click the **Apply** button to accept the changes made.

GVRP Port

On this page, users can view and configure the GVRP port settings. To view the following window, click **L2 Features > VLAN > GVRP > GVRP Port**, as shown below:

GVRP Port

GVRP Port

From Port: eth1/0/1 To Port: eth1/0/1 GVRP Status: Disabled Join Time (10-10000): 20 centiseconds Leave Time (10-10000): 60 centiseconds Leave All Time (10-10000): 1000 centiseconds

Note:
The Leave Time should be no less than 3 * Join Time.
Leave All Time should be greater than Leave Time.

Port	GVRP Status	Join Time	Leave Time	Leave All Time
eth1/0/1	Disabled	20	60	1000
eth1/0/2	Disabled	20	60	1000
eth1/0/3	Disabled	20	60	1000
eth1/0/4	Disabled	20	60	1000
eth1/0/5	Disabled	20	60	1000
eth1/0/6	Disabled	20	60	1000
eth1/0/7	Disabled	20	60	1000
eth1/0/8	Disabled	20	60	1000
eth1/0/9	Disabled	20	60	1000
eth1/0/10	Disabled	20	60	1000
eth1/0/11	Disabled	20	60	1000
eth1/0/12	Disabled	20	60	1000
eth1/0/13	Disabled	20	60	1000
eth1/0/14	Disabled	20	60	1000
eth1/0/15	Disabled	20	60	1000
eth1/0/16	Disabled	20	60	1000
eth1/0/17	Disabled	20	60	1000
eth1/0/18	Disabled	20	60	1000

Figure 5-12 GVRP Port Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
GVRP Status	Select the enable or disable the GVRP port status. This enables the port to dynamically become a member of a VLAN. By default, this option is disabled.
Join Time	Enter the Join Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 20 centiseconds.
Leave Time	Enter the Leave Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 60 centiseconds.
Leave All Time	Enter the Leave All Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 1000 centiseconds.

Click the **Apply** button to accept the changes made.

GVRP Advertise VLAN

On this page, users can view and configure the GVRP advertised VLAN settings. To view the following window, click **L2 Features > VLAN > GVRP > GVRP Advertise VLAN**, as shown below:

Figure 5-13 GVRP Advertise VLAN Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Action	Select the advertised VLAN to port mapping action that will be taken here. Options to choose from are All , Add , and Remove . When selecting All , all the advertised VLANs will be used.
Advertise VID List	Enter the advertised VLAN ID list here.

Click the **Apply** button to accept the changes made.

GVRP Forbidden VLAN

On this page, users can view and configure the GVRP forbidden VLAN settings. To view the following window, click **L2 Features > VLAN > GVRP > GVRP Forbidden VLAN**, as shown below:

Port	Forbidden VLAN
eth1/0/1	
eth1/0/2	
eth1/0/3	
eth1/0/4	
eth1/0/5	
eth1/0/6	
eth1/0/7	
eth1/0/8	
eth1/0/9	
eth1/0/10	
eth1/0/11	
eth1/0/12	
eth1/0/13	
eth1/0/14	
eth1/0/15	
eth1/0/16	
eth1/0/17	
eth1/0/18	
eth1/0/19	
eth1/0/20	
eth1/0/21	

Figure 5-14 GVRP Forbidden VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Action	Select the forbidden VLAN to port mapping action that will be taken here. Options to choose from are All , Add , and Remove . When selecting All , all the forbidden VLANs will be used.
Forbidden VID List	Enter the forbidden VLAN ID list here.

Click the **Apply** button to accept the changes made.

GVRP Statistics Table

On this page, GVRP statistics information is displayed. To view the following window, click **L2 Features > VLAN > GVRP > GVRP Statistics Table**, as shown below:

Port		JoinEmpty	JoinIn	LeaveEmpty	LeaveIn	LeaveAll	Empty
eth1/0/1	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/2	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/3	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/4	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/5	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/6	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/7	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/8	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/9	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/10	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0

Figure 5-15 GVRP Statistics Table Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number of which GVRP statistic information will be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the information for the specific port.

Click the **View All** button to view all GVRP statistic information.

Click the **Clear All** button to clear all the information in this table.

MAC VLAN

On this page, users can view and configure the MAC-based VLAN information. When a static MAC-based VLAN entry is created for a user, the traffic according to the specified VLAN operating on this port will be configured. To view the following window, click **L2 Features > VLAN > MAC VLAN**, as shown below:

MAC Address	VLAN ID	Priority	Status
00-11-22-33-44-55	1	0	Active

Figure 5-16 MAC VLAN Window

The fields that can be configured are described below:

Parameter	Description
-----------	-------------

MAC Address	Enter the unicast MAC address.
VLAN ID	Enter the VLAN ID that will be used.
Priority	Select the priority that is assigned to untagged packets. This value is between 0 and 7.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

VLAN Interface

On this page, users can view and configure VLAN interface settings. To view the following window, click **L2 Features > VLAN > VLAN Interface**, as shown below:



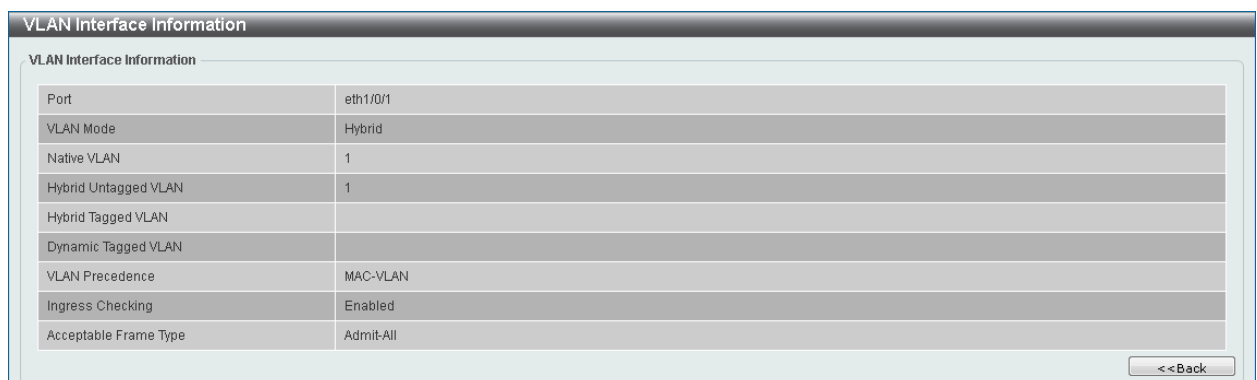
Port	VLAN Mode	Ingress Checking	Acceptable Frame Type		
eth1/0/1	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/2	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/3	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/4	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/5	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/6	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/7	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/8	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/9	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/10	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/11	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/12	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/13	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/14	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/15	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/16	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/17	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/18	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/19	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/20	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/21	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/22	Hybrid	Enabled	Admit-All	VLAN Detail	Edit
eth1/0/23	Hybrid	Enabled	Admit-All	VLAN Detail	Edit

Figure 5-17 VLAN Interface Window

Click the **View Detail** button to view more detailed information about the VLAN on the specific interface.

Click the **Edit** button to re-configure the specific entry.

After clicking the **VLAN Detail** button, the following page will appear.



VLAN Interface Information	
Port	eth1/0/1
VLAN Mode	Hybrid
Native VLAN	1
Hybrid Untagged VLAN	1
Hybrid Tagged VLAN	
Dynamic Tagged VLAN	
VLAN Precedence	MAC-VLAN
Ingress Checking	Enabled
Acceptable Frame Type	Admit-All

<<Back

Figure 5-18 VLAN Interface (VLAN Detail) Window

On this page, more detailed information about the VLAN of the specific interface is displayed. Click the <<**Back** button to return to the previous page.

After click the **Edit** button, the following page will appear. This is a dynamic page that will change when a different **VLAN Mode** was selected. When **Access** was selected as the **VLAN Mode**, the following page will appear.

Figure 5-19 VLAN Interface (Access) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access, Hybrid, Trunk, 802.1Q-Tunnel, Promiscuous, and Host .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only, Untagged Only, and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VLAN ID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.

Click the **Apply** button to accept the changes made.

Click the <<**Back** button to discard the changes made and return to the previous page.

When **Hybrid** was selected as the **VLAN Mode**, the following page will appear.

Figure 5-20 VLAN Interface (Hybrid) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are

	Access, Hybrid, Trunk, 802.1Q-Tunnel, Promiscuous, and Host.
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VLAN Precedence	Select the VLAN precedence option here. Options to choose from are Mac-based VLAN and Subnet-based VLAN .
Native VLAN	Tick this option to enable the native VLAN function.
VLAN ID	After ticking the Native VLAN option the following parameter will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select the action that will be taken here. Options to choose from are Add , Remove , Tagged , and Untagged .
Add Mode	Select whether to add an Untagged or Tagged parameters.
Allowed VLAN Range	Enter the allowed VLAN range information here.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

When **Trunk** was selected as the **VLAN Mode**, the following page will appear.

The screenshot shows the 'Configure VLAN Interface' window with the following settings:

- Port: eth1/0/1
- VLAN Mode: Trunk
- Acceptable Frame: Admit All
- Ingress Checking: Enabled Disabled
- Native VLAN: Native VLAN Untagged Tagged
- VLAN ID (1-4094): [Empty text box]
- Action: All
- Allowed VLAN Range: [Empty text box]

Buttons for '<<Back' and 'Apply' are visible at the bottom right.

Figure 5-21 VLAN Interface (Trunk) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access, Hybrid, Trunk, 802.1Q-Tunnel, Promiscuous, and Host.
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	After selecting Trunk as the VLAN Mode the following parameter will be available. Select to enable or disable the ingress checking function.
Native VLAN	Tick this option to enable the native VLAN function. Also select if this VLAN supports Untagged or Tagged frames.
VLAN ID	After ticking the Native VLAN option the following parameter will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select the action that will be taken here. Options to choose from are All , Add , Remove , Except , and Replace .
Allowed VLAN Range	Enter the allowed VLAN range information here.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

When **802.1Q-Tunnel** was selected as the **VLAN Mode**, the following page will appear.

Figure 5-22 VLAN Interface (802.1Q-Tunnel) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , 802.1Q-Tunnel , Promiscuous , and Host .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VLAN Precedence	Select the VLAN precedence option here. Options to choose from are Mac-based VLAN and Subnet-based VLAN .
VLAN ID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select the action that will be taken here. Options to choose from are Add and Remove .
Add Mode	Select to add an Untagged parameter.
Allowed VLAN Range	Enter the allowed VLAN range information here.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

When **Promiscuous** was selected as the **VLAN Mode**, the following page will appear.

Figure 5-23 VLAN Interface (Promiscuous) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , 802.1Q-Tunnel , Promiscuous , and Host .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

When **Host** was selected as the **VLAN Mode**, the following page will appear.

Figure 5-24 VLAN Interface (Host) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , 802.1Q-Tunnel , Promiscuous , and Host .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Subnet VLAN

On this page, users can view and configure the subnet VLAN settings. A subnet VLAN entry is an IP subnet-based VLAN classification rule. If an untagged or priority-tagged IP packet is received on a port, its source IP address will be used to match the subnet VLAN entries. If the source IP is in the subnet of an entry, the packet will be classified to the VLAN defined for this subnet. To view the following window, click **L2 Features > VLAN > Subnet VLAN**, as shown below:

Figure 5-25 Subnet VLAN Window

The fields that can be configured are described below:

Parameter	Description
IPv4 Network Prefix / Prefix Length	Select and enter the IPv4 address and prefix length value for the subnet VLAN here.
IPv6 Network Prefix / Prefix Length	Select and enter the IPv6 address and prefix length value for the subnet VLAN here.
VLAN ID	Enter the VLAN ID for the subnet VLAN here.
Priority	Select the priority value used here. This value is between 0 and 7. A lower value takes higher priority.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Private VLAN

On this page, users can view and configure the private VLAN settings. To view the following window, click **L2 Features > VLAN > Private VLAN**, as shown below:

Figure 5-26 Private VLAN Window

The fields that can be configured for **Private VLAN** are described below:

Parameter	Description
VLAN ID List	Enter the private VLAN ID list here.
State	Select to enable or disable the private VLAN state here.
Type	Select the type of private VLAN that will be created here. Options to choose from are Community , Isolated , and Primary .

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Private VLAN Association** are described below:

Parameter	Description
VLAN ID List	Enter the private VLAN ID list here.
Action	Select the action that will be taken for the private VLAN here. Options

	to choose from are Add , Remove , and Disabled .
Secondary VLAN ID List	Enter the secondary private VLAN ID here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Private VLAN Host Association** are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Primary VLAN ID	Enter the primary private VLAN ID here.
Secondary VLAN ID	Enter the secondary private VLAN ID here. When ticking the Remove Association option, specifies that this configuration will not be enabled.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Private VLAN Mapping** are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Primary VLAN ID	Enter the primary private VLAN ID here.
Action	Select the action that will be taken for the private VLAN here. Options to choose from are Add , Remove , and Disabled .
Secondary VLAN ID List	Enter the secondary private VLAN ID here. When ticking the Remove Mapping option, specifies that this configuration will not be enabled.

Click the **Apply** button to accept the changes made.

Spanning Tree

STP Global Settings

On this page, users can view and configure the STP global settings. To view the following window, click **L2 Features > Spanning Tree > STP Global Settings**, as shown below:

Spanning Tree Global Settings

Spanning Tree State
Spanning Tree State: Disabled Enabled Apply

STP Traps
STP New Root Trap: Disabled Enabled
STP Topology Change Trap: Disabled Enabled Apply

Spanning Tree Mode
Spanning Tree Mode: RSTP Apply

Spanning Tree Priority
Priority (0-61440): 32768 Apply

Spanning Tree Configuration
Bridge Max Age (6-40): 20 sec Bridge Hello Time (1-2): 2 sec
Bridge Forward Time (4-30): 15 sec TX Hold Count (1-10): 6 times
Max Hops (1-40): 20 times NNI BPDU Address: Dot1d Apply

Figure 5-27 STP Global Settings Window

The field that can be configured for **Spanning Tree State** is described below:

Parameter	Description
Spanning Tree State	Select to enable or disable the STP global state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **STP Traps** are described below:

Parameter	Description
STP New Root Trap	Select to enable or disable the STP new root trap option here.
STP Topology Change Trap	Select to enable or disable the STP topology change trap option here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Spanning Tree Mode** are described below:

Parameter	Description
Spanning Tree Mode	Select the STP mode used here. Options to choose from are MSTP , RSTP , and STP .

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Spanning Tree Priority** are described below:

Parameter	Description
Priority	Select the STP priority value here. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Spanning Tree Configuration** are described below:

Parameter	Description
Spanning Tree Mode	Select the STP mode used here. Options to choose from are MSTP , RSTP , and STP .
Priority	Select the STP priority value here. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.
Bridge Max Age	Enter the bridge's maximum age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The maximum age value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the switch has spanning tree configuration values consistent with other devices on the bridged LAN.
Bridge Hello Time	After selecting RSTP/STP as the Spanning Tree Mode , this parameter will be available. Enter the bridge's hello time value here. This value must be between 1 and 2 seconds. By default, this value is

	2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port per port basis.
Bridge Forward Time	Enter the bridge's forwarding time value here. This value must be between 4 and 30 seconds. By default, this value is 15 seconds. Any port on the switch spends this time in the listening state while moving from the blocking state to the forwarding state.
TX Hold Count	Enter the transmit hold count value here. This value must be between 1 and 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.
Max Hops	Enter the maximum number of hops that are allowed. This value must be between 1 and 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The switch will then discard the BPDU packet and the information held for the port will age out.
NNI BPDU Address	Select the NNI BPDU Address option here. Options to choose from are Dot1d and Dot1ad . By default, this option is Dot1d . This parameter is used to determine the BPDU protocol address for STP in the service provide site. It can use an 802.1d STP address, 802.1ad service provider STP address, or a user defined multicast address.

Click the **Apply** button to accept the changes made.

STP Port Settings

On this page, users can view and configure the STP port settings. To view the following window, click **L2 Features > Spanning Tree > STP Port Settings**, as shown below:

The screenshot shows the 'STP Port Settings' window. At the top, there are configuration fields for 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Cost' (0/2000000, 0=Auto), 'Link Type' (Auto), 'BPDU Forward' (Disabled), 'State' (Enabled), 'Port Fast' (Network), 'Priority' (128), 'Guard Root' (Disabled), 'TCN Filter' (Disabled), and 'Hello Time (1-2)' (with an 'Apply' button). Below these fields is a table with the following data:

Port	State	Cost	Guard Root	Link Type	Port Fast	TCN Filter	BPDU Forward	Priority
eth1/0/1	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/2	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/3	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/4	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/5	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/6	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/7	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/8	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/9	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/10	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/11	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/12	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/13	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/14	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/15	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/16	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/17	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128
eth1/0/18	Enabled	0/200000	Disabled	auto/p2p	auto/non-edge	Disabled	Disabled	128

Figure 5-28 STP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Cost	Enter the cost value here. This value must be between 1 and 200000000. This value defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is 200000, a Gigabit port is 20000, and a 10 Gigabit port is 2000. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.
Guard Root	Select to enable or disable the guard root function.
Link Type	Select the link type option here. Options to choose from are Auto , P2P , and Shared . A full-duplex port is considered to have a point-to-point (P2P) connection. On the opposite, a half-duplex port is considered to have a Shared connection. The port cannot transit into the forwarding state rapidly by setting the link type to Shared . By default this option is Auto .
Port Fast	Select the port fast option here. Options to choose from are Network , Disabled , and Edge . In the Network mode the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. In the Disable mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. In the Edge mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. By default, this option is Network .
TCN Filter	Select to enable or disable the TCN filter option. Enabling TC filtering on a port is useful for an ISP to prevent the external bridge to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is Disabled .
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is Disabled .
Priority	Select the priority value here. Options to choose from are 0 to 240 . By default this option is 0 . A lower value has higher priority.
Hello Time	Enter the hello time value here. This value must be between 1 and 2 seconds. This value specifies the interval that a designated port will wait between the periodic transmissions of each configuration message.

Click the **Apply** button to accept the changes made.

MST Configuration Identification

On this page, users can view and configure the MST configuration identification settings. These settings will uniquely identify a multiple spanning tree instance set on the switch. The switch initially possesses one CIST, or Common Internal Spanning Tree, of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted. To view the following window, click **L2 Features > Spanning Tree > MST Configuration Identification**, as shown below:

Figure 5-29 MST Configuration Identification Window

The fields that can be configured for **MST Configuration Settings** are described below:

Parameter	Description
Configuration Name	Enter the MST. This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). If a Configuration Name is not set, this field will show the MAC address to the device running MSTP.
Revision Level	Enter the revision level value here. This value must be between 0 and 65535 . By default, this value is 0 . This value, along with the Configuration Name, identifies the MSTP region configured on the switch.

Click the **Apply** button to accept the changes made.

In the **Private VLAN Synchronize** section, the user can click the **Apply** button to synchronize the private VLANs.

The fields that can be configured for **Instance ID Settings** are described below:

Parameter	Description
Instance ID	Enter the instance ID here. This value must be between 1 and 4094 .
Action	Select the action that will be taken here. Options to choose from are Add VID and Remove VID .
VID List	Enter the VID list value here. This field is used to specify the VID range from configured VLANs set on the switch.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

STP Instance

On this page, users can view and configure the STP instance settings. To view the following window, click **L2 Features > Spanning Tree > STP Instance**, as shown below:

Instance	Instance State	Instance Priority
CIST	Disabled	32768(32768 sysid 0)

CIST Global Info[Mode RSTP]	
Bridge Address	00-17-9A-14-6B-10
Designated Root Address / Priority	00-00-00-00-00-00 / 0
Regional Root Bridge Address / Priority	00-00-00-00-00-00 / 0
Designated Bridge Address / Priority	00-00-00-00-00-00 / 0

Figure 5-30 STP Instance Window

Click the **Edit** button to re-configure the specific entry.

MSTP Port Information

On this page, users can view and configure the MSTP port information settings. To view the following window, click **L2 Features > Spanning Tree > MSTP Port Information**, as shown below:

Instance ID	Cost	Priority	Status	Role
CIST	200000	128	Forwarding	NonStp

Figure 5-31 MSTP Port Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number that will be cleared here.

Click the **Clear Detected Protocol** button to clear the detected protocol settings for the port selected.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The switch supports up to 16 port trunk groups with 1 to 12 ports in each group.

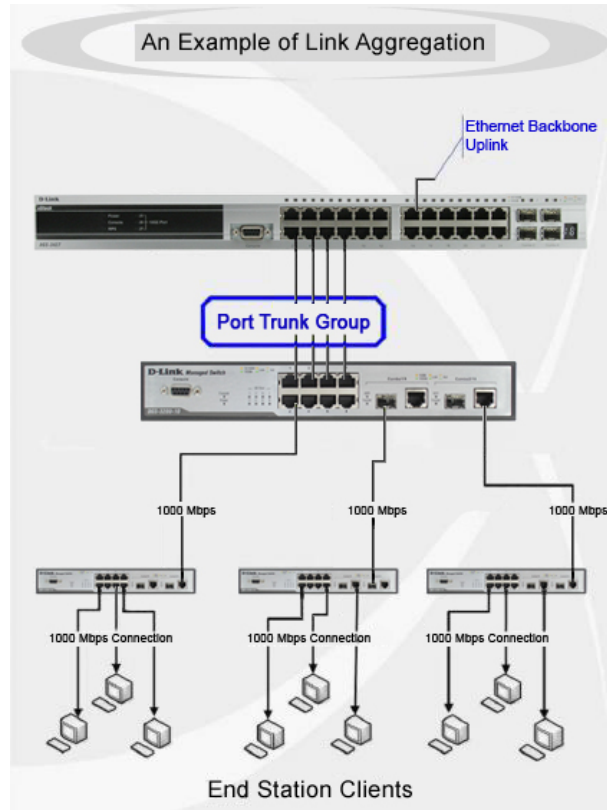


Figure 5-32 Example of Port Trunk Group

The switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The switch allows the creation of up to 16 link aggregation groups, each group consisting of 1 to 12 links (ports). Each port can only belong to a single link aggregation group.

All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking and 802.1X must not be enabled on the trunk group. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are

configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

On this page, users can view and configure the link aggregation settings. To view the following window, click **L2 Features > Link Aggregation**, as shown below:

Figure 5-33 Link Aggregation Window

The fields that can be configured for **Link Aggregation** are described below:

Parameter	Description
System Priority	Enter the system's priority value used here. This value must be between 1 and 65535 . By default, this value is 32768 . The system priority determines which ports can join a port-channel and which ports are put in the stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority
Load Balance Algorithm	Select the load balancing algorithm that will be used here. Options to choose from are Source MAC , Destination MAC , Source Destination MAC , Source IP , Destination IP , Source Destination IP , Source L4 Port , Destination L4 Port , and Source Destination L4 Port . By default, this option is Source Destination MAC .

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Trunking Information** are described below:

Parameter	Description
From Port ~ To Port	Select the list of ports that will be associated with this configuration here.
Channel Group	Enter the channel group number here. This value must be between 1 and 16 . The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are On , Active , and Passive . If the mode On is specified, the channel group type is static. If the mode Active or Passive is specified, the channel group type is LACP. A channel group can only consist of either static

members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Click the **Channel Detail** button to view more detailed information about the channel.

After clicking the **Channel Detail** button, the following page will be available.

Channel Group

Channel Group Information

Channel Group: 1
Protocol: Static

Channel Group Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
eth1/0/10	N/A	N/A	down	N/A	N/A	Edit
eth1/0/11	N/A	N/A	down	N/A	N/A	Edit
eth1/0/12	N/A	N/A	down	N/A	N/A	Edit
eth1/0/13	N/A	N/A	down	N/A	N/A	Edit
eth1/0/14	N/A	N/A	down	N/A	N/A	Edit
eth1/0/15	N/A	N/A	down	N/A	N/A	Edit
eth1/0/16	N/A	N/A	down	N/A	N/A	Edit

Channel Group Neighbor Information

Port	Partner System ID	Partner PortNo	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
eth1/0/10	N/A	N/A	N/A	N/A	N/A
eth1/0/11	N/A	N/A	N/A	N/A	N/A
eth1/0/12	N/A	N/A	N/A	N/A	N/A
eth1/0/13	N/A	N/A	N/A	N/A	N/A
eth1/0/14	N/A	N/A	N/A	N/A	N/A
eth1/0/15	N/A	N/A	N/A	N/A	N/A
eth1/0/16	N/A	N/A	N/A	N/A	N/A

Note:
LACP State:
bncl: Port is attached to an aggregator and bundled with other ports.

<<Back

Figure 5-34 Link Aggregation (Channel Detail) Window

Click the **Edit** button to re-configure the specific entry.

Click the **<<Back** button to return to the previous page.

L2 Protocol Tunnel

On this page, users can view and configure the Layer 2 protocol tunnel settings. To view the following window, click **L2 Features > L2 Protocol Tunnel**, as shown below:

L2 Protocol Tunnel

L2 Protocol Tunnel Global Setting | L2 Protocol Tunnel Port Setting

CoS for Encapsulated Packets: 0 Default

Drop Threshold (100-20000): 0 Default

Apply

Protocol	Drop Counter
GVRP	0
STP	0
01-00-0C-CC-CC-CC	0
01-00-0C-CC-CC-CD	0

Figure 5-35 L2 Protocol Tunnel (L2 Protocol Tunnel Global Setting) Window

The fields that can be configured for **L2 Protocol Tunnel Global Settings** are described below:

Parameter	Description
CoS for Encapsulated Packets	Select the CoS value for encapsulated packets here. This value is between 0 and 7 . Tick the Default option to use the default value.
Drop Threshold	Enter the drop threshold value here. This value must be between 100 and 2000 . By default, this value is 0 . The tunneling of the Layer 2 protocol packets will consume CPU processing power in encapsulating, decapsulating, and forwarding of the packet. Use this option to restrict the CPU processing bandwidth consumed by specifying a threshold on the number of all Layer 2 protocol packets that can be processed by the system. When the maximum number of packets is exceeded, the excessive protocol packets are dropped.

Click the **Apply** button to accept the changes made.

After selecting the **L2 Protocol Tunnel Port Setting** tab option, at the top of the page, the following page will be available.

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
eth1/0/11	gvrp	-	-	0	0	0

Figure 5-36 L2 Protocol Tunnel (L2 Protocol Tunnel Port Setting) Window

The fields that can be configured for **L2 Protocol Tunnel Port Setting** are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type option here. Options to choose from are None , Shutdown , and Drop .
Tunneled Protocol	Select the tunneled protocol option here. Options to choose from are GVRP , STP , Protocol MAC , and All .
Protocol MAC	After selecting the Protocol MAC option as the Tunneled Protocol , the following option will be available. Select the protocol MAC option here. Options to choose from are 01-00-0C-CC-CC-CC and 01-00-0C-CC-CC-CD .
Threshold	After selecting the Shutdown or Drop options as the Type , the following parameter will be available. Enter the threshold value here. This value must be between 1 and 4096 .

Click the **Apply** button to accept the changes made.

Click the **Clear All** button to clear all the counter information.

Click the **Clear** button to clear all the counter information of the specific entry.

L2 Multicast Control

Multicast Filtering

On this page, users can view and configure the Layer 2 multicast filtering settings. To view the following window, click **L2 Features > L2 Multicast Control > Multicast Filtering**, as shown below:

Figure 5-37 Multicast Filtering Window

The fields that can be configured are described below:

Parameter	Description
VLAN ID List	Enter the VLAN ID list that will be used for this configuration here.
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are Forward Unregistered , Forward All , and Filter Unregistered . When selecting the Forward Unregistered option, registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. When selecting the Forward All option, all multicast packets will be flooded based on the VLAN domain. When selecting the Filter Unregistered option, registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

Click the **Apply** button to accept the changes made.

6. Layer 3 Features

ARP
Gratuitous ARP
IPv4 Interface
IPv4 Static/Default Route
IPv4 Route Table
IPv6 Interface
IPv6 Static/Default Route
IPv6 Route Table

ARP

ARP Aging Time

On this page, users can view and configure the ARP aging time settings. To view the following window, click **L3 Features > ARP > ARP Aging Time**, as shown below:

Interface Name	Timeout (min)
vlan1	240

Figure 6-1 ARP Aging Time Window

The fields that can be configured are described below:

Parameter	Description
Timeout	After click the Edit button, enter the ARP aging timeout value here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Static ARP

On this page, users can view and configure the static ARP settings. To view the following window, click **L3 Features > ARP > Static ARP**, as shown below:

VRF Name	Interface Name	IP Address	Hardware Address	Age	Type
vlan1	vlan1	10.90.90.90	00-17-9A-14-23-D0	forever	

Figure 6-2 Static ARP Window

The fields that can be configured are described below:

Parameter	Description
VRF Name	Enter the Virtual Routing and Forwarding (VRF) instance name used here. This name can be up to 12 characters long.
IP Address	Enter the IP address that will be associated with the MAC address here.
Hardware Address	Enter the MAC address that will be associated with the IP address here.

Click the **Apply** button to accept the changes made.

Click the **Find** button to find the entry, based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Proxy ARP

On this page, users can view and configure the proxy ARP settings. The Proxy ARP feature of the switch will allow the switch to reply to ARP requests destined for another device by faking its identity (IP and MAC Address) as the original ARP responder. Therefore, the switch can then route packets to the intended destination without configuring static routing or a default gateway. The host, usually a Layer 3 switch, will respond to packets for another device. To view the following window, click **L3 Features > ARP > Proxy ARP**, as shown below:

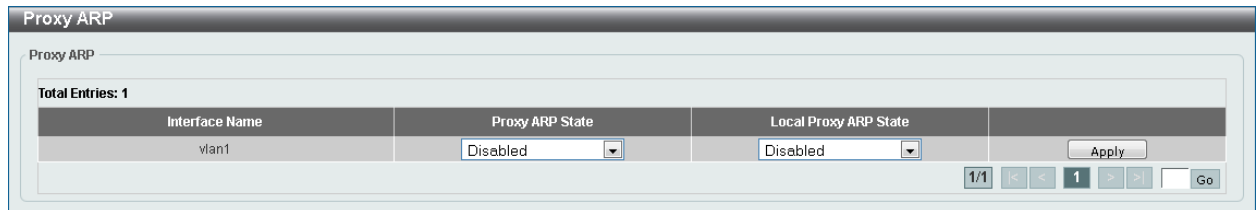


Figure 6-3 Proxy ARP Window

The fields that can be configured are described below:

Parameter	Description
Proxy ARP State	Select to enable or disable the proxy ARP state here.
Local Proxy ARP State	Select to enable or disable the local proxy ARP state here. This local proxy ARP function allows the switch to respond to the proxy ARP, if the source IP and destination IP are in the same interface.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

ARP Table

On this page, users can view and configure the ARP table settings. To view the following window, click **L3 Features > ARP > ARP Table**, as shown below:

ARP Table

ARP Search

VRF Name: 12 chars

Interface VLAN (1-4094):

Hardware Address: 00-11-22-33-44-55-FF

IP Address: . . .

MASK Address: . . .

Type: All

Mgmt:

Find

Total Entries: 2

Interface Name	IP Address	MAC Address	Age (min)	Type
vlan1	10.90.90.6	10-BF-48-D6-E2-E2	240	
vlan1	10.90.90.90	00-17-9A-14-6B-10	forever	

Clear All

Delete

Delete

1/1 < > 1 Go

Figure 6-4 ARP Table Window

The fields that can be configured are described below:

Parameter	Description
VRF Name	Enter the Virtual Routing and Forwarding (VRF) instance name used here. This name can be up to 12 characters long.
Interface VLAN	Enter the interface's VLAN ID used here. This value must be between 1 and 4094 .
IP Address	Select and enter the IP address to display here.
MASK Address	After the IP Address option was selected, enter the mask address for the IP address here.
Hardware Address	Select and enter the MAC address to display here.
Type	Select the type option here. Options to choose from are All and Dynamic .
Mgmt	Select this option to display the Management port's information.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear All** button to clear all the information.

Click the **Delete** button to remove the specific entry.

Gratuitous ARP

On this page, users can view and configure the gratuitous ARP settings. A gratuitous ARP request packet is an ARP request packet where the source and the destination IP address are both set to the IP address of the sending device and the destination MAC address is the broadcast address.

Generally, a device use the gratuitous ARP request packet to discover whether the IP address is duplicated by other hosts or to preload or reconfigure the ARP cache entry of hosts connected to the interface. To view the following window, click **L3 Features > Gratuitous ARP**, as shown below:

Gratuitous ARP

Gratuitous ARP Global Settings

IP Gratuitous ARP State: Enabled Disabled

IP Gratuitous ARP Dad-Reply State: Enabled Disabled

Gratuitous ARP Learning State: Enabled Disabled

Apply

Gratuitous ARP Send Interval

Total Entries: 1

Interface Name	Interval Time (sec)
vlan1	0

Edit

1/1 < > 1 Go

Figure 6-5 Gratuitous ARP Window

The fields that can be configured are described below:

Parameter	Description
IP Gratuitous ARP State	Select to enable or disable the learning of gratuitous ARP packets in the ARP cache table.
IP Gratuitous ARP Dad-Reply State	Select to enable or disable the IP gratuitous ARP Dad-reply state.
Gratuitous ARP Learning State	Select to enable or disable the gratuitous ARP learning state. Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. This option used to enable or disable the learning of ARP entries in the ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

IPv4 Interface

On this page, users can view and configure the IPv4 interface settings. To view the following window, click **L3 Features > IPv4 Interface**, as shown below:

Interface	State	IP Address	Mask	Secondary	Link Status
vlan1	Enabled	10.90.90.90	255.0.0.0	No	Up

Figure 6-6 IPv4 Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface's VLAN ID here. This value must be between 1 and 4094 .

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Edit** button, the following page will be available.

Figure 6-7 IPv4 Interface (Edit) Window

The fields that can be configured are described below:

Parameter	Description
State	Select to enable or disable the IPv4 interface's global state.
Get IP From	Select the get IP from option here. Options to choose from are Static and DHCP . When the Static option is selected, users can enter the IPv4 address of this interface manually in the fields provided. When the DHCP option is selected, this interface will obtain IPv4 information automatically from the DHCP server located on the local network.
IP Address	Enter the IPv4 address for this interface here.
Mask	Enter the IPv6 subnet mask for this interface here.
Secondary	Tick this option to use the IPv4 address and mask as the secondary interface configuration.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

IPv4 Static/Default Route

On this page, users can view and configure the IPv4 static and default route settings. The switch supports static routing for IPv4 formatted addressing. Users can create up to 1000 static route entries for IPv4. For IPv4 static routes, once a static route has been set, the switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP request will not be sent.

The switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become active.

Entries into the switch's forwarding table can be made using both an IP address subnet mask and a gateway. To view the following window, click **L3 Features > IPv4 Static/Default Route**, as shown below:

Figure 6-8 IPv4 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
VRF Name	Enter the VRF instance name used here. This name can be up to 12 characters long.
IP Address	Enter the IPv4 address for this route here. Tick the Default Route option to use the default route as the IPv4 address.
Netmask	Enter the IPv4 network mask for this route here.
Gateway	Enter the gateway address for this route here.
Backup State	Select the backup state option here. Options to choose from are Primary , Backup , and Weight . When the Primary option is selected, the route will be used as the primary route to the destination. When the Backup option is selected, the route will be used as the backup route to the destination. When the Weight option is selected, the weight number must be entered with value greater than zero, but less than the maximum paths number. This number is used to replicate identical route path (multiple copies) in routing table, so the path get more chance to be hit for traffic routing. If weight number is not specified for the static route, the default for the path that exists in the hashing table is one copy. This value must be between 1 and 32 .

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

IPv4 Route Table

On this page, users can view and configure the IPv4 route table settings. To view the following window, click **L3 Features > IPv4 Route Table**, as shown below:

Figure 6-9 IPv4 Route Table Window

The fields that can be configured are described below:

Parameter	Description
Network Address	Enter the IPv4 network address here. In the first space enter the network prefix and in the second space enter the network mask.
IP Address	Enter the single IPv4 address here.
RIP	Select this option to display only RIP routes.
OSPF	Select this option to display only OSPF routes.
BGP	Select this option to display only BGP routes.
Connected	Select this option to display only connected routes.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.

Click the **Find** button to locate a specific entry based on the information entered.

IPv6 Interface

On this page, users can view and configure the IPv6 interface's settings.

To view the following window, click **L3 Features > IPv6 Interface**, as shown below:



Figure 6-10 IPv6 Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface's ID that will be associated with the IPv6 entry.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Detail** button to view and configure more detailed settings for the IPv6 interface entry.

After clicking the **Detail** button, the following page will be available.

Figure 6-11 IPv6 Interface (Detail, IPv6 Interface Settings) Window

The fields that can be configured for **Interface** are described below:

Parameter	Description
IPv6 State	Select to enable or disable the IPv6 interface's global state here.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Static IPv6 Address Settings** are described below:

Parameter	Description
IPv6 Address	Enter the IPv6 address for this IPv6 interface here. Select the EUI-64 option to configure an IPv6 address on the interface using the EUI-64 interface ID. Select the Link Local option to configure a link-local address for the IPv6 interface.

Click the **Apply** button to accept the changes made.

After selecting the **Interface Address** tab option, at the top of the page, the following page will be available.

Figure 6-12 IPv6 Interface (Detail, Interface Address) Window

Click the **Delete** button to delete the specified entry.

IPv6 Static/Default Route

On this page, users can view and configure the IPv6 static or default routes. To view the following window, click **L3 Features > IPv6 Static/Default Route**, as shown below:

Figure 6-13 IPv6 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
Network Prefix/Prefix Length	Enter the IPv6 address and prefix length for this route here. Tick the Default Route option to use the default route as the IPv6 address.
Interface VLAN	Enter the interface's VLAN ID that will be associated with this route here.
Next Hop IPv6 Address	Enter the next hop IPv6 address here.
Backup State	Select the backup state option here. Options to choose from are Primary , Backup , and Distance . When the Primary option is selected, the route is specified as the primary route to the destination. When the Backup option is selected, the route is specified as the backup route to the destination. When the Distance option is selected, enter the administrative distance of the static route in the space provided. This value must be between 1 and 255 . A lower value represents a better route. If not specified, the default administrative distance for a static route is 1 .

Click the **Apply** button to accept the changes made.

IPv6 Route Table

On this page, users can view and configure the IPv6 route table. To view the following window, click **L3 Features > IPv6 Route Table**, as shown below:

Figure 6-14 IPv6 Route Table Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	Enter the IPv6 address and prefix length to display here. Select the Longer Prefixes option to display the route and all of the more

	specific routes.
IPv6 Address	Enter the IPv6 address to display here.
Interface VLAN	Enter the interface's VLAN ID to display here.
RIPng	Select this option to display only RIPng routes.
OSPFv3	Select this option to display only OSPFv3 routes.
Database	Select this option to display all the related entries in the routing database instead of just the best route.
Connected	Select this option to display only connected routes.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.

Click the **Find** button to locate a specific entry based on the information entered.

7. Quality of Service (QoS)

Basic Settings
Advanced Settings

Basic Settings

Port Default CoS

On this page, users can view and configure the port's default CoS settings. To view the following window, click **QoS > Basic Settings > Port Default CoS**, as shown below:

Port	Default CoS	Override
eth1/0/1	0	No
eth1/0/2	0	No
eth1/0/3	0	No
eth1/0/4	0	No
eth1/0/5	0	No
eth1/0/6	0	No
eth1/0/7	0	No
eth1/0/8	0	No
eth1/0/9	0	No
eth1/0/10	0	No
eth1/0/11	0	No
eth1/0/12	0	No
eth1/0/13	0	No
eth1/0/14	0	No
eth1/0/15	0	No
eth1/0/16	0	No
eth1/0/17	0	No
eth1/0/18	0	No
eth1/0/19	0	No
eth1/0/20	0	No

Figure 7-1 Port Default CoS Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are 0 to 7 . Select the Override option to override the CoS of the packets. The default CoS will be applied to all incoming packets, tagged or untagged, received by the port. Select the None option to specify that the CoS of the packets will be the packet's CoS if the packets are tagged, and will be the port default CoS if the packet is untagged.

Click the **Apply** button to accept the changes made.

Port Scheduler Method

On this page, users can view and configure the port scheduler method settings. To view the following window, click **QoS > Basic Settings > Port Scheduler Method**, as shown below:

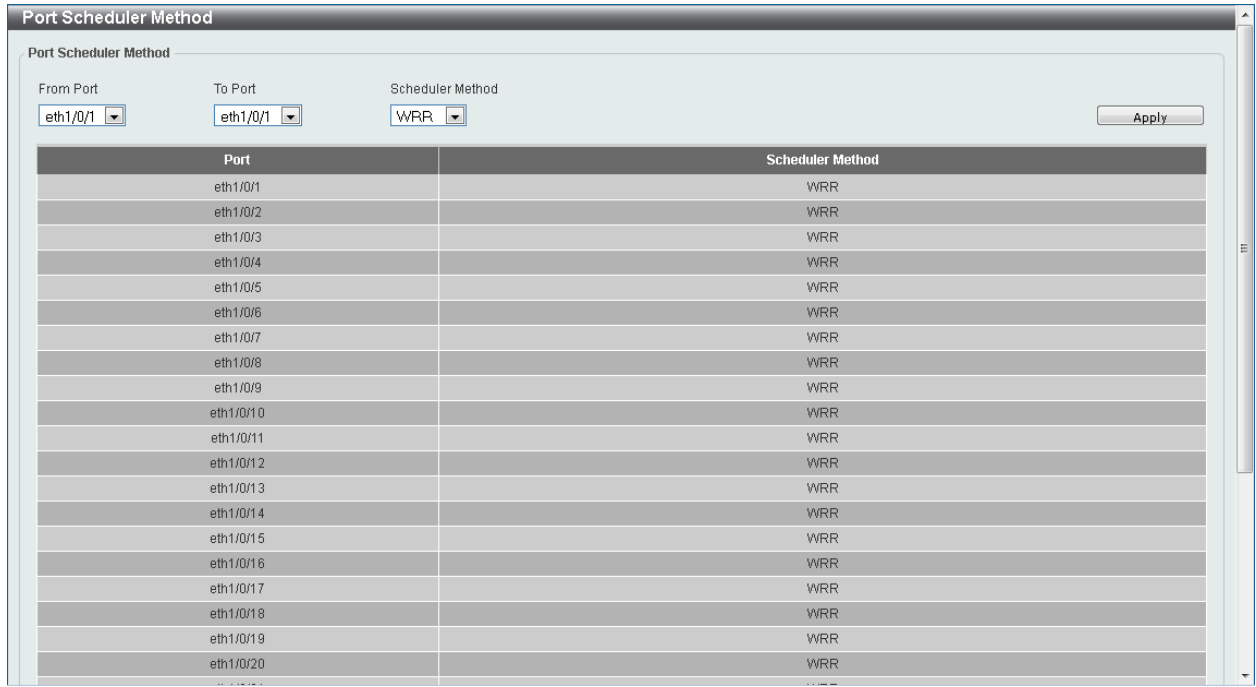


Figure 7-2 Port Scheduler Method Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Scheduler Method	<p>Select the scheduler method that will be applied to the specified port(s). Options to choose from are Strict Priority (SP), Round-Robin (RR), Weighted Round-Robin (WRR), Weighted Deficit Round-Robin (WDRR), and Enhanced Transmission Selection (ETS). By default, the output queue scheduling algorithm is WRR.</p> <p>Strict Priority (SP) specifies that all queues use strict priority scheduling. It provides strict priority access to the queues from the highest CoS queue to the lowest.</p> <p>Round-Robin (RR) specifies that all queues use round-robin scheduling. It provides fair access to service a single packet at each queue before moving on to the next one.</p> <p>Weighted Round-Robin (WRR) operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1 and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time.</p> <p>Weighted Deficit Round-Robin (WDRR) operates by serving an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time. All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this</p>

condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration.

To set a CoS queue in the **SP** mode, any higher priority CoS queue must also be in the strict priority mode.

Enhanced Transmission Selection (**ETS**) provides bandwidth allocation on converged links in end stations and bridges in a Data Center Bridging (DCB) environment. Using bandwidth allocations, different traffic classes within different traffic types such as LAN, SAN, IPC and management can be configured to provide bandwidth allocation, low-latency or best effort transmit characteristics.

Click the **Apply** button to accept the changes made.

Queue Settings

On this page, users can view and configure the queue settings. To view the following window, click **QoS > Basic Settings > Queue Settings**, as shown below:

Port	Queue ID	WRR Weight	WDRR Quantum
eth1/0/1	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	1	1
eth1/0/2	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	1	1
eth1/0/3	0	1	1
	1	1	1
	2	1	1
	3	1	1

Figure 7-3 Queue Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Queue ID	Enter the queue ID value here. This value must be between 0 and 7 .
WRR Weight	Enter the WRR weight value here. This value must be between 0 and 127 . To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. So the weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. This value must be between 0

and **127**.

Click the **Apply** button to accept the changes made.

CoS to Queue Mapping

On this page, users can view and configure the CoS-to-Queue mapping settings. To view the following window, click **QoS > Basic Settings > CoS to Queue Mapping**, as shown below:

CoS	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Figure 7-4 CoS to Queue Mapping Window

The fields that can be configured are described below:

Parameter	Description
Queue ID	Select the queue ID that will be mapped to the corresponding CoS value. Options to choose from are 0 to 7 .

Click the **Apply** button to accept the changes made.

Port Rate Limiting

On this page, users can view and configure the port rate limiting settings. To view the following window, click **QoS > Basic Settings > Port Rate Limiting**, as shown below:

Port Rate Limiting

From Port: eth1/0/1 To Port: eth1/0/1 Direction: Input

Rate Limit: Bandwidth (8-10000000) kbps Percent (1-100) % None

Burst Size (0-128000) kbyte kbyte

Port	Input		Output	
	Rate	Burst	Rate	Burst
eth1/0/1	No Limit	No Limit	No Limit	No Limit
eth1/0/2	No Limit	No Limit	No Limit	No Limit
eth1/0/3	No Limit	No Limit	No Limit	No Limit
eth1/0/4	No Limit	No Limit	No Limit	No Limit
eth1/0/5	No Limit	No Limit	No Limit	No Limit
eth1/0/6	No Limit	No Limit	No Limit	No Limit
eth1/0/7	No Limit	No Limit	No Limit	No Limit
eth1/0/8	No Limit	No Limit	No Limit	No Limit
eth1/0/9	No Limit	No Limit	No Limit	No Limit
eth1/0/10	No Limit	No Limit	No Limit	No Limit
eth1/0/11	No Limit	No Limit	No Limit	No Limit
eth1/0/12	No Limit	No Limit	No Limit	No Limit
eth1/0/13	No Limit	No Limit	No Limit	No Limit
eth1/0/14	No Limit	No Limit	No Limit	No Limit
eth1/0/15	No Limit	No Limit	No Limit	No Limit
eth1/0/16	No Limit	No Limit	No Limit	No Limit
eth1/0/17	No Limit	No Limit	No Limit	No Limit
eth1/0/18	No Limit	No Limit	No Limit	No Limit

Figure 7-5 Port Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. Options to choose from are Input and Output . When Input is selected, the rate limit for ingress packets is configured. When Output is selected, the rate limit for egress packets is configured.
Rate Limit	<p>Select and enter the rate limit value here.</p> <p>When Bandwidth is selected, enter the input/output bandwidth value used in the space provided. This value must be between 8 and 10000000 kbps. Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes.</p> <p>When Percent is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes.</p> <p>Select the None option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress will send a pause frame or a flow control frame when the received traffic exceeds the limitation.</p>

Click the **Apply** button to accept the changes made.

Queue Rate Limiting

On this page, users can view and configure the queue rate limiting settings. To view the following window, click **QoS > Basic Settings > Queue Rate Limiting**, as shown below:

Port	Queue0		Queue1		Queue2		Queue3		Queue4		Queue5		Queue6		Queue7	
	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate
eth1/0/1	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/2	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/3	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/4	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/5	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/6	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/7	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/8	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/9	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/10	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/11	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/12	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/13	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/14	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/15	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/16	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...

Figure 7-6 Queue Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Queue ID	Select the queue ID that will be configured here. Options to choose from are 0 to 7 .
Rate Limit	<p>Select and enter the queue rate limit settings here.</p> <p>When the Min Bandwidth option is selected, enter the minimum bandwidth rate limit value in the space provided. This value must be between 8 and 1000000 kbps. Also enter the maximum bandwidth (Max Bandwidth) rate limit in the space provided. This value must be between 8 and 1000000 kbps.</p> <p>When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available.</p> <p>When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied.</p> <p>The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum guaranteed bandwidth of one CoS cannot be used across physical ports.</p> <p>When the Min Percent option is selected, enter the minimum bandwidth percentage value in the space provided. This value must be between 1 and 100 percent (%). Also enter the maximum percentage value (Max Percent) in the space provided. This value must be between 1 and 100 percent (%).</p>

Click the **Apply** button to accept the changes made.

Advanced Settings

DSCP Mutation Map

On this page, users can view and configure the Differentiated Services Code Point (DSCP) mutation map settings. When a packet is received by an interface, based on a DSCP mutation map, the incoming DSCP can be mutated to another DSCP immediately before any QoS operations. The DSCP mutation is helpful to integrate domains with different DSCP assignments. The DSCP-CoS map and DSCP-color map will still be based on the packet's original DSCP. All the subsequent operations will base on the mutated DSCP. To view the following window, click **QoS > Advanced Settings > DSCP Mutation Map**, as shown below:

DSCP Mutation Map

DSCP Mutation Map

Mutation Name: Input DSCP List (0-63): Output DSCP (0-63):

Mutation Name	Digit in tens	Digit in ones										
		0	1	2	3	4	5	6	7	8	9	
Mutation1	00	0	1	2	3	4	5	6	7	8	9	<input type="button" value="Delete"/>
	10	10	11	12	13	14	15	16	17	18	19	
	20	20	21	22	23	24	25	26	27	28	29	
	30	30	31	32	33	34	35	36	37	38	39	
	40	40	41	42	43	44	45	46	47	48	49	
	50	50	51	52	53	54	55	56	57	58	59	
	60	60	61	62	63							

Figure 7-7 DSCP Mutation Map Window

The fields that can be configured are described below:

Parameter	Description
Mutation Name	Enter the DSCP mutation map name here. This name can be up to 32 characters long.
Input DSCP List	Enter the input DSCP list value here. This value must be between 0 and 63 .
Output DSCP List	Enter the output DSCP list value here. This value must be between 0 and 63 .

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Port Trust State and Mutation Binding

On this page, users can view and configure port trust state and mutation binding settings. To view the following window, click **QoS > Advanced Settings > Port Trust State and Mutation Binding**, as shown below:

Port Trust State and Mutation Binding

Port Trust State and Mutation Binding

From Port: To Port: Trust State: DSCP Mutation Map: 32 chars None

Port	Trust State	DSCP Mutation Map
eth1/0/1	trust CoS	
eth1/0/2	trust CoS	
eth1/0/3	trust CoS	
eth1/0/4	trust CoS	
eth1/0/5	trust CoS	
eth1/0/6	trust CoS	
eth1/0/7	trust CoS	
eth1/0/8	trust CoS	
eth1/0/9	trust CoS	
eth1/0/10	trust CoS	
eth1/0/11	trust CoS	
eth1/0/12	trust CoS	
eth1/0/13	trust CoS	
eth1/0/14	trust CoS	
eth1/0/15	trust CoS	
eth1/0/16	trust CoS	
eth1/0/17	trust CoS	
eth1/0/18	trust CoS	
eth1/0/19	trust CoS	
eth1/0/20	trust CoS	

Figure 7-8 Port Trust State and Mutation Binding Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Trust State	Select the port trust state option here. Options to choose from are CoS and DSCP .
DSCP Mutation Map	Select and enter the DSCP mutation map name used here. This name can be up to 32 characters long. Select the None option to not allocate a DSCP mutation map to the port(s).

Click the **Apply** button to accept the changes made.

DSCP CoS Mapping

On this page, users can view and configure the DSCP CoS mapping settings. To view the following window, click **QoS > Advanced Settings > DSCP CoS Mapping**, as shown below:

Port	CoS	DSCP List
eth1/0/1	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63
eth1/0/2	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63
eth1/0/3	0	0-7
	1	8-15
	2	16-23
	3	24-31

Figure 7-9 DSCP CoS Mapping Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
CoS	Select the CoS value to map to the DSCP list. Options to choose from are 0 to 7 .
DSCP List	Enter the DSCP list value to map to the CoS value here. This value must be between 0 and 63 .

Click the **Apply** button to accept the changes made.

CoS Color Mapping

On this page, users can view and configure the CoS color mapping settings. To view the following window, click **QoS > Advanced Settings > CoS Color Mapping**, as shown below:

Port	Color	CoS List
eth1/0/1	Green	0-7
	Yellow	
	Red	
eth1/0/2	Green	0-7
	Yellow	
	Red	
eth1/0/3	Green	0-7
	Yellow	
	Red	
eth1/0/4	Green	0-7
	Yellow	
	Red	
eth1/0/5	Green	0-7
	Yellow	
	Red	
eth1/0/6	Green	0-7
	Yellow	
	Red	
eth1/0/7	Green	0-7
	Yellow	
	Red	

Figure 7-10 CoS Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
CoS List	Enter the CoS value that will be mapped to the color. This value must be between 0 and 7 .
Color	Select the color option that will be mapped to the CoS value. Options to choose from are Green , Yellow , and Red .

Click the **Apply** button to accept the changes made.

DSCP Color Mapping

On this page, users can view and configure the DSCP color mapping settings. To view the following window, click **QoS > Advanced Settings > DSCP Color Mapping**, as shown below:

Figure 7-11 DSCP Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
DSCP List	Enter the DSCP list value here that will be mapped to a color. This value must be between 0 and 63 .
Color	Select the color option that will be mapped to the DSCP value. Options to choose from are Green , Yellow , and Red .

Click the **Apply** button to accept the changes made.

Class Map

On this page, users can view and configure the class map settings. To view the following window, click **QoS > Advanced Settings > Class Map**, as shown below:

Figure 7-12 Class Map Window

The fields that can be configured are described below:

Parameter	Description
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.

Multiple Match Criteria	Select the multiple match criteria option here. Options to choose from are Match All and Match Any .
--------------------------------	--

Click the **Apply** button to accept the changes made.

Click the **Match** button to configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Match** button, the following page will be available.

Figure 7-13 Class Map (Match) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to match nothing to this class map.
Specify	Select the option to match something to this class map.
Access List Name	Select and enter the access list name that will be matched with this class map here. This name can be up to 32 characters long.
CoS List	Select and enter the CoS list value that will be matched with this class map here. This value must be between 0 and 7 . Tick the Inner option to match the inner most CoS of QinQ packets on a Layer 2 class of service (CoS) marking.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. This value must be between 0 and 63 . Tick the IPv4 only option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. This value must be between 0 and 7 . Tick the IPv6 only option to match IPv6 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are ARP, BGP, DHCP, DNS, EGP, FTP, IPv4, IPv6, NetBIOS, NFC, NTP, OSPF, PPPOE, RIP, RSTP, SSH, Telnet, and TFTP .
VLAN List	Select and enter the VLAN list value that will be matched with the class map here. This value must be between 1 and 4094 . Tick the Inner option to match the inner-most VLAN ID in an 802.1Q double tagged frame.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Aggregate Policer

On this page, users can view and configure the aggregate policer settings. To view the following window, click **QoS > Advanced Settings > Aggregate Policer**, as shown below:

The screenshot shows the 'Aggregate Policer' configuration window. It has two tabs: 'Single Rate Settings' (selected) and 'Two Rate Settings'. The 'Single Rate Settings' section includes fields for 'Aggregate Policer Name *', 'Average Rate * (0-10000000)' in Kbps, 'Normal Burst Size (0-16384)' in Kbyte, 'Maximum Burst Size (0-16384)' in Kbyte, 'Confirm Action' (Transmit), 'Exceed Action' (Transmit), 'Violate Action' (None), and 'Color Aware' (None). There are also dropdown menus for 'DSCP' and '1P' for the Confirm and Exceed actions. An 'Apply' button is at the bottom right. Below the settings is a table with columns: Name, Average Rate, Normal Burst Size, Max. Burst Size, Conform Action, Exceed Action, Violate Action, Color Aware, and a Delete button.

Name	Average Rate	Normal Burst Size	Max. Burst Size	Conform Action	Exceed Action	Violate Action	Color Aware	
APN-1	100	100		transmit	transmit		Disabled	Delete

Figure 7-14 Aggregate Policer (Single Rate Setting) Window

The fields that can be configured are described below:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer's name here.
Average Rate	Enter the average rate value here. This value must be between 0 and 10000000 kbps.
Normal Burst Size	Enter the normal burst size value here. This value must be between 0 and 16384 Kbytes.
Maximum Burst Size	Enter the maximum burst size value here. This value must be between 0 and 16384 Kbytes.
Confirm Action	<p>Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to Transmit. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <p>When selecting the Drop option, the packet will be dropped.</p> <p>When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.</p> <p>When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value.</p> <p>When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.</p> <p>When selecting the Transmit option, packets will be transmitted unaltered.</p>
Exceed Action	<p>Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is Drop. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <p>When selecting the Drop option, the packet will be dropped.</p> <p>When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the</p>

	<p>new IP DSCP value.</p> <p>When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value.</p> <p>When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.</p> <p>When selecting the Transmit option, packets will be transmitted unaltered.</p>
Violate Action	<p>Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for single rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <p>When selecting the Drop option, the packet will be dropped.</p> <p>When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.</p> <p>When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value.</p> <p>When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.</p> <p>When selecting the Transmit option, packets will be transmitted unaltered.</p>
Color Aware	<p>Select the color aware option here. Options to choose from are None and Enabled. When color aware is not specified, the policer works in the color blind mode. When color aware is enabled, the policer works in the color aware mode.</p>

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

After selecting the **Two Rate Setting** tab option, at the top of the page, the following page will be available.

Name	CIR	Confirm Burst	PIR	Peak Burst	Confirm Action	Exceed Action	Violate Action	Color Aware	
APN-2	100	100	100	120	transmit	drop	drop	Disabled	Delete

Figure 7-15 Aggregate Policer (Two Rate Setting) Window

The fields that can be configured are described below:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer's name here.
CIR	Enter the Committed Information Rate (CIR) value here. This value must be between 0 and 10000000 kbps. The committed packet rate is the first token bucket for the two-rate metering.
Confirm Burst	Enter the confirm burst value here. This value must be between 0 and 16384 Kbytes. The confirm burst value specifies the burst size for the first token bucket in kbps.
PIR	Enter the Peak information Rate (PIR) value here. This value must be between 0 and 10000000 kbps. The peak information rate is the second token bucket for the two-rate metering.
Peak Burst	Enter the peak burst value here. This value must be between 0 and 16384 Kbytes. The peak burst value is the burst size for the second token bucket in kilobytes.
Confirm Action	<p>Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to Transmit. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <p>When selecting the Drop option, the packet will be dropped.</p> <p>When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.</p> <p>When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value.</p> <p>When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.</p> <p>When selecting the Transmit option, packets will be transmitted unaltered.</p>
Exceed Action	<p>Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is Drop. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <p>When selecting the Drop option, the packet will be dropped.</p> <p>When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.</p> <p>When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value.</p> <p>When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.</p> <p>When selecting the Transmit option, packets will be transmitted unaltered.</p>
Violate Action	Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for single rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from

	<p>are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <p>When selecting the Drop option, the packet will be dropped.</p> <p>When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.</p> <p>When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value.</p> <p>When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.</p> <p>When selecting the Transmit option, packets will be transmitted unaltered.</p>
Color Aware	<p>Select the color aware option here. Options to choose from are None and Enabled. When color aware is not specified, the policer works in the color blind mode. When color aware is enabled, the policer works in the color aware mode.</p>

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Policy Map

On this page, users can view and configure the policy map settings. To view the following window, click **QoS > Advanced Settings > Policy Map**, as shown below:

Figure 7-16 Policy Map Window

The fields that can be configured for **Create/Delete Policy Map** are described below:

Parameter	Description
Policy Map Name	Enter the policy map's name here that will be created or deleted. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Traffic Policy** are described below:

Parameter	Description
Policy Map Name	Enter the policy map's name here. This name can be up to 32

	characters long.
Class Map Name	Enter the class map's name here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Policy Binding

On this page, users can view and configure the policy binding settings. To view the following window, click **QoS > Advanced Settings > Policy Binding**, as shown below:

Figure 7-17 Policy Binding Window

The fields that can be configured are described below:

Parameter	Description
From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. Options to choose from are Input and Output . Input specified ingress traffic and output specifies egress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. Select the None option to not tie a policy map to this entry.

Click the **Apply** button to accept the changes made.

8. Access Control List (ACL)

ACL Access List
ACL Interface Access Group
ACL VLAN Access Map
ACL VLAN Filter

ACL Access List

On this page, users can view and configure the ACL access list settings. To view the following window, click **ACL > ACL Access List**, as shown below:

Figure 8-1 ACL Access List Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type to find here. Options to choose from are IP ACL , IPv6 ACL , MAC ACL , and Expert ACL .
ACL Name	Enter the ACL name here. This name can be up to 32 characters long.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add ACL** button to create a new ACL profile.

Click the **Clear All Counter** button to clear all the counter information displayed.

Click the **Clear Counter** button to clear the counter information for the rule displayed.

Click the **Add Rule** button to create an ACL rule for the ACL profile selected.

Standard IP ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Figure 8-2 Standard IP ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL , Extend IP ACL , Standard IPv6 ACL , Extend IPv6 ACL , Extend MAC ACL , and Expert ACL .
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating a **Standard IP ACL** profile, the newly created **Standard IP ACL** profile will be displayed in the ACL profile display table, as shown below:

The screenshot shows the 'ACL Access List' window. At the top, there are fields for 'ACL Type' (set to 'IP ACL') and 'ACL Name' (set to '32 chars'). Below these is a 'Total Entries: 1' indicator. A table lists the ACL profile with columns: ACL Name, ACL Type, Start Sequence No., Step, Counter State, and Remark. The entry is 'Standard-I...', 'Standard IP ACL', '10', '10', 'Disabled'. There are 'Edit' and 'Delete' buttons for this entry. Below the table is a pagination control showing '1/1' and a 'Go' button. At the bottom, there is an 'ACL Rules' section with 'Clear All Counter', 'Clear Counter', and 'Add Rule' buttons, and a table with columns: Rule ID, Action, Rule, Time Range Name, and Counter.

Figure 8-3 Standard IP ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click on the **Add Rule** button.

This screenshot is similar to Figure 8-3, but the 'Standard-I...' entry in the ACL table is now bolded. The 'ACL Rules' section at the bottom is now titled 'Standard-IP-ACL-1 Rules' and contains the same 'Clear All Counter', 'Clear Counter', and 'Add Rule' buttons.

Figure 8-4 Standard IP ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

Figure 8-5 Standard IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule Number	Enter the ACL rule number here. This value must be between 1 and 65535 . If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

The screenshot shows the 'ACL Access List' configuration window. At the top, there are fields for 'ACL Type' (set to 'IP ACL') and 'ACL Name' (set to '32 chars'). Below this, a table lists 'Total Entries: 1'. The table has columns: ACL Name, ACL Type, Start Sequence No., Step, Counter State, and Remark. The entry shown is 'Standard-I...' with ACL Type 'Standard IP ACL', Start Sequence No. '10', Step '10', Counter State 'Enabled', and an empty Remark field. There are 'Apply' and 'Delete' buttons for this entry. Below the table, there are navigation controls: '1/1', '<<', '1', '>>', and 'Go'. Underneath, there is a section for 'Standard-IP-ACL-1 Rules' with buttons for 'Clear All Counter', 'Clear Counter', and 'Add Rule'. A table shows the rule details: Rule ID '10', Action 'Permit', Rule 'any any', Time Range Name, and Counter. There is a 'Delete' button for this rule. Navigation controls for the rules table are also present: '1/1', '<<', '1', '>>', and 'Go'.

Figure 8-6 Standard IP ACL (Counter State Enabled) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

The screenshot shows the 'ACL Access List' configuration window, similar to Figure 8-6 but with more details. The 'ACL Name' field is '32 chars'. The 'Total Entries: 1' table has columns: ACL Name, ACL Type, Start Sequence No., Step, Counter State, and Remark. The entry is 'Standard-I...' with ACL Type 'Standard IP ACL', Start Sequence No. '10', Step '10', Counter State 'Enabled', and Remark. There are 'Edit' and 'Delete' buttons for this entry. Below the table, there are navigation controls: '1/1', '<<', '1', '>>', and 'Go'. Underneath, there is a section for 'Standard-IP-ACL-1 Rules' with buttons for 'Clear All Counter', 'Clear Counter', and 'Add Rule'. A table shows the rule details: Rule ID '10', Action 'Permit', Rule 'any any', Time Range Name, and Counter '(In: 0 packets Egr: 0...'. There is a 'Delete' button for this rule. Navigation controls for the rules table are also present: '1/1', '<<', '1', '>>', and 'Go'.

Figure 8-7 Standard IP ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Extend IP ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Add ACL Access List

Add ACL Access List

ACL Type:

ACL Name:

Note: The first character of acl name must be a letter.

Figure 8-8 Extend IP ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL , Extend IP ACL , Standard IPv6 ACL , Extend IPv6 ACL , Extend MAC ACL , and Expert ACL .
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an **Extend IP ACL** profile, the newly created **Extend IP ACL** profile will be displayed in the ACL profile display table, as shown below:

ACL Access List

ACL Type: ACL Name:

Total Entries: 2

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
Standard-I...	Standard IP ACL	10	10	Enabled		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Extended-I...	Extend IP ACL	10	10	Disabled		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

1/1 < < < 1 > > >

ACL Rules

Rule ID	Action	Rule	Time Range Name	Counter

Figure 8-9 Extend IP ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click on the **Add Rule** button.

The screenshot shows the 'ACL Access List' window. At the top, there are fields for 'ACL Type' (set to 'IP ACL') and 'ACL Name' (set to '32 chars'). Below this, a table lists 'Total Entries: 2':

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark
Standard-I...	Standard IP ACL	10	10	Enabled	
Extended-I...	Extend IP ACL	10	10	Disabled	

Below the table, there are 'Edit' and 'Delete' buttons for each entry. At the bottom, there is a section for 'Extended-IP-ACL-1 Rules' with 'Clear All Counter', 'Clear Counter', and 'Add Rule' buttons.

Figure 8-10 Extend IP ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

The screenshot shows the 'Add ACL Rule' window. It contains the following configuration options:

- ACL Name:** Extended-IP-ACL-1
- ACL Type:** Extend IP ACL
- Rule Number (1-65535):** (Empty field, note: (If it isn't specified, the system automatically assigns.))
- Action:** Permit Deny
- Protocol Type:** TCP (Selected from a dropdown menu)
- Match IP Address:**
 - Source:** Any, Host, IP, Wildcard
 - Destination:** Any, Host, IP, Wildcard
- Match Port:** Source Port and Destination Port (Each with a 'Please Select' dropdown and two numeric input fields for port ranges)
- TCP Flag:** ack fin psh rst syn urg
- IP Precedence:** IP Precedence (with 'Please Select' dropdowns for 'ToS' and 'DSCP')
- DSCP (0-63):** DSCP (with 'Please Select' dropdown and numeric input field)
- Time Range:** 32 chars

At the bottom right, there are '<<Back' and 'Apply' buttons.

Figure 8-11 Extend IP ACL (Add Rule) Window

This is a dynamic page. Every selection made in the **Protocol Type** option will change the bottom part of this page.

The **fixed** fields that can be configured are described below:

Parameter	Description
Rule Number	Enter the ACL rule number here. This value must be between 1 and 65535 . If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , EIGRP , ESP , GRE , IGMP , OSPF , PIM , VRRP , IP-in-IP , PCP , Protocol ID , and None .
----------------------	--

After selecting the **TCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Figure 8-12 Extend IP ACL (Add Rule) TCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are = , > , < , ≠ , and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all

	ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are =, >, <, ≠, and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg .
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **UDP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Figure 8-13 Extend IP ACL (Add Rule) UDP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are = , > , < , ≠ , and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are = , > , < , ≠ , and Range . When selecting the = option, the

	specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14, and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **ICMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. The 'Protocol Type' is set to 'ICMP'. The 'Match IP Address' section has 'Any' selected for both Source and Destination. The 'Match ICMP' section has 'Specify ICMP Message Type' set to 'Please Select'. The 'IP Precedence' and 'ToS' are also set to 'Please Select'. The 'Time Range' field is empty and labeled '32 chars'. Navigation buttons '<<Back' and 'Apply' are visible at the bottom right.

Figure 8-14 Extend IP ACL (Add Rule) ICMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP

	address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **EIGRP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add ACL Rule

Add ACL Rule

ACL Name: Extended-IP-ACL-1
 ACL Type: Extend IP ACL
 Rule Number (1-65535): [] (If it isn't specified, the system automatically assigns.)
 Action: Permit Deny
 Protocol Type: **eigrp** [] 88 (0~255) Fragments

Match IP Address

Source: Any Host [] IP [] Wildcard []
 Destination: Any Host [] IP [] Wildcard []

IP Precedence [Please Select] ToS [Please Select]
 DSCP (0-63) [Please Select] []

Time Range: [32 chars]

<<Back Apply

Figure 8-15 Extend IP ACL (Add Rule) EIGRP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **ESP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. The 'ACL Name' is 'Extended-IP-ACL-1' and the 'ACL Type' is 'Extend IP ACL'. The 'Rule Number' is empty, with a note that the system will assign it. The 'Action' is set to 'Permit'. The 'Protocol Type' is 'esp' with a value of '50'. The 'Match IP Address' section has 'Any' selected for both Source and Destination. Below this, there are dropdowns for 'IP Precedence' and 'ToS', both set to 'Please Select'. There is also a 'DSCP (0-63)' dropdown set to 'Please Select' and a 'Time Range' field set to '32 chars'. At the bottom right, there are '<<Back' and 'Apply' buttons.

Figure 8-16 Extend IP ACL (Add Rule) ESP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **GRE** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. The 'Protocol Type' is set to 'gre'. The 'Match IP Address' section is expanded, showing options for Source and Destination. The 'Action' is set to 'Permit'. The 'Rule Number' is empty, and the 'Time Range' is set to '32 chars'. There are 'Back' and 'Apply' buttons at the bottom right.

Figure 8-17 Extend IP ACL (Add Rule) GRE Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14, and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule,

here.

After selecting the **IGMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. The 'Action' is set to 'Permit' and the 'Protocol Type' is 'igmp'. The 'Match IP Address' section has 'Any' selected for both Source and Destination. The 'IP Precedence' and 'ToS' fields are set to 'Please Select'. The 'Time Range' field contains '32 chars'. Buttons for '<<Back' and 'Apply' are visible at the bottom right.

Figure 8-18 Extend IP ACL (Add Rule) IGMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .

DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **OSPF** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. The 'Protocol Type' is set to 'ospf'. The 'Match IP Address' section has 'Any' selected for both Source and Destination. The 'Action' is set to 'Permit'. There are dropdown menus for 'IP Precedence' and 'ToS', and a 'DSCP' field. A 'Time Range' field is also present with a character count of 32.

Figure 8-19 Extend IP ACL (Add Rule) OSPF Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-

	delay), 9, 10, 11, 12, 13, 14, and 15.
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **PIM** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. The 'Protocol Type' is set to 'pim'. The 'Action' is 'Permit'. The 'Match IP Address' section is expanded, showing options for Source and Destination (Any, Host, IP, Wildcard). The 'IP Precedence' and 'ToS' fields are set to 'Please Select'. The 'Time Range' field is empty, showing '32 chars'.

Figure 8-20 Extend IP ACL (Add Rule) PIM Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP

	precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **VRRP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' window with the following configuration:

- ACL Name: Extended-IP-ACL-1
- ACL Type: Extend IP ACL
- Rule Number (1-65535): (empty)
- Action: Permit Deny
- Protocol Type: vrrp
- Match IP Address:
 - Source: Any, Host, IP, Wildcard
 - Destination: Any, Host, IP, Wildcard
- IP Precedence: Please Select
- ToS: Please Select
- DSCP (0-63): Please Select
- Time Range: 32 chars

Figure 8-21 Extend IP ACL (Add Rule) VRRP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.

IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **IP-in-IP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. The 'Protocol Type' is set to 'ipinip'. The 'Match IP Address' section has 'Any' selected for both Source and Destination. The 'Action' is set to 'Permit'. There are dropdown menus for 'IP Precedence' and 'ToS', and a 'DSCP' field. A 'Time Range' field is also present.

Figure 8-22 Extend IP ACL (Add Rule) IP-in-IP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination

	IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **PCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' window with the following configuration:

- ACL Name: Extended-IP-ACL-1
- ACL Type: Extend IP ACL
- Rule Number (1-65535): [Empty]
- Action: Permit Deny
- Protocol Type: **pcp** (0-255) Fragments
- Match IP Address:
 - Source: Any, Host, IP, Wildcard
 - Destination: Any, Host, IP, Wildcard
- IP Precedence: Please Select, ToS: Please Select
- DSCP (0-63): Please Select, [Empty]
- Time Range: 32 chars

Figure 8-23 Extend IP ACL (Add Rule) PCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the

	conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **Protocol ID** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' window with the following configuration:

- ACL Name:** Extended-IP-ACL-1
- ACL Type:** Extend IP ACL
- Rule Number (1-65535):** (empty field)
- Action:** Permit Deny
- Protocol Type:** Protocol ID (dropdown), (0~255) (text field), Fragments
- Match IP Address:**
 - Source:** Any, Host, IP, Wildcard (text field)
 - Destination:** Any, Host, IP, Wildcard (text field)
- IP Precedence:** Please Select (dropdown), **ToS:** Please Select (dropdown)
- DSCP (0-63):** Please Select (dropdown), (text field)
- Time Range:** 32 chars (text field)
- Buttons:** <<Back, Apply

Figure 8-24 Extend IP ACL (Add Rule) Protocol ID Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Protocol	Enter the Protocol ID value in the space provided. This value must be between 0 and 255 .
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a

	wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **None** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' window with the following configuration:

- ACL Name:** Extended-IP-ACL-1
- ACL Type:** Extend IP ACL
- Rule Number (1-65535):** (Empty field, note: (If it isn't specified, the system automatically assigns.)
- Action:** Permit Deny
- Protocol Type:** None (Selected in dropdown)
- Match IP Address:**
 - Source:** Any, Host, IP, Wildcard
 - Destination:** Any, Host, IP, Wildcard
- IP Precedence:** Please Select (Dropdown)
- ToS:** Please Select (Dropdown)
- DSCP (0-63):** Please Select (Dropdown)
- Time Range:** 32 chars (Text field)
- Buttons:** <<Back, Apply

Figure 8-25 Extend IP ACL (Add Rule) None Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this

	rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

Figure 8-26 Extend IP ACL (Counter State Enabled) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.

Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

The screenshot shows the 'ACL Access List' window. At the top, there are fields for 'ACL Type' (set to 'IP ACL') and 'ACL Name' (set to '32 chars'). Below this is a table with 'Total Entries: 2'. The table has columns: ACL Name, ACL Type, Start Sequence No., Step, Counter State, Remark, Edit, and Delete. The entries are:

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	Edit	Delete
Standard-I...	Standard IP ACL	10	10	Enabled		Edit	Delete
Extended-I...	Extend IP ACL	10	10	Enabled		Edit	Delete

Below the table are navigation buttons: 1/1, <-, <, 1, >, >, and Go. Underneath is the 'Extended-IP-ACL-1 Rules' section with buttons for 'Clear All Counter', 'Clear Counter', and 'Add Rule'. It contains a table with columns: Rule ID, Action, Rule, Time Range Name, Counter, and Delete. The entry is:

Rule ID	Action	Rule	Time Range Name	Counter	Delete
10	Permit	tcp any any		(Ing: 0 packets Egr: 0...	Delete

Navigation buttons for this section are: 1/1, <-, <, 1, >, >, and Go.

Figure 8-27 Extend IP ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Standard IPv6 ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

The screenshot shows the 'Add ACL Access List' window. It has fields for 'ACL Type' (set to 'Standard IPv6 ACL') and 'ACL Name' (set to '32 chars'). There is an 'Apply' button at the bottom right. A note at the bottom left states: 'Note: The first character of acl name must be a letter.'

Figure 8-28 Standard IPv6 ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL , Extend IP ACL , Standard IPv6 ACL , Extend IPv6 ACL , Extend MAC ACL , and Expert ACL .
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating a **Standard IPv6 ACL** profile, the newly created **Standard IPv6 ACL** profile will be displayed in the ACL profile display table, as shown below:

The screenshot shows the 'ACL Access List' window. At the top, there are fields for 'ACL Type' (set to 'IP ACL') and 'ACL Name' (set to '32 chars'), with a 'Find' button. Below this, it says 'Total Entries: 3' and has an 'Add ACL' button. The main table lists three entries:

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
Standard-I...	Standard IP ACL	10	10	Enabled		Edit Delete
Extended-I...	Extend IP ACL	10	10	Enabled		Edit Delete
Standard-I...	Standard IPv6 ACL	10	10	Disabled		Edit Delete

Below the table is a pagination control showing '1/1' and a 'Go' button. At the bottom, there are buttons for 'Clear All Counter', 'Clear Counter', and 'Add Rule'. Below these is a table for 'ACL Rules' with columns: Rule ID, Action, Rule, Time Range Name, Counter.

Figure 8-29 Standard IPv6 ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click on the **Add Rule** button.

This screenshot is similar to Figure 8-29, but the 'Standard IPv6 ACL' entry in the table is bolded. Below the table, the 'Standard-IPv6-ACL-1 Rules' section is active, showing the 'Add Rule' button. The 'ACL Rules' table at the bottom is also visible.

Figure 8-30 Standard IPv6 ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

Figure 8-31 Standard IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule Number	Enter the ACL rule number here. This value must be between 1 and 65535 . If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

The screenshot shows the 'ACL Access List' configuration window. At the top, there are fields for 'ACL Type' (set to 'IP ACL') and 'ACL Name' (set to '32 chars'). Below this, a table lists 'Total Entries: 3'. The first entry is a 'Standard IPv6 ACL' with 'Start Sequence No.' 10, 'Step' 10, and 'Counter State' 'Enabled'. Below the table, there are navigation buttons and a 'Go' button. At the bottom, there is a section for 'Standard-IPv6-ACL-1 Rules' with a table showing one rule with 'Rule ID' 10, 'Action' 'Permit', and 'Rule' 'any any'. There are also buttons for 'Clear All Counter', 'Clear Counter', and 'Add Rule'.

Figure 8-32 Standard IPv6 ACL (Counter State Enabled) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

The screenshot shows the 'ACL Access List' configuration window, similar to Figure 8-32, but with the 'Standard-IPv6-ACL-1 Rules' section expanded. The table below the main ACL list shows one rule with 'Rule ID' 10, 'Action' 'Permit', and 'Rule' 'any any'. The 'Counter' column for this rule shows '(Ing: 0 packets Egr: 0...'. There are also buttons for 'Clear All Counter', 'Clear Counter', and 'Add Rule'.

Figure 8-33 Standard IPv6 ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Extend IPv6 ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Figure 8-34 Extend IPv6 ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL , Extend IP ACL , Standard IPv6 ACL , Extend IPv6 ACL , Extend MAC ACL , and Expert ACL .
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an **Extend IPv6 ACL** profile, the newly created **Extend IPv6 ACL** profile will be displayed in the ACL profile display table, as shown below:

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
Standard-I...	Standard IP ACL	10	10	Enabled		Edit Delete
Extended-I...	Extend IP ACL	10	10	Enabled		Edit Delete
Standard-I...	Standard IPv6 ACL	10	10	Enabled		Edit Delete
Extended-I...	Extend IPv6 ACL	10	10	Disabled		Edit Delete

Figure 8-35 Extend IPv6 ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click on the **Add Rule** button.

ACL Access List

ACL Type: ACL Name:

Total Entries: 4

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
Standard-I...	Standard IP ACL	10	10	Enabled		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Extended-I...	Extend IP ACL	10	10	Enabled		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Standard-I...	Standard IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Extended-I...	Extend IPv6 ACL	10	10	Disabled		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

1/1

Extended-IPv6-ACL-1 Rules

Rule ID	Action	Rule	Time Range Name	Counter

Figure 8-36 Extend IPv6 ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

Add ACL Rule

Add ACL Rule

ACL Name: Extended-IPv6-ACL-1
 ACL Type: Extend IPv6 ACL
 Rule Number (1-65535): (If it isn't specified, the system automatically assigns.)
 Action: Permit Deny
 Protocol Type: (0~255) Fragments

Match IPv6 Address

Source: Any Host
 IPv6 Prefix Length:

Destination: Any Host
 IPv6 Prefix Length:

Match Port

Source Port: (0-65535) (0-65535)
 Destination Port: (0-65535) (0-65535)

TCP Flag: ack fin psh rst syn urg
 DSCP (0-63):
 Flow Label (0-1048575):
 Time Range:

Figure 8-37 Extend IPv6 ACL (Add Rule) Window

This is a dynamic page. Every selection made in the **Protocol Type** option will change the bottom part of this page.

The **fixed** fields that can be configured are described below:

Parameter	Description
Rule Number	Enter the ACL rule number here. This value must be between 1 and 65535 . If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from

	are Permit and Deny .
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , Protocol ID , ESP , PCP , SCTP , and None .

After selecting the **TCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. The 'Action' is set to 'Permit' and 'Protocol Type' is 'TCP'. Under 'Match IPv6 Address', both 'Source' and 'Destination' are set to 'Any' with an IPv6 address of '2012::1'. The 'Match Port' section has 'Please Select' dropdowns for both source and destination ports. At the bottom, there are 'TCP Flag' checkboxes (ack, fin, psh, rst, syn, urg), a 'DSCP' dropdown, and a 'Flow Label' field. The 'Time Range' is set to '32 chars'. Navigation buttons '<<Back' and 'Apply' are at the bottom right.

Figure 8-38 Extend IPv6 ACL (Add Rule) TCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are = , > , < , ≠ , and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be

	used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are =, >, <, ≠, and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **UDP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add ACL Rule

Add ACL Rule

ACL Name: Extended-IPv6-ACL-1
 ACL Type: Extend IPv6 ACL
 Rule Number (1-65535): (If it isn't specified, the system automatically assigns.)
 Action: Permit Deny
 Protocol Type: **UDP** (0~255) Fragments

Match IPv6 Address

Source: Any Host 2012::1 Prefix Length
 IPv6 2012::1

Destination: Any Host 2012::1 Prefix Length
 IPv6 2012::1

Match Port

Source Port: **Please Select** (0-65535) **Please Select** (0-65535)
 Destination Port: **Please Select** (0-65535) **Please Select** (0-65535)

DSCP (0-63): **Please Select**
 Flow Label (0-1048575):
 Time Range: 32 chars

<< Back Apply

Figure 8-39 Extend IPv6 ACL (Add Rule) UDP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
-----------	-------------

Source	Select and enter the source information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are = , > , < , ≠ , and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are = , > , < , ≠ , and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **ICMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add ACL Rule

Add ACL Rule

ACL Name: Extended-IPv6-ACL-1
 ACL Type: Extend IPv6 ACL
 Rule Number (1-65535): (If it isn't specified, the system automatically assigns.)
 Action: Permit Deny
 Protocol Type: ICMP (0~255) Fragments

Match IPv6 Address

Source: Any Host 2012::1
 IPv6 2012::1 Prefix Length
 Destination: Any Host 2012::1
 IPv6 2012::1 Prefix Length

Match ICMP

Specify ICMP Message Type: Please Select
 ICMP Message Type (0~255): Message Code (0~255):

DSCP (0-63): Please Select
 Flow Label (0-1048575):
 Time Range: 32 chars

<<Back Apply

Figure 8-40 Extend IPv6 ACL (Add Rule) ICMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **Protocol ID** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' window. The 'ACL Name' is 'Extended-IPv6-ACL-1' and the 'ACL Type' is 'Extend IPv6 ACL'. The 'Rule Number' field is empty with a note '(If it isn't specified, the system automatically assigns.)'. The 'Action' is set to 'Permit'. The 'Protocol Type' is 'Protocol ID'. The 'Match IPv6 Address' section has 'Any' selected for both Source and Destination. The 'DSCP' is set to 'Please Select'. The 'Flow Label' and 'Time Range' fields are empty. The 'Time Range' field has a hint '32 chars'. There are '<<Back' and 'Apply' buttons at the bottom right.

Figure 8-41 Extend IPv6 ACL (Add Rule) Protocol ID Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Protocol	Enter the Protocol ID value used here. This value must be between 0 and 255 .
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **ESP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add ACL Rule

Add ACL Rule

ACL Name: Extended-IPv6-ACL-1

ACL Type: Extend IPv6 ACL

Rule Number (1-65535): (If it isn't specified, the system automatically assigns.)

Action: Permit Deny

Protocol Type: (0~255) Fragments

Match IPv6 Address

Source: Any Host IPv6

Destination: Any Host IPv6

DSCP (0-63):

Flow Label (0-1048575):

Time Range:

<<Back Apply

Figure 8-42 Extend IPv6 ACL (Add Rule) ESP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **PCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Figure 8-43 Extend IPv6 ACL (Add Rule) PCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **SCTP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add ACL Rule

Add ACL Rule

ACL Name: Extended-IPv6-ACL-1

ACL Type: Extend IPv6 ACL

Rule Number (1-65535): (If it isn't specified, the system automatically assigns.)

Action: Permit Deny

Protocol Type: (0~255) Fragments

Match IPv6 Address

Source: Any Host IPv6 Prefix Length

Destination: Any Host IPv6 Prefix Length

DSCP (0-63):

Flow Label (0-1048575):

Time Range:

<<Back Apply

Figure 8-44 Extend IPv6 ACL (Add Rule) SCTP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **None** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Figure 8-45 Extend IPv6 ACL (Add Rule) None Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

ACL Access List

ACL Type: ACL Name: Find

Total Entries: 4 Add ACL

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	Edit	Delete
Standard-I...	Standard IP ACL	10	10	Enabled		Edit	Delete
Extended-I...	Extend IP ACL	10	10	Enabled		Edit	Delete
Standard-I...	Standard IPv6 ACL	10	10	Enabled		Edit	Delete
Extended-I...	Extend IPv6 ACL	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value="Enabled"/>	<input type="text"/>	Apply	Delete

1/1 < << 1 >> > Go

Extended-IPv6-ACL-1 Rules Clear All Counter Clear Counter Add Rule

Rule ID	Action	Rule	Time Range Name	Counter	Delete
10	Permit	tcp any any			Delete

1/1 < << 1 >> > Go

Figure 8-46 Extend IPv6 ACL (Counter State Enabled) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

ACL Access List

ACL Type: ACL Name: Find

Total Entries: 4 Add ACL

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	Edit	Delete
Standard-I...	Standard IP ACL	10	10	Enabled		Edit	Delete
Extended-I...	Extend IP ACL	10	10	Enabled		Edit	Delete
Standard-I...	Standard IPv6 ACL	10	10	Enabled		Edit	Delete
Extended-I...	Extend IPv6 ACL	10	10	Enabled		Edit	Delete

1/1 < << 1 >> > Go

Extended-IPv6-ACL-1 Rules Clear All Counter Clear Counter Add Rule

Rule ID	Action	Rule	Time Range Name	Counter	Delete
10	Permit	tcp any any		(Ing: 0 packets Egr: 0...	Delete

1/1 < << 1 >> > Go

Figure 8-47 Extend IPv6 ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Extend MAC ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Figure 8-48 Extend MAC ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL , Extend IP ACL , Standard IPv6 ACL , Extend IPv6 ACL , Extend MAC ACL , and Expert ACL .
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an **Extend MAC ACL** profile, the newly created **Extend MAC ACL** profile will be displayed in the ACL profile display table, as shown below:

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
Standard-I...	Standard IP ACL	10	10	Enabled		Edit Delete
Extended-I...	Extend IP ACL	10	10	Enabled		Edit Delete
Extended-M...	Extend MAC ACL	10	10	Disabled		Edit Delete
Standard-I...	Standard IPv6 ACL	10	10	Enabled		Edit Delete
Extended-I...	Extend IPv6 ACL	10	10	Enabled		Edit Delete

Figure 8-49 Extend MAC ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click on the **Add Rule** button.

ACL Access List

ACL Type: ACL Name:

Total Entries: 5

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	Edit	Delete
Standard-I...	Standard IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-M...	Extend MAC ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Standard-I...	Standard IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

1/1

Extended-MAC-ACL-1 Rules

Rule ID	Action	Rule	Time Range Name	Counter
---------	--------	------	-----------------	---------

Figure 8-50 Extend MAC ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

Add ACL Rule

Add ACL Rule

ACL Name: Extended-MAC-ACL-1

ACL Type: Extend Mac ACL

Rule Number (1-65535): (If it isn't specified, the system automatically assigns.)

Action: Permit Deny

Match MAC Address

Source: Any Host MAC Wildcard

Destination: Any Host MAC Wildcard

Match Ethernet Type

Specify Ethernet Type:

Ethernet Type (0x600-0xFFFF):

Ethernet Type Mask (0x0-0xFFFF):

CoS: Inner CoS:

VID (1-4094): Inner VID (1-4094):

Time Range:

Figure 8-51 Extend MAC ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule Number	Enter the ACL rule number here. This value must be between 1 and 65535 . If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option

	will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are aarp , appletalk , decent-iv , etype-6000 , etype-8042 , lat , lavc-sca , mop-console , mop-dump , vines-echo , vines-ip , xns-idp , and arp .
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x600 and 0xFFFF . When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF . When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value used here. This value is between 0 and 7 .
Inner CoS	Select the inner CoS value used here. This value is between 0 and 7 .
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

The screenshot shows the 'ACL Access List' configuration window. At the top, 'ACL Type' is set to 'IP ACL' and 'ACL Name' is '32 chars'. Below this, a table lists 5 ACL entries. The third entry, 'Extended-M...', is selected and its configuration is shown in a detailed view below. In this view, 'Counter State' is set to 'Enabled' and 'Remark' is empty. Below the detailed view, 'Extended-MAC-ACL-1 Rules' are listed, showing a single rule with ID 10, Action 'Permit', and Rule 'any any'.

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
Standard-I...	Standard IP ACL	10	10	Enabled		Edit Delete
Extended-I...	Extend IP ACL	10	10	Enabled		Edit Delete
Extended-M...	Extend MAC ACL	10	10	Enabled		Apply Delete
Standard-I...	Standard IPv6 ACL	10	10	Enabled		Edit Delete
Extended-I...	Extend IPv6 ACL	10	10	Enabled		Edit Delete

Rule ID	Action	Rule	Time Range Name	Counter
10	Permit	any any		

Figure 8-52 Extend MAC ACL (Counter State Enabled) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

The screenshot shows the 'ACL Access List' configuration window. At the top, there are fields for 'ACL Type' (set to 'IP ACL') and 'ACL Name' (set to '32 chars'), with a 'Find' button. Below this, it indicates 'Total Entries: 5' and an 'Add ACL' button. A table lists five ACL entries:

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	Edit	Delete
Standard-I...	Standard IP ACL	10	10	Enabled		Edit	Delete
Extended-I...	Extend IP ACL	10	10	Enabled		Edit	Delete
Extended-M...	Extend MAC ACL	10	10	Enabled		Edit	Delete
Standard-I...	Standard IPv6 ACL	10	10	Enabled		Edit	Delete
Extended-I...	Extend IPv6 ACL	10	10	Enabled		Edit	Delete

Below the table, there are navigation buttons (1/1, <, <<, 1, >>, >) and a 'Go' button. A sub-section titled 'Extended-MAC-ACL-1 Rules' contains buttons for 'Clear All Counter', 'Clear Counter', and 'Add Rule'. It displays a single rule:

Rule ID	Action	Rule	Time Range Name	Counter	Delete
10	Permit	any any		(In: 0 packets Egr: 0...	Delete

Navigation buttons (1/1, <, <<, 1, >>, >) and a 'Go' button are also present at the bottom of this section.

Figure 8-53 Extend MAC ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Expert ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

The screenshot shows the 'Add ACL Access List' configuration window. It has a title bar 'Add ACL Access List' and a subtitle 'Add ACL Access List'. There are two input fields: 'ACL Type' (set to 'Expert ACL') and 'ACL Name' (set to '32 chars'). An 'Apply' button is located at the bottom right. A red note at the bottom states: 'Note: The first character of acl name must be a letter.'

Figure 8-54 Expert ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL , Extend IP ACL , Standard IPv6 ACL , Extend IPv6 ACL , Extend MAC ACL , and Expert ACL .
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an **Expert ACL** profile, the newly created **Expert ACL** profile will be displayed in the ACL profile display table, as shown below:

ACL Access List

ACL Access List

ACL Type: ACL Name:

Total Entries: 6

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
Standard-I...	Standard IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-M...	Extend MAC ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Expert-ACL...	Expert ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Standard-I...	Standard IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

1/1

ACL Rules

Rule ID	Action	Rule	Time Range Name	Counter

Figure 8-55 Expert ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click on the **Add Rule** button.

ACL Access List

ACL Access List

ACL Type: ACL Name:

Total Entries: 6

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
Standard-I...	Standard IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-M...	Extend MAC ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Expert-ACL...	Expert ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Standard-I...	Standard IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

1/1

Expert-ACL-1 Rules

Rule ID	Action	Rule	Time Range Name	Counter

Figure 8-56 Expert ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

Figure 8-57 Expert ACL (Add Rule) Window

This is a dynamic page. Every selection made in the **Protocol Type** option will change the bottom part of this page.

The **fixed** fields that can be configured are described below:

Parameter	Description
Rule Number	Enter the ACL rule number here. This value must be between 1 and 65535 . If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , EIGRP , ESP , GRE , IGMP , OSPF , PIM , VRRP , IP-in-IP , PCP , Protocol ID , and None .

After selecting the **TCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Figure 8-58 Expert ACL (Add Rule) TCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose

	from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are =, >, <, ≠, and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are =, >, <, ≠, and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **UDP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Figure 8-59 Expert ACL (Add Rule) UDP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is

	selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are =, >, <, ≠, and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are =, >, <, ≠, and Range . When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14, and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **ICMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Figure 8-60 Expert ACL (Add Rule) ICMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the

	destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **EIGRP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Figure 8-61 Expert ACL (Add Rule) EIGRP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is

	selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **ESP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' window for an ESP rule. The form is titled 'Add ACL Rule' and contains the following fields and options:

- ACL Name:** Expert-ACL-1
- ACL Type:** Expert ACL
- Rule Number (1-65535):** 50 (If it isn't specified, the system automatically assigns.)
- Action:** Permit Deny
- Protocol Type:** esp (0~255) Fragments
- Match IP Address:**
 - Source: Any, Host, IP, Wildcard
 - Destination: Any, Host, IP, Wildcard
- Match MAC Address:**
 - Source: Any, Host, MAC, Wildcard
 - Destination: Any, Host, MAC, Wildcard
- IP Precedence:** Please Select
- ToS:** Please Select
- DSCP (0-63):** Please Select
- Outer VID (1-4094):** [Empty]
- Inner VID (1-4094):** [Empty]
- CoS:** Please Select
- Inner CoS:** Please Select
- Time Range:** 32 chars

Buttons at the bottom right: <<Back, Apply

Figure 8-62 Expert ACL (Add Rule) ESP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
-----------	-------------

Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **GRE** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. The 'Protocol Type' is set to 'gre'. The 'Match IP Address' section has 'Any' selected for both Source and Destination. The 'Match MAC Address' section has 'Any' selected for both Source and Destination. The 'Action' is set to 'Permit'. The 'Rule Number' is empty. The 'Outer VID' and 'Inner VID' are empty. The 'CoS' and 'Inner CoS' are set to 'Please Select'. The 'Time Range' is set to '32 chars'. There are '<< Back' and 'Apply' buttons at the bottom right.

Figure 8-63 Expert ACL (Add Rule) GRE Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose

	from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **IGMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add ACL Rule

Add ACL Rule

ACL Name: Expert-ACL-1

ACL Type: Expert ACL

Rule Number (1-65535): (blank) (If it isn't specified, the system automatically assigns.)

Action: Permit Deny

Protocol Type: igmp (0~255) Fragments

Match IP Address

Source: Any Host IP Wildcard

Destination: Any Host IP Wildcard

Match MAC Address

Source: Any Host MAC Wildcard

Destination: Any Host MAC Wildcard

IP Precedence: Please Select ToS: Please Select

DSCP (0-63): Please Select

Outer VID (1-4094): (blank) Inner VID (1-4094): (blank)

CoS: Please Select Inner CoS: Please Select

Time Range: 32 chars

<< Back Apply

Figure 8-64 Expert ACL (Add Rule) IGMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14, and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7 .

Time Range	Enter the time profile name that will be associated with this ACL rule, here.
-------------------	---

After selecting the **OSPF** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window for OSPF. The 'ACL Name' is 'Expert-ACL-1' and the 'ACL Type' is 'Expert ACL'. The 'Rule Number' is a text input field. The 'Action' is set to 'Permit'. The 'Protocol Type' is 'ospf' with a port number of '89'. The 'Match IP Address' section has 'Any' selected for both Source and Destination. The 'Match MAC Address' section has 'Any' selected for both Source and Destination. There are also dropdown menus for 'IP Precedence', 'DSCP', 'Outer VID', 'Inner VID', 'CoS', and 'Inner CoS', and a 'Time Range' field with '32 chars' entered. 'Back' and 'Apply' buttons are at the bottom right.

Figure 8-65 Expert ACL (Add Rule) OSPF Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard

	value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **PIM** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration page. The fields are as follows:

- ACL Name:** Expert-ACL-1
- ACL Type:** Expert ACL
- Rule Number (1-65535):** (Empty field, note: (If it isn't specified, the system automatically assigns.))
- Action:** Permit Deny
- Protocol Type:** pim (Selected from dropdown), 103 (Port number), Fragments
- Match IP Address:**
 - Source: Any, Host, IP, Wildcard
 - Destination: Any, Host, IP, Wildcard
- Match MAC Address:**
 - Source: Any, Host (11-DF-36-4B-A7-CC), MAC (11-DF-36-4B-A7-CC), Wildcard (11-DF-36-4B-A7-CC)
 - Destination: Any, Host (11-DF-36-4B-A7-CC), MAC (11-DF-36-4B-A7-CC), Wildcard (11-DF-36-4B-A7-CC)
- IP Precedence:** Please Select (Dropdown), **ToS:** Please Select (Dropdown)
- DSCP (0-63):** Please Select (Dropdown)
- Outer VID (1-4094):** (Empty field), **Inner VID (1-4094):** (Empty field)
- CoS:** Please Select (Dropdown), **Inner CoS:** Please Select (Dropdown)
- Time Range:** 32 chars (Text field)

Buttons at the bottom right: << Back, Apply

Figure 8-66 Expert ACL (Add Rule) PIM Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14, and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .

Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **VRRP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration window. Key fields include:

- ACL Name: Expert-ACL-1
- ACL Type: Expert ACL
- Rule Number: (empty)
- Action: Permit
- Protocol Type: vrrp
- Match IP Address: Source and Destination options (Any, Host, IP, Wildcard)
- Match MAC Address: Source and Destination options (Any, Host, MAC, Wildcard)
- IP Precedence and DSCP: Both set to 'Please Select'
- Outer VID and Inner VID: Both set to 'Please Select'
- CoS and Inner CoS: Both set to 'Please Select'
- Time Range: 32 chars

Figure 8-67 Expert ACL (Add Rule) VRRP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this

	rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **IP-in-IP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add ACL Rule

Add ACL Rule

ACL Name: Expert-ACL-1
 ACL Type: Expert ACL
 Rule Number (1-65535): (If it isn't specified, the system automatically assigns.)
 Action: Permit Deny
 Protocol Type: (0~255) Fragments

Match IP Address

Source: Any Host
 IP
 Wildcard:

Destination: Any Host
 IP
 Wildcard:

Match MAC Address

Source: Any Host
 MAC
 Wildcard:

Destination: Any Host
 MAC
 Wildcard:

IP Precedence ToS
 DSCP (0-63)

Outer VID (1-4094): Inner VID (1-4094):
 CoS: Inner CoS:
 Time Range:

<<Back Apply

Figure 8-68 Expert ACL (Add Rule) IP-in-IP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is

	selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **PCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' window for PCP. The form is titled 'Add ACL Rule' and contains the following fields and options:

- ACL Name:** Expert-ACL-1
- ACL Type:** Expert ACL
- Rule Number (1-65535):** (If it isn't specified, the system automatically assigns.)
- Action:** Permit Deny
- Protocol Type:** pcp (dropdown), 108 (input), (0~255) (range), Fragments
- Match IP Address:**
 - Source:** Any, Host, IP, Wildcard
 - Destination:** Any, Host, IP, Wildcard
- Match MAC Address:**
 - Source:** Any, Host, MAC, Wildcard
 - Destination:** Any, Host, MAC, Wildcard
- IP Precedence:** Please Select (dropdown), **ToS:** Please Select (dropdown)
- DSCP (0-63):** Please Select (dropdown)
- Outer VID (1-4094):** (input), **Inner VID (1-4094):** (input)
- CoS:** Please Select (dropdown), **Inner CoS:** Please Select (dropdown)
- Time Range:** 32 chars (input)

Buttons: <<Back, Apply

Figure 8-69 Expert ACL (Add Rule) PCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
-----------	-------------

Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **Protocol ID** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration page. The 'Protocol Type' is set to 'Protocol ID'. The 'Match IP Address' section has 'Any' selected for both Source and Destination. The 'Match MAC Address' section has 'Any' selected for both Source and Destination. The 'IP Precedence' and 'DSCP' options are set to 'Please Select'. The 'Outer VID' and 'Inner VID' fields are empty. The 'CoS' and 'Inner CoS' options are set to 'Please Select'. The 'Time Range' is set to '32 chars'. There are '<< Back' and 'Apply' buttons at the bottom right.

Figure 8-70 Expert ACL (Add Rule) Protocol ID Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Protocol	Enter the Protocol ID value used here. This value must be between 0 and 255 .
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard

	value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2 (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14 , and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

After selecting the **None** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

The screenshot shows the 'Add ACL Rule' configuration page. The ACL Name is 'Expert-ACL-1' and the ACL Type is 'Expert ACL'. The Rule Number is empty, with a note that the system will assign it if not specified. The Action is set to 'Permit'. The Protocol Type is set to 'None'. The Match IP Address section has 'Any' selected for both Source and Destination. The Match MAC Address section has 'Any' selected for both Source and Destination. The IP Precedence and ToS are both set to 'Please Select'. The DSCP is set to 'Please Select'. The Outer VID and Inner VID are empty. The CoS and Inner CoS are both set to 'Please Select'. The Time Range is set to '32 chars'. There are '<< Back' and 'Apply' buttons at the bottom right.

Figure 8-71 Expert ACL (Add Rule) None Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination information here. Options to choose from are Any , Host , MAC , and Wildcard . When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host's MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine) , 1 (priority) , 2, (immediate) , 3 (flash) , 4 (flash-override) , 5 (critical) , 6 (internet) , and 7 (network) . After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal) , 1 (min-monetary-cost) , 2 (max-reliability) , 3, 4 (max-throughput) , 5, 6, 7, 8 (min-delay) , 9, 10, 11, 12, 13, 14, and 15 .
ToS	Select the Type of Service option here. Options to choose from are 0 to 15 .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Outer VID	Enter the outer VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094 .
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .

Inner CoS	Select the inner Class of Service (CoS) value here. Options to choose from are from 0 to 7.
Time Range	Enter the time profile name that will be associated with this ACL rule, here.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

ACL Access List

ACL Type: ACL Name:

Total Entries: 6

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	Edit	Delete
Standard-I...	Standard IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-M...	Extend MAC ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Expert-ACL...	Expert ACL	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value="Enabled"/>	<input type="text"/>	<input type="button" value="Apply"/>	<input type="button" value="Delete"/>
Standard-I...	Standard IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

1/1

Expert-ACL-1 Rules

Rule ID	Action	Rule	Time Range Name	Counter	Delete
10	Permit	tcp any any any any			<input type="button" value="Delete"/>

1/1

Figure 8-72 Expert ACL (Counter State Enabled) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

ACL Access List

ACL Type: ACL Name:

Total Entries: 6

ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	Edit	Delete
Standard-I...	Standard IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IP ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-M...	Extend MAC ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Expert-ACL...	Expert ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Standard-I...	Standard IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Extended-I...	Extend IPv6 ACL	10	10	Enabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

1/1

Expert-ACL-1 Rules

Rule ID	Action	Rule	Time Range Name	Counter	Delete
10	Permit	tcp any any any		(In: 0 packets Egr. 0...)	<input type="button" value="Delete"/>

1/1

Figure 8-73 Expert ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

ACL Interface Access Group

On this page, users can view and configure the ACL interface access group settings. To view the following window, click **ACL > ACL Interface Access Group**, as shown below:

ACL Interface Access Group

ACL Interface Access Group

From Port: To Port: Action: Type: ACL Name: Direction:

Port	In				Out			
	IP ACL	IPv6 ACL	MAC ACL	Expert ACL	IP ACL	IPv6 ACL	MAC ACL	Expert ACL
eth1/0/1								
eth1/0/2								
eth1/0/3								
eth1/0/4								
eth1/0/5								
eth1/0/6								
eth1/0/7								
eth1/0/8								
eth1/0/9								
eth1/0/10								
eth1/0/11								
eth1/0/12								
eth1/0/13								
eth1/0/14								
eth1/0/15								
eth1/0/16								
eth1/0/17								
eth1/0/18								
eth1/0/19								
eth1/0/20								

Figure 8-74 ACL Interface Access Group Window

The fields that can be configured are described below:

Parameter	Description
-----------	-------------

From Port ~ To Port	Select the range of ports that will be used for this configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the ACL type here. Options to choose from are IP ACL , IPv6 ACL , MAC ACL , and Expert ACL .
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.
Direction	Select the direction here. Options to choose from are In and Out .

Click the **Apply** button to accept the changes made.

ACL VLAN Access Map

On this page, users can view and configure the ACL VLAN access map settings. To view the following window, click **ACL > ACL VLAN Access Map**, as shown below:

Figure 8-75 ACL VLAN Access Map Window

The fields that can be configured are described below:

Parameter	Description
Access Map Name	Enter the access map's name here. This name can be up to 32 characters long.
Sub Map Number	Enter the sub-map's number here. This value must be between 1 and 65535 .
Action	Select the action that will be taken here. Options to choose from are Forward , Drop , and Redirect . When the Redirect option is selected, select the redirected interface from the drop-down list.
Counter State	Select whether to enable or disable the counter state.

Click the **Apply** button to accept the changes made.

Click the **Clear All Counter** button to clear the counter information for all the access maps.

Click the **Clear Counter** button to clear the counter information for the specified access map.

Click the **Find** button to locate a specific entry based on the information entered.

ACL VLAN Filter

On this page, users can view and configure the ACL VLAN filter settings. To view the following window, click **ACL > ACL VLAN Filter**, as shown below:

Figure 8-76 ACL VLAN Filter Window

The fields that can be configured are described below:

Parameter	Description
Access Map Name	Enter the access map's name here. This name can be up to 32 characters long.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
VID List	Enter the VLAN ID list that will be used here. Select the All VLANs option to apply this configuration to all the VLANs configured on this switch.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

9. Security

Trusted Host

Trusted Host

On this page, users can view and configure the trusted host settings. To view the following window, click **Security > Trusted Host**, as shown below:

Figure 9-1 Trusted Host Window

The fields that can be configured are described below:

Parameter	Description
Access Class	Enter the access class' name here. This name can be up to 32 characters long.
Type	Select the trusted host type here. Options to choose from are Telnet , SSH , Ping , HTTP , and HTTPS .

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

10. Monitoring

Mirror Settings Traffic

Mirror Settings

On this page, users can view and configure the mirror feature's settings. The switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a monitoring device to the mirroring port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view the following window, click **Monitoring > Mirror Settings**, as shown below:

Figure 10-1 Mirror Settings Window

The fields that can be configured for **RSPAN VLAN Settings** are described below:

Parameter	Description
VLAN ID List	Enter the VLAN list's ID(s) that will be associated with this configuration here.

Click the **Add** button to add the VLAN(s) to the configuration.

Click the **Delete** button to delete the VLAN(s) from the configuration.

The fields that can be configured for **Mirror Settings** are described below:

Parameter	Description
Session Number	Select the mirror session number for this entry here. This number is between 1 and 4.
Destination	Tick the checkbox, next to the Destination option, to configure the destination for this port mirror entry. In the first drop-down menu select the destination type option. Options

	<p>to choose from are Port and Remote VLAN.</p> <p>After selecting the Port option, select the destination port number from the second drop-down menu.</p> <p>After selecting the Remote VLAN option, select the destination port number from the seconds drop-down menu and enter the VID in the space provided. The VID must be between 2 and 4094.</p>
Source	<p>Tick the checkbox, next to the Source option, to configure the source for this port mirror entry.</p> <p>In the first drop-down menu select the source type option. Options to choose from are Port, ACL, and Remote VLAN.</p> <p>After selecting the Port option, select the From Port number and the To Port number from the second and third drop-down menus. Lastly select the Frame Type option from the fourth drop-down menu. Options to choose from as the Frame Type are Both, RX, and TX. When selecting Both, traffic in both the incoming and outgoing directions will be mirrored. When selecting RX, traffic in only the incoming direction will be mirrored. When selecting TX, traffic in only the outgoing direction will be mirrored.</p> <p>After selecting the ACL option, enter the ACL profile name in the space provided.</p> <p>After selecting the Remote VLAN option, enter the VID in the space provided. The VID must be between 2 and 4094.</p>

Click the **Add** button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

The fields that can be configured for **Mirror Session Table** are described below:

Parameter	Description
Mirror Session Type	<p>Select the mirror session type of information that will be displayed from the drop-down menu. Options to choose from are All Session, Session Number, Remote Session, and Local Session.</p> <p>After selecting the Session Number option, select the session number from the second drop-down menu. This number is from 1 to 4.</p>

Click the **Find** button to locate a specific entry based on the information entered.

Traffic

Traffic Monitoring by Direction

On this page, users can monitor traffic, per-port, in a certain direction. The two directions, that can be selected, are received (**RX**) or transmitted (**TX**) packets. After selecting a **Port** number and then selecting the **Direction** option from the drop-down list, click the **Apply** button to view the page below:

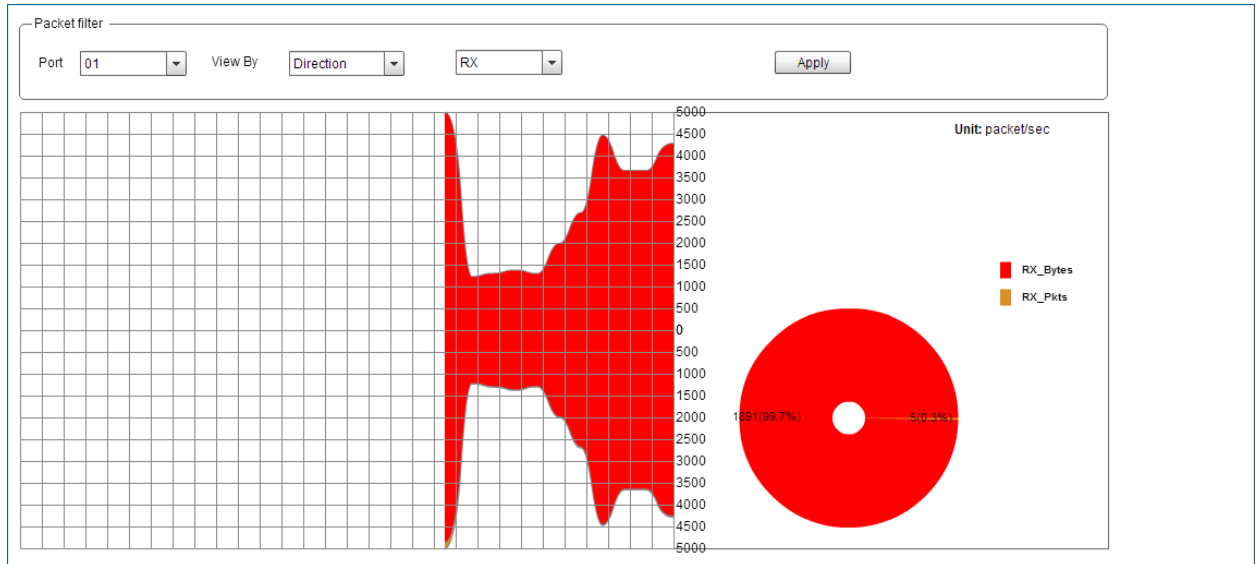


Figure 10-2 Traffic Monitoring by Direction Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number to display.
View By	Select the View By option here. Options to choose from are Direction , Type , Size , and Error .
Direction	Select the direction information to display for the port selected. Options to choose from are received (RX) and transmitted (TX).

Click the **Apply** button to initiate the display information based to the selections made.

Traffic Monitoring by Type

On this page, users can monitor traffic, per-port, of a certain type. After selecting a **Port** number and then selecting the **Type** option from the drop-down list, click the **Apply** button to view the page below:

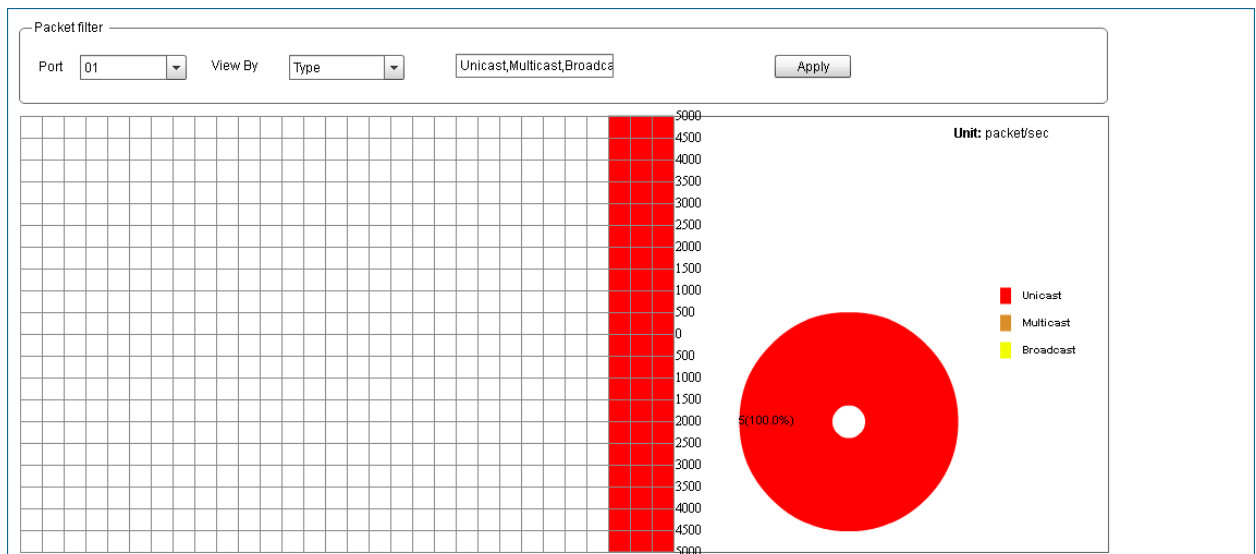


Figure 10-3 Traffic Monitoring by Type Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number to display.
View By	Select the View By option here. Options to choose from are Direction , Type , Size , and Error .
Type	Select the type of information to display for the port selected. Options to choose from are Unicast , Multicast , Broadcast , and All .

Click the **Apply** button to initiate the display information based to the selections made.

Traffic Monitoring by Size

On this page, users can monitor traffic, per-port, of a certain packet size. After selecting a **Port** number and then selecting the **Size** option from the drop-down list, click the **Apply** button to view the page below:

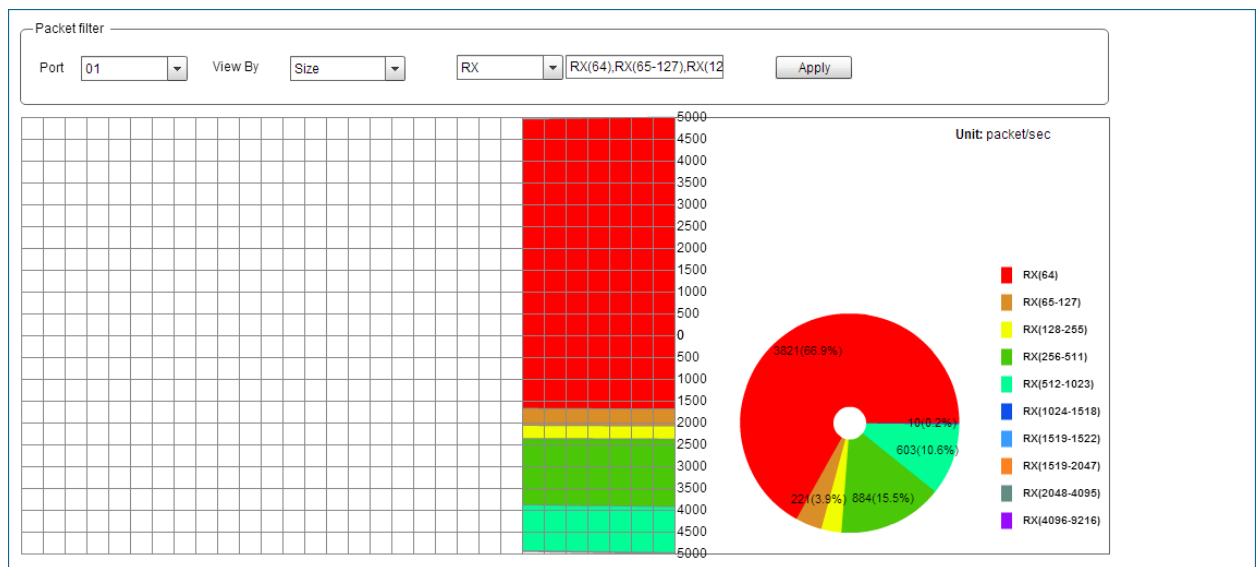


Figure 10-4 Traffic Monitoring by Size Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number to display.
View By	Select the View By option here. Options to choose from are Direction , Type , Size , and Error .
Direction	Select the direction of the traffic that will be monitored. Options to choose from are received (RX) and transmitted (TX).
Size	Select the size of the information to display for the port selected. Options to choose from are 64 , 65-127 , 128-255 , 256-511 , 512-1023 , 1024-1518 , 1519-1522 , 1519-2047 , 2048-4095 , 4096-9216 , and All .

Click the **Apply** button to initiate the display information based to the selections made.

Traffic Monitoring by Error

On this page, users can monitor traffic, per-port, of a certain error type and direction. After selecting a **Port** number and then selecting the **Error** option from the drop-down list, click the **Apply** button to view the page below:

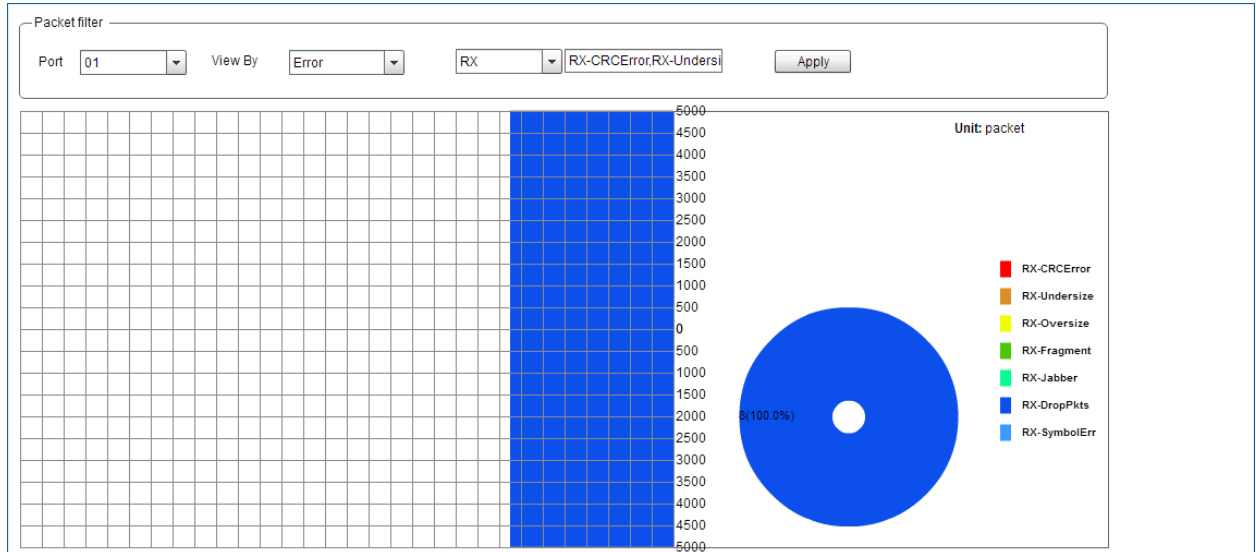


Figure 10-5 Traffic Monitoring by Error Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number to display.
View By	Select the View By option here. Options to choose from are Direction , Type , Size , and Error .
Direction	Select the error direction of the information to display for the port selected. Options to choose from are received (RX) and transmitted (TX).
Error Type	Select the error type of the information to display for the port selected.

Click the **Apply** button to initiate the display information based to the selections made.

11. Save and Tools

Save Configuration
Firmware Upgrade & Backup
Configuration Restore & Backup
Log Backup
Reset
Reboot System

Save Configuration

On this page, users can save the running configuration to the start-up configuration. This is to prevent the loss of configuration in the event of a power failure. To view the following window, click **Save > Save Configuration**, as shown below:

Figure 11-1 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
File Path	Enter the filename and path in the space provided.

Click the **Apply** button to save the configuration.

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

On this page, users can initiate a firmware upgrade from a local PC using HTTP. To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

Figure 11-2 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source URL	Enter the source filename and path of the firmware file located on the local PC. This field can be up to 64 characters long. Alternatively click the Browse button to navigate to the location of the firmware file located on the local PC.
Destination URL	Enter the destination path and location where the new firmware should be stored on the switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from TFTP

On this page, users can initiate a firmware upgrade from a TFTP server. To view the following window, click **Tools > Firmware Upgrade & Backup > firmware Upgrade from TFTP**, as shown below:

Figure 11-3 Firmware Upgrade from TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
VRF Name	Enter the VRF name here. This name can be up to 12 characters long.
Source URL	Enter the source filename and path of the firmware file located on the TFTP server here. This field can be up to 64 characters long.
Destination URL	Enter the destination path and location where the new firmware should be stored on the switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

On this page, users can initiate a firmware backup to a local PC using HTTP. To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

Figure 11-4 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source URL	Enter the source filename and path of the firmware file located on the switch here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to TFTP

On this page, users can initiate a firmware backup to a TFTP server. To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP**, as shown below:

Figure 11-5 Firmware Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
VRF Name	Enter the VRF name here. This name can be up to 12 characters long.
Source URL	Enter the source filename and path of the firmware file located on the switch here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Configuration Restore & Backup

Configuration Restore from HTTP

On this page, users can initiate a configuration restore from a local PC using HTTP. To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

Figure 11-6 Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source URL	Enter the source filename and path of the configuration file located on the local PC. This field can be up to 64 characters long. Alternatively click the Browse button to navigate to the location of the configuration file located on the local PC.
Destination URL	Enter the destination path and location where the configuration file should be stored on the switch. This field can be up to 64 characters long. Select the running-config option to restore and overwrite the running configuration file on the switch. Select the startup-config

option to restore and overwrite the start-up configuration file on the switch.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from TFTP

On this page, users can initiate a configuration restore from a TFTP server. To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:

Figure 11-7 Configuration Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
VRF Name	Enter the VRF name here. This name can be up to 12 characters long.
Source URL	Enter the source filename and path of the configuration file located on the TFTP server here. This field can be up to 64 characters long.
Destination URL	Enter the destination path and location where the configuration file should be stored on the switch. This field can be up to 64 characters long. Select the running-config option to restore and overwrite the running configuration file on the switch. Select the startup-config option to restore and overwrite the start-up configuration file on the switch.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

On this page, users can initiate a configuration file backup to a local PC using HTTP. To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

Figure 11-8 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source URL	Enter the source filename and path of the configuration file located on

the switch here. This field can be up to 64 characters long. Select the **running-config** option to backup the running configuration file from the switch. Select the **startup-config** option to backup the start-up configuration file from the switch.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to TFTP

On this page, users can initiate a configuration file backup to a TFTP server. To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:

Figure 11-9 Configuration Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
VRF Name	Enter the VRF name here. This name can be up to 12 characters long.
Source URL	Enter the source filename and path of the configuration file located on the switch here. This field can be up to 64 characters long. Select the running-config option to backup the running configuration file from the switch. Select the startup-config option to backup the start-up configuration file from the switch.
Destination URL	Enter the destination path and location where the configuration file should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Log Backup

Log Backup to HTTP

On this page, users can initiate a system log backup to a local PC using HTTP. To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:

Figure 11-10 Log Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Log Type	Select the log type that will be backed up to the local PC using HTTP. When the System Log option is selected, the system log will be backed up. When the Attack Log is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Log Backup to TFTP

On this page, users can initiate a system log backup to a TFTP server. To view the following window, click **Tools > Log Backup > Log Backup to TFTP**, as shown below:

Figure 11-11 Log Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
VRF Name	Enter the VRF name here. This name can be up to 12 characters long.
Destination URL	Enter the destination path and location where the log file should be stored on the TFTP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the TFTP server. When the System Log option is selected, the system log will be backed up. When the Attack Log is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Reset

On this page, users can reset the switch's configuration to the factory default settings. To view the following window, click **Tools > Reset**, as shown below:

Figure 11-12 Reset Window

Select the **The Switch will be reset to its factory defaults including IP address and stacking information, and then will save, reboot** option to reset the switch's configuration to its factory default settings.

Select the **The Switch will be reset to its factory defaults except IP address, and then will save, reboot** option to reset the switch's configuration to its factory default settings. This option will exclude the IP address from being changed.

Select the **The Switch will be reset to its factory defaults including IP address** option to reset the switch's configuration to its factory default settings.

Click the **Apply** button to initiate the factory default reset and reboot the switch.

Reboot System

On this page, users can reboot the switch and alternatively save the configuration before doing so. To view the following window, click **Tools > Reboot System**, as shown below:

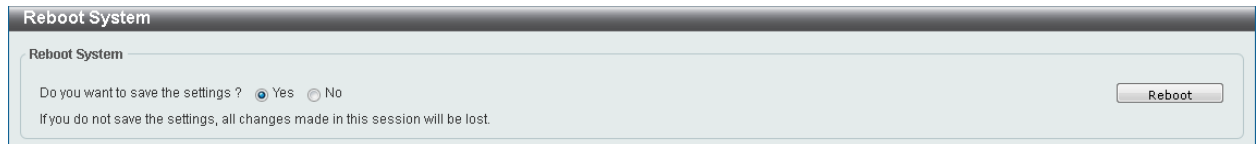


Figure 11-13 Reboot System Window

When rebooting the switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the switch.

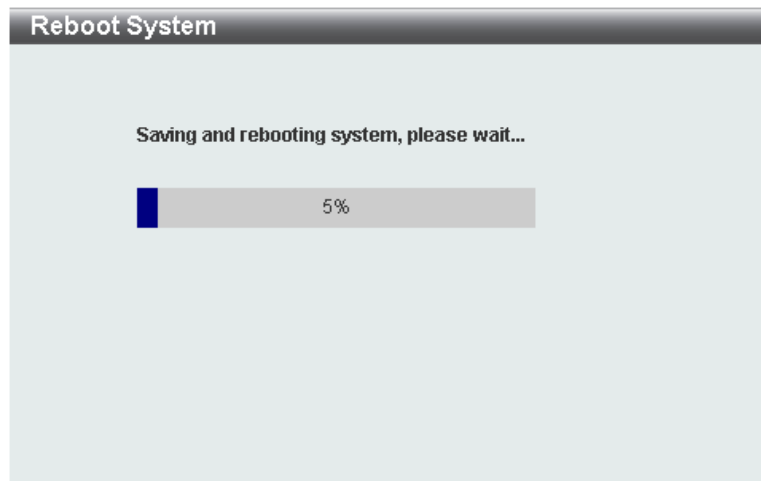


Figure 11-14 Reboot System (Rebooting) Window

Appendix A - Password Recovery Procedure

This section describes the procedure for resetting passwords on the D-Link DXS-3600 Series switch.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords will be forgotten or destroyed, so network administrators need to reset these passwords. This section will explain how the **Password Recovery** feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on this switch to easily recover passwords.

Complete these steps to reset the password:

- For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
- Power on the Switch. After the **UART init** is loaded to 100%, the switch will allow 2 seconds for the user to press the hotkey [**^**] (**Shift+6**) to enter the "Password Recovery Mode." Once the Switch enters the "Password Recovery Mode," all ports on the Switch will be disabled.

```

Boot Procedure                                     V1.10.008
-----
Power On Self Test ..... 100 %

MAC Address   : 00-17-9A-14-6B-10
H/W Version  : B1

Please Wait, Loading V2.00.012 Runtime Image ..... 100 %
UART init ..... 100 %

```

Password Recovery Mode

```
Switch(reset-config)#
```

In the "Password Recovery Mode" only the following commands can be used.

no enable password	This command is used to delete all account level passwords.
no login password	This command is used to clear the local login methods.
no username	This command is used to delete all local user accounts.
password-recovery	This command is used to initiate the password recovery procedure.
reload	This command is used to save and reboot the switch.
reload clear running-config	This command is used to reset the running configuration to the factory default settings and then reboot the switch.
show running-config	This command is used to display the current running configuration.
show username	This command is used to display local user account information.

Appendix B - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this switch.

802.1X

Log Description	Severity
<p>Event description: 802.1X Authentication failure.</p> <p>Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> reason: The reason for the failed authentication. username: The user that is being authenticated.. interface-id: The interface name. macaddr: The MAC address of thr authenticated device. 	Warning
<p>Event description: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: The user that is being authenticated. interface-id: The interface name. macaddr: The MAC address of the authenticated device. 	Informational

AAA

Log Description	Severity
<p>Event description: This log will be generated when AAA global state is enabled or disabled.</p> <p>Log Message: AAA is <status>.</p> <p>Parameters description:</p> <ul style="list-style-type: none"> status: The status indicates the AAA enabled or disabled. 	Informational
<p>Event description: This log will be generated when login successfully.</p> <p>Log Message: Successful login through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <ul style="list-style-type: none"> exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. Username: It indicates the username for authentication. 	Informational
<p>Event description: This log will be generated when login failure.</p> <p>Log Message: Login failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p>	Warning

<p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	
<p>Event description: This log will be generated when the remote server does not respond to the login authentication request.</p> <p>Log Message: Login failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>server-ip: It indicates the AAA server IP address.</p> <p>username: It indicates the username for authentication.</p>	Warning
<p>Event description: This log will be generated when enable privilege successfully.</p> <p>Log Message: Successful enable privilege through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: none, local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>Username: It indicates the username for authentication.</p>	Informational
<p>Event description: This log will be generated when enable privilege failure.</p> <p>Log Message: Enable privilege failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	Warning
<p>Event description: This log will be generated when the remote server does not respond to the enable password authentication request.</p> <p>Log Message: Enable privilege failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>server-ip: It indicates the AAA server IP address.</p> <p>username: It indicates the username for authentication.</p>	Warning

<p>Event description: This log will be generated when RADIUS assigned a valid VLAN ID attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> server-ip: It indicates the RADIUS server IP address. vid: The assign VLAN ID that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication. 	Informational
<p>Event description: This log will be generated when RADIUS assigned a valid bandwidth attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface -id> (Username: <username>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> server-ip: It indicates the RADIUS server IP address. Direction: It indicates the direction for bandwidth control, e.g.: ingress or egress. Threshold: The assign threshold of bandwidth that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication. 	Informational
<p>Event description: This log will be generated when RADIUS assigned a valid priority attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port < interface -id> (Username: <username>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> server-ip: It indicates the RADIUS server IP address. priority: The assign priority that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication. 	Informational
<p>Event description: This log will be generated when RADIUS assigned ACL script but fails to apply to the system due to insufficient resource.</p> <p>Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port < interface -id> (<acl-script>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> server-ip: It indicates the RADIUS server IP address. username: It indicates the username for authentication. interface-id: It indicates the port number of the client authenticated. acl-script: The assign ACL script that authorized by from RADIUS server. 	Warning

BGP

Log Description	Severity
<p>Event description: BGP FSM with Peer has gone to the successfully established state.</p> <p>Log Message: BGP-6-ESTABLISH: BGP connection is successfully established (Peer:<ipaddr>).</p> <p>Parameters description:</p> <ul style="list-style-type: none"> ipaddr: IP address of BGP peer. 	Informational

<p>Event description: BGP connection is normally closed.</p> <p>Log Message: BGP-6-NORMALCLOSE: BGP connection is normally closed (Peer:<ipaddr>).</p> <p>Parameters description: ipaddr: IP address of BGP peer.</p>	Informational
<p>Event description: BGP connection is closed due to error (Error Code, Error Subcode and Data fields Refer to RFC).</p> <p>Log Message: BGP-4-ERRCLOSE: BGP connection is closed due to error (Code:<num> Subcode:<num> Field:<field> Peer:<ipaddr>).</p> <p>Parameters description: num: Error Code or Error Subcode is defined in RFC 4271 etc. field: field value when an error happen. ipaddr: IP address of the BGP peer.</p>	Warning
<p>Event description: Receive a BGP notify packet with an undefined error code or sub error code in RFC 4271.</p> <p>Log Message: BGP-4-RCVUNKOWNERR: BGP Notify: unkown Error code(num), Sub Error code(num), Peer:<ipaddr>.</p> <p>Parameters description: num: Error Code or Error Subcode is defined in RFC 4271 etc. ipaddr: IP address of BGP peer.</p>	Warning
<p>Event description: Receive a BGP update packet but the next_hop points to a local interface.</p> <p>Log Message: BGP-4-BADNHOP: BGP Update Attr NHop: Erroneous NHop <ipaddr> Peer:<ipaddr>.</p> <p>Parameters description: ipaddr: IP address of BGP peer.</p>	Warning
<p>Event description: BGP connection is closed due to some events happens. (Event refer to RFC)</p> <p>Log Message: BGP-4-EVENTCLOSE: BGP connection is closed due to Event: <num> (Peer:<ipaddr>).</p> <p>Parameters description: num: Event is defined in RFC 4271 etc. ipaddr: IP address of BGP peer.</p>	Warning
<p>Event description: BGP connection is closed due to receive notify packet. (Error Code and Error Subcode refer to RFC)</p> <p>Log Message: BGP-4-NOTIFYCLOSE: BGP connection is closed due to Notify: Code <num> Subcode <num> (Peer:<ipaddr>).</p> <p>Parameters description: num: Error Code or Error Subcode is defined in RFC 4271 etc. ipaddr: IP address of BGP peer.</p>	Warning
<p>Event description: The number of bgp prefix received from this neighbor reaches the threshold.</p> <p>Log Message: BGP-6-PEERPFXMAX: The number of prefix received reaches <num>, max <limit> (Peer < ipaddr >).</p> <p>Parameters description: num: The number of prefix received. limit: Max number of prefix allowed to receive. ipaddr: IP address of BGP peer.</p>	Information
<p>Event description: The total bgp prefix number received exceeds the limit.</p>	Information

Log Message: BGP-6-TOTALPFXMAX: The total number of prefix received reaches max prefix limit.	
Event description: BGP received unnecessary AS4-PATH attribute from new (4-bytes AS) BGP peer Log Message: BGP-4-RCVUNNECEAS4PATH: Received AS4-PATH attribute from new (4-bytes AS) peer. (Peer <ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Warning
Event description: BGP received unnecessary AS4-AGGREGATOR attribute from new (4-bytes AS) BGP peer Log Message: BGP-4-RCVUNNECEAS4AGGRE: Received AS4-AGGREGATOR attribute from new (4-bytes AS) peer. (Peer <ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Warning
Event description: BGP received AS_CONFED_SEQUENCE or AS_CONFED_SET path segment type in AS4-PATH attribute. Log Message: BGP-4-RCVASCONFEDINAS4PATH: Received AS_CONFED_SEQUENCE or AS_CONFED_SET path segment type in AS4-PATH attribute. (Peer <ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Warning
Event description: BGP received invalid AS4-PATH attribute. Log Message: BGP-4-RCVBADAS4PATH: Received invalid AS4-PATH attribute. Value : <STRING> (Peer <ipaddr>). Parameters description: STRING: Detailed description about the invalid attribute. ipaddr: IP address of BGP peer.	Warning
Event description: BGP received invalid AS4- AGGREGATOR attribute. Log Message: BGP-4-RCVBADAS4AGGRE: Received invalid AS4-AGGREGATOR attribute. Value : <STRING> (Peer <ipaddr>). Parameters description: STRING: Detailed description about the invalid attribute. ipaddr: IP address of BGP peer.	Warning

BPDU Protection

Log Description	Severity
Event description: Record the event when the BPDU attack happened. Log Message: <interface-id> enter STP BPDU under protection state (mode: <mode>) Parameters description: interface-id: Interface on which detected STP BPDU attack. mode: BPDU Protection mode of the interface. Mode can be drop, block, or shutdown	Informational
Event description: Record the event when the STP BPDU attack recovered. Log Message: <interface-id> recover from BPDU under protection state. Parameters description: interface-id: Interface on which detected STP BPDU attack.	Informational

CFM

Log Description	Severity
<p>Event description: Cross-connect is detected</p> <p>Log Message: CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents the MEPID of the MEP. The value 0 means unknown MEPID. macaddr: Represents the MAC address of the MEP. The value all zeros mean unknown MAC address. <p>Note: In CFM hardware mode, remote MEP information (mepid and macaddr) is unknown.</p>	Critical
<p>Event description: Error CFM CCM packet is detected</p> <p>Log Message: CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents the MEPID of the MEP. The value 0 means unknown MEPID. macaddr: Represents the MAC address of the MEP. The value all zeros means unknown MAC address. <p>Note: In CFM hardware mode, remote MEP information (mepid and macaddr) is unknown.</p>	Warning
<p>Event description: cannot receive the remote MEP's CCM packet</p> <p>Log Message: CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP. 	Warning
<p>Event description: Remote MEP's MAC reports an error status</p> <p>Log Message: CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>,</p>	Warning

Local(Port <[unitID:]portNum>, Direction:<mepdirection>)

Parameters description:

- vlanid: Represents the VLAN identifier of the MEP.
 - mdlevel: Represents the MD level of the MEP.
 - unitID: Represents the ID of the device in the stacking system.
 - portNum: Represents the logical port number of the MEP.
 - mepdirection: Represents the MEP direction, which can be "inward" or "outward".
 - mepid: Represents the MEPID of the MEP.
 - macaddr: Represents the MAC address of the MEP.
-

Event description: Remote MEP detects CFM defects Informational

Log Message: CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)

Parameters description:

- vlanid: Represents the VLAN identifier of the MEP.
 - mdlevel: Represents the MD level of the MEP.
 - unitID: Represents the ID of the device in the stacking system.
 - portNum: Represents the logical port number of the MEP.
 - mepdirection: Represents the MEP direction, which can be "inward" or "outward".
 - mepid: Represents the MEPID of the MEP.
 - macaddr: Represents the MAC address of the MEP.
-
-

CFM Extension

Log Description	Severity
<p>Event description: AIS condition detected</p> <p>Log Message: AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP. 	Notice
<p>Event description: AIS condition cleared</p> <p>Log Message: AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP. 	Notice

<p>Event description: LCK condition detected</p> <p>Log Message: LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP. 	Notice
<p>Event description: LCK condition cleared</p> <p>Log Message: LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP. 	Notice

Configuration/Firmware

Log Description	Severity
<p>Event description: Firmware upgraded successfully.</p> <p>Log Message: [Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description:</p> <ul style="list-style-type: none"> unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. 	Informational
<p>Event description: Firmware upgraded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description:</p> <ul style="list-style-type: none"> unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. 	Warning
<p>Event description: Firmware uploaded successfully.</p> <p>Log Message: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description:</p>	Informational

<p>unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	
<p>Event description: Firmware uploaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	Warning
<p>Event description: Configuration downloaded successfully.</p> <p>Log Message: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	Informational
<p>Event description: Configuration downloaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	Warning
<p>Event description: Configuration uploaded successfully.</p> <p>Log Message: [Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	Informational
<p>Event description: Configuration uploaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user.</p>	Warning

ipaddr: Represent client IP address.
macaddr : Represent client MAC address.

DDM

Log Description	Severity
<p>Event description: DDM exceeded or recover from DDM alarm threshold</p> <p>Log Message: Optical transceiver <interface-id> [component] [high-low] alarm threshold [exceedType]</p> <p>Parameters description:</p> <p>interface-id: The port number.</p> <p>component: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power.</p> <p>high-low: High or low threshold.</p> <p>exceedType: indicate exceed threshold or recover to normal event, the value should be "exceeded" or "exceeding back to normal"</p>	Critical
<p>Event description: DDM exceeded or recover from DDM warning threshold</p> <p>Log Message: Optical transceiver <interface-id> [component] [high-low] warning threshold [exceedType]</p> <p>Parameters description:</p> <p>interface-id: The port number.</p> <p>component: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power.</p> <p>high-low: High or low threshold.</p> <p>exceedType: indicate exceed threshold or recover to normal event, the value should be "exceeded" or "exceeding back to normal"</p>	Warning

DHCPv6 Client

Log Description	Severity
<p>Event description: DHCPv6 client interface administrator state changed.</p> <p>Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled disabled].</p> <p>Parameters description:</p> <p><ipif-name>: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: DHCPv6 client obtains an ipv6 address from a DHCPv6 server.</p> <p>Log Message: DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name>.</p> <p>Parameters description:</p> <p>ipv6address: ipv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The ipv6 address obtained from a DHCPv6 server starts renewing.</p> <p>Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts renewing.</p> <p>Parameters description:</p>	Informational

ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	
Event description: The ipv6 address obtained from a DHCPv6 server renews success. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> renews success. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event description: The ipv6 address obtained from a DHCPv6 server starts rebinding Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event description: The ipv6 address obtained from a DHCPv6 server rebinds success Log Message: The IPv6 address < ipv6address > on interface <ipif-name> rebinds success. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface..	Informational
Event description: The ipv6 address from a DHCPv6 server was deleted. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> was deleted. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event description: DHCPv6 client PD interface administrator state changed. Log Message: DHCPv6 client PD on interface <intf-name> changed state to <enabled disabled> Parameters description: intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: DHCPv6 client PD obtains an IPv6 prefix from a delegation router. Log Message: DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> Parameters description: ipv6networkaddr: ipv6 preifx obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix obtained from a delegation router starts renewing. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing. Parameters description: ipv6networkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix obtained from a delegation router renews	Informational

success.

Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success.

Parameters description:

ipv6networkaddr: IPv6 prefix obtained from a delegation router.

intf-name: Name of the DHCPv6 client PD nterface.

Event description: The IPv6 prefix obtained from a delegation router starts rebinding. Informational

Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding.

Parameters description:

ipv6address: IPv6 prefix obtained from a delegation router.

intf-name: Name of the DHCPv6 client PD interface.

Event description: The IPv6 prefix obtained from a delegation router rebinds success. Informational

Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success.

Parameters description:

ipv6address: IPv6 prefix obtained from a delegation router.

intf-name: Name of the DHCPv6 client PD interface.

Event description: The IPv6 prefix from a delegation router was deleted. Informational

Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted.

Parameters description:

ipv6address: IPv6 prefix obtained from a delegation router.

intf-name: Name of the DHCPv6 client PD interface.

DHCPv6 Relay

Log Description

Severity

Event description: DHCPv6 relay on a specify interface's administrator state changed Informational

Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled]

Parameters description:

<ipif-name>: Name of the DHCPv6 relay agent interface.

DHCPv6 Server

Log Description

Severity

Event description: The address of the DHCPv6 Server pool is used up Informational

Log Message: The address of the DHCPv6 Server pool <pool-name> is used up.

Parameters description:

<pool-name>: Name of the DHCPv6 Server pool.

Event description: The number of allocated ipv6 addresses is equal to 4096 Informational

Log Message: The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 4096.

DLMS

Log Description	Severity
Event Description: Input an illegal activation code. Log Message: Illegal activation code (AC: <string25>). Parameters Description: <string25>: Activation Code	Informational
Event Description: License Expired. Log Message: License expired (license:<license-model>, AC: <string25>). Parameters Description: <license-model>: License Model Name. <string25>: Activation Code	Critical
Event Description: License successfully installed. Log Message: License successfully installed (license:<license-model>, AC: <string25>). Parameters Description: <license-model>: License Model Name. <string25>: Activation Code	Informational
Event Description:When a license is going to expire, it will be logged before 30 days. Log Message: License will expire in 30 days. (license:<license-model>, AC: <string25>). Parameters Description: <license-model>: License Model Name. <string25>: Activation Code	Informational

DOS Prevention

Log Description	Severity
Event description: Record the event if any attacking packet is received in the interval. Log Message: <dos-type> is dropped from (IP :< ip-address> Port: <interface-id>). Parameters description: dos-type: The type of DoS attack will be one of the followings. ip-address: IP address of attacker. interface-id: the attacked interface.	Notice

DULD

Log Description	Severity
Event description: A unidirectional link has been detected on this port Log Message: <interface-id> is unidirectional. Parameters description: unitID: the unit ID portNum: port number	Informational

Dynamic ARP Inspection

Log Description	Severity
<p>Event description: This log will be generated when DAI detect invalid ARP packet.</p> <p>Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>).</p> <p>Parameters description:</p> <p> type: The type of ARP packet, it indicates that ARP packet is request or ARP response.</p>	Warning
<p>Event description: This log will be generated when DAI detect valid ARP packet.</p> <p>Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>).</p> <p>Parameters description:</p> <p> type: The type of ARP packet, it indicates that ARP packet is request or ARP response.</p>	Informational

ERPS

Log Description	Severity
<p>Event description: Signal failure detected</p> <p>Log Message: Signal failure detected on node <macaddr></p> <p>Parameters description:</p> <p> macaddr: The system MAC address of the node</p>	Notice
<p>Event description: Signal failure cleared</p> <p>Log Message: Signal failure cleared on node <macaddr></p> <p>Parameters description:</p> <p> macaddr: The system MAC address of the node.</p>	Notice
<p>Event description: RPL owner conflict</p> <p>Log Message: RPL owner conflicted on the ring <macaddr></p> <p>Parameters description:</p> <p> macaddr: The system MAC address of the node</p>	Warning

Interface

Log Description	Severity
<p>Event description: Port link up.</p> <p>Log Message: Port < interface-id > link up, <link state></p> <p>Parameters description:</p> <p> portNum: 1.Interger value;2.Represent the logic port number of the device.</p> <p> link state: for ex: , 100Mbps FULL duplex</p>	Informational
<p>Event description: Port link down.</p> <p>Log Message: Port < interface-id > link down</p> <p>Parameters description:</p> <p> portNum: 1.Interger value;2.Represent the logic port number of the device.</p>	Informational

IP Directed-Broadcast

Log Description	Severity
<p>Event description: IP Directed-broadcast rate exceed 50 packets per second on a certain subnet.</p> <p>Log Message: IP Directed Broadcast packet rate is high on subnet. [(IP: <ipaddr>)]</p> <p>Parameters description:</p> <p>IP: the Broadcast IP destination address.</p>	Informational
<p>Event description: IP Directed-broadcast rate exceed 100 packets per second</p> <p>Log Message: IP Directed Broadcast rate is high.</p> <p>Parameters description:</p>	Informational

LACP

Log Description	Severity
<p>Event description: Link Aggregation Group link up.</p> <p>Log Message: Link Aggregation Group < group_id > link up.</p> <p>Parameters description:</p> <p>group_id: The group id of the link down aggregation group.</p>	Informational
<p>Event description: Link Aggregation Group link down.</p> <p>Log Message: Link Aggregation Group < group_id > link down.</p> <p>Parameters description:</p> <p>group_id: The group id of the link down aggregation group.</p>	Informational
<p>Event description: Member port attach to Link Aggregation Group.</p> <p>Log Message: <ifname> attach to Link Aggregation Group <group_id>.</p> <p>Parameters description:</p> <p>ifname: The interface name of the port that attach to aggregation group.</p> <p>group_id: The group id of the aggregation group that port attach to.</p>	Informational
<p>Event description: Member port detach from Link Aggregation Group.</p> <p>Log Message: <ifname> detach from Link Aggregation Group <group_id>.</p> <p>Parameters description:</p> <p>ifname: The interface name of the port that detach from aggregation group.</p> <p>group_id: The group id of the aggregation group that port detach from.</p>	Informational

LBD

Log Description	Severity
<p>Event description: Record the event when an interface detect loop.</p> <p>Log Message: <interface-id> LBD loop occurred.</p> <p><interface-id > VLAN <vlan-id> LBD loop occurred.</p> <p>Parameters description:</p> <p>interface-id: Interface on which loop is detected.</p> <p>vlan-id: VLAN on which loop is detected.</p>	Critical
<p>Event description: Record the event when an interface loop recovered.</p> <p>Log Message: <interface-id> LBD loop recovered.</p> <p><interface-id> VLAN <vlan-id> LBD loop recovered.</p>	Critical

Parameters description:

interface-id: Interface on which loop is detected.

vlan-id: VLAN on which loop is detected.

Event description: Record the event when the number of VLANs that loop back has occurred exceeds a reserved number. Critical

Log Message: Loop VLAN numbers overflow.

Parameters description:**LLDP-MED**

Log Description	Severity
<p>Event description: LLDP-MED topology change detected</p> <p>Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters description:</p> <p>portNum: The port number.</p> <p>chassisType: chassis ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) <p>chassisID: chassis ID.</p> <p>portType: port ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) <p>portID: port ID.</p> <p>deviceClass: LLDP-MED device type.</p>	Notice
<p>Event description: Conflict LLDP-MED device type detected</p> <p>Log Message: Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters description:</p> <p>portNum: The port number.</p> <p>chassisType: chassis ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 	Notice

3. portComponent(3)
 4. macAddress(4)
 5. networkAddress(5)
 6. interfaceName(6)
 7. local(7)
 chassisID: chassis ID.
 portType: port ID subtype.
 Value list:
 1. interfaceAlias(1)
 2. portComponent(2)
 3. macAddress(3)
 4. networkAddress(4)
 5. interfaceName(5)
 6. agentCircuitId(6)
 7. local(7)
 portID: port ID.
 deviceClass: LLDP-MED device type.

Event description: Incompatible LLDP-MED TLV set detected

Notice

Log Message: Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)

Parameters description:

portNum: The port number.
 chassisType: chassis ID subtype.
 Value list:
 1. chassisComponent(1)
 2. interfaceAlias(2)
 3. portComponent(3)
 4. macAddress(4)
 5. networkAddress(5)
 6. interfaceName(6)
 7. local(7)
 chassisID: chassis ID.
 portType: port ID subtype.
 Value list:
 1. interfaceAlias(1)
 2. portComponent(2)
 3. macAddress(3)
 4. networkAddress(4)
 5. interfaceName(5)
 6. agentCircuitId(6)
 7. local(7)
 portID: port ID.
 deviceClass: LLDP-MED device type.

Login/Logout CLI

Log Description	Severity
-----------------	----------

<p>Event description: Login through console successfully.</p> <p>Log Message: [Unit <unitID>,]Successful login through Console (Username: <username>)</p> <p>Parameters description: unitID: The unit ID. username: Represent current login user.</p>	Informational
<p>Event description: Login through console unsuccessfully.</p> <p>Log Message: [Unit <unitID>,] Login failed through Console (Username: <username>)</p> <p>Parameters description: unitID: The unit ID. username: Represent current login user.</p>	Warning
<p>Event description: Console session timed out.</p> <p>Log Message: [Unit <unitID>,] Console session timed out (Username: <username>)</p> <p>Parameters description: unitID: The unit ID. username: Represent current login user.</p>	Informational
<p>Event description: Logout through console.</p> <p>Log Message: [Unit <unitID>,] Logout through Console (Username: <username>)</p> <p>Parameters description: unitID: The unit ID. username: Represent current login user.</p>	Informational
<p>Event description: Login through telnet successfully.</p> <p>Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description: username: Represent current login user. ipaddr: Represent client IP address.</p>	Informational
<p>Event description: Login through telnet unsuccessfully.</p> <p>Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description: username: Represent current login user. ipaddr: Represent client IP address.</p>	Warning
<p>Event description: Telnet session timed out.</p> <p>Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description: username: Represent current login user. ipaddr: Represent client IP address.</p>	Informational
<p>Event description: Logout through telnet.</p> <p>Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description: username: Represent current login user. ipaddr: Represent client IP address.</p>	Informational
<p>Event description: Login through SSH successfully.</p> <p>Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>)</p>	Informational

Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	
Event description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>)	Critical
Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	
Event description: SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>)	Informational
Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	
Event description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational
Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	

MAC

Log Description	Severity
Event description: the host has passed MAC authentication Log Message: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Informational
Event description: the host has aged out. Log Message: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Informational
Event description: the host failed to pass the authentication. Log Message: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Critical
Event description: the authorized user number on the whole device has reached the maximum user limit. Log Message: MAC-based Access Control enters stop learning state..	Warning

Event description: the authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: MAC-based Access Control recovers from stop learning state.	Warning
Event description: the authorized user number on an interface has reached the maximum user limit. Log Message: <interface-id> enters MAC-based Access Control stop learning state Parameters description: interface-id: the interface on which the host is authenticated.	Warning
Event description: the authorized user number on an interface is below the maximum user limit in a time interval. Log Message: <interface-id> recovers from MAC-based Access Control stop learning state. Parameters description: interface-id: the interface on which the host is authenticated.	Warning

Management Port

Log Description	Severity
Event description: Record the event if any error frames which can affect management port Notice: Connectivity, such as CRC errors, alignment and jabber errors, is detected every two minutes. Log Message: Detected <counter> <error-counter-name> on <interface-id>. Parameters description: counter: The error frame counters. error-counter-name: Error counter name, include: rxFCSErrorPkts, rxAlignmentErrorPkts, rxCodeErrorPkts, rxUndersizedPkts, rxOversizedPkts, rxFragmentPkts, rxJabbers,rxDropPkts, txExcessiveDeferralPkts, txFCSErrorPkts, txLateCollisionPkts, txExcessiveCollisionPkts and txDropPkts counter. interface-id: Out of band management interface.	Notice

Module

Log Description	Severity
Event Description: Module inserts and can works. Log Message: Module <module-type> is inserted. Parameters Description: module-type: the expansion module name.	Informational
Event Description: Module inserts and can't works. Log Message: Module < module-type > inserts but can't work except reboot device. Parameters Description: module-type: the expansion module name.	Warning
Event Description: Module hot removes. Log Message: Module < module-type > is removed. Parameters Description: module-type: the expansion module name.	Informational

MPLS

Log Description	Severity
Event description: LSP is up Log Message: LSP <lsp_id> is up Parameters description: lsp_id: The established LSP ID	Informational
Event description: LSP is down Log Message: LSP <lsp_id> is down Parameters description: lsp_id: The deleted LSP ID	Informational

MSTP Debug Enhancement

Log Description	Severity
Event description: Topology changed. Log Message: Topology changed [([Instance:<InstanceID>], <interface-id> ,MAC:<macaddr>)] Parameters description: InstanceID: Instance ID. portNum:Port ID macaddr: MAC address	Notice
Event description: Spanning Tree new Root Bridge Log Message: [CIST CIST Regional MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>) Parameters description: InstanceID: Instance ID. macaddr: Mac address value: priority value	Informational
Event description: Spanning Tree Protocol is enabled Log Message: Spanning Tree Protocol is enabled	Informational
Event description: Spanning Tree Protocol is disabled Log Message: Spanning Tree Protocol is disabled	Informational
Event description: New root port Log Message: New root port selected [([Instance:<InstanceID>], <interface-id>)] Parameters description: InstanceID: Instance ID. portNum:Port ID	Notice
Event description: Spanning Tree port status changed Log Message: Spanning Tree port status change [([Instance:<InstanceID>], <interface-id>)] <old_status> -> <new_status> Parameters description: InstanceID: Instance ID. portNum: Port ID old_status: Old status	Notice

new_status: New status	
Event description: Spanning Tree port role changed.	Informational
Log Message: Spanning Tree port role change. [([Instance:<InstanceID>], <interface-id>)] <old_role> -> <new_role>	
Parameters description: InstanceID: Instance ID. portNum:Port ID/ old_role: Old role new_status:New role	
Event description: Spanning Tree instance created.	Informational
Log Message: Spanning Tree instance create. Instance:<InstanceID>	
Parameters description: InstanceID: Instance ID.	
Event description: Spanning Tree instance deleted.	Informational
Log Message: Spanning Tree instance delete. Instance:<InstanceID>	
Parameters description: InstanceID: Instance ID.	
Event description: Spanning Tree Version changed.	Informational
Log Message: Spanning Tree version change. New version:<new_version>	
Parameters description: new_version: New STP version.	
Event description: Spanning Tree MST configuration ID name and revision level changed.	Informational
Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name> ,revision level <revision_level>).	
Parameters description: name : New name. revision_level:New revision level.	
Event description: Spanning Tree MST configuration ID VLAN mapping table deleted.	Informational
Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]).	
Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	
Event description: Spanning Tree MST configuration ID VLAN mapping table added.	Informational
Log Message: Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]).	
Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	

OSPFv2 Enhancement

Log Description	Severity
Event description: OSPF interface link state changed.	Informational

<p>Log Message: OSPF-6-INTFSTATECHANGE: OSPF interface <intf-name> changed state to [Up Down]</p> <p>Parameters description: intf-name: Name of OSPF interface.</p>	
<p>Event description: OSPF interface administrator state changed.</p> <p>Log Message: OSPF-6-INTFADMINCHANGE: OSPF protocol on interface <intf-name> changed state to [Enabled Disabled]</p> <p>Parameters description: intf-name: Name of OSPF interface.</p>	Informational
<p>Event description: One OSPF interface changed from one area to another.</p> <p>Log Message: OSPF-6-INTFAREACHANGE: OSPF interface <intf-name> changed from area <area-id> to area <area-id></p> <p>Parameters description: intf-name: Name of OSPF interface. area-id: OSPF area ID.</p>	Informational
<p>Event description: One OSPF neighbor state changed from Loading to Full.</p> <p>Log Message: OSPF-5-NBRLOADINGTOFULL: OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full</p> <p>Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.</p>	Notice
<p>Event description: One OSPF neighbor state changed from Full to Down.</p> <p>Log Message: OSPF-5-NBRFULLTODOWN: OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down</p> <p>Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.</p>	Notice
<p>Event description: One OSPF neighbor state's dead timer expired.</p> <p>Log Message: OSPF-5-DTIMEXPIRED: OSPF nbr <nbr-id> on interface <intf-name> dead timer expired</p> <p>Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.</p>	Notice
<p>Event description: One OSPF virtual neighbor state changed from Loading to Full.</p> <p>Log Message: OSPF-5-VNBRLOADINGTOFULL: OSPF nbr <nbr-id> on virtual link changed state from Loading to Full</p> <p>Parameters description: nbr-id: Neighbor's router ID.</p>	Notice
<p>Event description: One OSPF virtual neighbor state changed from Full to Down.</p> <p>Log Message: OSPF-5-VNBRFULLTODOWN: OSPF nbr <nbr-id> on virtual link changed state from Full to Down</p> <p>Parameters description: nbr-id: Neighbor's router ID.</p>	Notice
<p>Event description: OSPF router ID was changed.</p> <p>Log Message: OSPF-6-RIDCHANGE: OSPF router ID changed to <router-id></p> <p>Parameters description: router-id: OSPF router ID.</p>	Informational
<p>Event description: Enable OSPF.</p>	Informational

Log Message: OSPF-6-STATECHANGE: OSPF state changed to [Enabled | Disabled]

Peripheral

Log Description	Severity
<p>Event description: Fan Recovered.</p> <p>Log Message: Unit <id>, <fan-descr> back to normal.</p> <p>Parameters description:</p> <p> Unit <id>: The unit ID.</p> <p> fan-descr: The FAN ID and position.</p>	Critical
<p>Event description: Fan Fail</p> <p>Log Message: Unit <id> <fan-descr> failed</p> <p>Parameters description:</p> <p> Unit <id>: The unit ID.</p> <p> fan-descr: The FAN ID and position.</p>	Critical
<p>Event description: Temperature sensor enters alarm state.</p> <p>Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree></p> <p>Parameters description:</p> <p> unitID: The unit ID.</p> <p> thermal-sensor-descr: The sensor ID and position.</p> <p> degree: The current temperature.</p>	Critical
<p>Event description: Temperature recovers to normal.</p> <p>Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal</p> <p>Parameters description:</p> <p> unitID: The unit ID.</p> <p> thermal-sensor-descr: The sensor ID and position.</p>	Critical
<p>Event description: Power failed.</p> <p>Log Message: Unit <unit-id> <power-descr> failed</p> <p>Parameters description:</p> <p> unitID: The unit ID.</p> <p> power-descr: The power position and ID.</p>	Critical
<p>Event description: Power is recovered.</p> <p>Log Message: Unit <unit-id> <power-descr> back to normal</p> <p>Parameters description:</p> <p> unitID: The unit ID.</p> <p> power-descr: The power position and ID.</p>	Critical
<p>Event description: Air flow abnormal.</p> <p>Log Message: Unit <unit-id> detecting abnormal air flow.</p> <p>Parameters description:</p> <p> unitID: The unit ID.</p>	Critical
<p>Event description: Air flow recovered.</p> <p>Log Message: Unit <unit-id> abnormal air flow back to normal.</p> <p>Parameters description:</p> <p> unitID: The unit ID.</p>	Critical

Port Security

Log Description	Severity
Event description: Address full on a port Log Message: MAC address <macaddr> causes port security violation on <interface-id> Parameters description: macaddr: The violation MAC address. interface-id: The interface name.	Warning
Event description: Address full on system Log Message: Limit on system entry number has been exceeded.	Warning

RIPng

Log Description	Severity
Event description: The RIPng state of interface changed Log Message: RIPng-6-INTFSTATECHANGE :RIPng protocol on interface <intf-name> changed state to <enabled disabled> Parameters description: intf-name: Interface name.	Informational

Safeguard

Log Description	Severity
Event description: When the CPU utilization is over the rising threshold, the switch enters exhausted mode. Log Message: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode. Parameters description: unit-id: the unit ID	Warning
Event description: When the CPU utilization is lower than the falling threshold, the switch enters normal mode. Log Message: Unit <unit-id>, Safeguard Engine enters NORMAL mode. Parameters description: unit_id: the unit ID.	Informational

SNMP

Log Description	Severity
Event Description: SNMP request received with invalid community string Log Message: SNMP request received from <ipaddr> with invalid community string. Parameters Description: ipaddr: The IP address.	Informational

SSH

Log Description	Severity
Event description: SSH server is enabled. Log Message: SSH server is enabled	Informational
Event description: SSH server is disabled. Log Message: SSH server is disabled	Informational
Event description: This log will be generated when SSH log failed (not via AAA method). Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr ipv6address>). Parameters description: username: User name which logs in fail. ipaddr: IP address of host from which the user logged in. ipv6address: IPv6 address of host from which the user logged in.	Critical

Stacking

Log Description	Severity
Event description: Hot insertion. Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion. Parameters description: unitID: Box ID. macaddr: MAC address.	Informational
Event description: Hot removal. Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal. Parameters description: unitID: Box ID. macaddr: MAC address.	Informational
Event description: Stacking topology change. Log Message: Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>). Parameters description: Stack_TP_TYPE: The stacking topology type is one of the following: 1. Ring, 2. Chain. unitID: Box ID. macaddr: MAC address.	Informational
Event description: Backup master changed to master. Log Message: Backup master changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
Event description: Slave changed to master Log Message: Slave changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational

Event description: Box ID conflict.	Critical
Log Message: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>).	
Parameters description: unitID: Box ID. macaddr: The MAC addresses of the conflicting boxes.	

Traffic Control

Log Description	Severity
Event description: Broadcast storm occurrence. Log Message: <interface-id> Broadcast storm is occurring. Parameters description: interface-id: The interface name.	Warning
Event description: Broadcast storm cleared. Log Message: <interface-id> Broadcast storm has cleared. Parameters description: interface-id: The interface name.	Informational
Event description: Multicast storm occurrence. Log Message: <interface-id> Multicast storm is occurring. Parameters description: interface-id: The interface name.	Warning
Event description: Multicast Storm cleared. Log Message: <interface-id>Multicast storm has cleared. Parameters description: interface-id: The interface name.	Informational
Event description: Storm us ocured. Log Message: <Broadcast Multicast Unicast> storm is occurring on <interface-id>. Parameters description: Broadcast: Storm is resulted by broadcast packets(DA = FF:FF:FF:FF:FF:FF). Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast and known IP multicast. Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets interface-id: The interface ID on which a storm is occurring.	Warning
Event description: Storm is cleared. Log Message: <Broadcast Multicast Unicast> storm is cleared on <interface-id>. Parameters description: Broadcast: Broadcast storm is cleared. Multicast: Multicast storm is cleared. Unicast: Unicast storm (including both known and unknown unicast packets) is cleared. interface-id: The interface ID on which a storm is cleared.	Informational
Event description: Port shut down due to a packet storm	Warning

Log Message: <interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm.

Parameters description:

interface-id: The interface name.

Broadcast: The interface is disabled by broadcast storm.

Multicast: The interface is disabled by multicast storm.

Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).

VPLS

Log Description	Severity
Event description: VPLS link up Log Message: VPLS <vpls_name> link up Parameters description: vpls_name: The name of the link up VPLS	Informational
Event description: VPLS link down Log Message: VPLS <vpls_name> link down Parameters description: vpls_name: The name of the link down VPLS	Informational

VPWS

Log Description	Severity
Event description: Pseudo-wire link down Log Message: Pseudo-wire id <vc_id> peer ip <ipaddr> link down Parameters description: vc_id: The link down Pseudo-wire ID ipaddr: The peer IP address of the link down Pseudo-wire	Informational
Event description: Pseudo-wire link up Log Message: Pseudo-wire id <vc_id> peer ip <ipaddr> link up Parameters description: vc_id: The link up Pseudo-wire ID ipaddr: The peer IP address of the link up Pseudo-wire	Informational
Event description: Pseudo-wire is deleted Log Message: Pseudo-wire id <vc_id> peer ip <ipaddr> is deleted Parameters description: vc_id: The deleted Pseudo-wire ID ipaddr: The peer IP address of the deleted Pseudo-wire	Informational
Event description: Pseudo-wire link standby Log Message: Pseudo-wire id <vc_id> peer ip <ipaddr> link standby Parameters description: vc_id: The link standby Pseudo-wire ID ipaddr: The peer IP address of the link standby Pseudo-wire	Informational

VRRP Debug Enhancement

Log Description	Severity
<p>Event description: One virtual router state becomes Master.</p> <p>Log Message: VRRP-6-STATEMASTER:VR <vr-id> at interface <intf-name> switch to Master</p> <p>Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.</p>	Informational
<p>Event description: One virtual router state becomes Backup.</p> <p>Log Message: VRRP-6-STATEBACKUP: VR <vr-id> at interface <intf-name> switch to Backup</p> <p>Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.</p>	Informational
<p>Event description: One virtual router state becomes Init.</p> <p>Log Message: VRRP-6-STATEINIT: VR <vr-id> at interface <intf-name> switch to Init</p> <p>Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.</p>	Informational
<p>Event description: Authentication type mismatch of one received VRRP advertisement message.</p> <p>Log Message: VRRP-4-AUTHTYPEMIS:Authentication type mismatch on VR <vr-id> at interface <intf-name></p> <p>Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.</p>	Warning
<p>Event description: Authentication checking fail of one received VRRP advertisement message.</p> <p>Log Message: VRRP-4-AUTHFAIL: Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type></p> <p>Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based. Auth-type: VRRP interface authentication type.</p>	Warning
<p>Event description: Checksum error of one received VRRP advertisement message.</p> <p>Log Message: VRRP-4-BADCHK:Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name></p> <p>Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.</p>	Warning
<p>Event description: Virtual router ID mismatch of one received VRRP advertisement message.</p> <p>Log Message: VRRP-4-VRIDMIS: Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name></p> <p>Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.</p>	Warning

<p>Event description: Advertisement interval mismatch of one received VRRP advertisement message.</p> <p>Log Message: VRRP-4-ADVMIS: Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name></p> <p>Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.</p>	Warning
<p>Event description: A virtual MAC address is added into switch L2 table</p> <p>Log Message: VRRP-5-MACADD: Added a virtual MAC <vrrp-mac-addr> into L2 table</p> <p>Parameters description: vrrp-mac-addr: VRRP virtual MAC address</p>	Notice
<p>Event description: A virtual MAC address is deleted from switch L2 table.</p> <p>Log Message: VRRP-5-MACDEL: Deleted a virtual MAC <vrrp-mac-addr> from L2 table</p> <p>Parameters description: vrrp-mac-addr: VRRP virtual MAC address</p>	Notice
<p>Event description: A virtual MAC address is adding into switch L3 table.</p> <p>Log Message: VRRP-5-MACL3ADD: Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table</p> <p>Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address</p>	Notice
<p>Event description: A virtual MAC address is deleting from switch L3 table.</p> <p>Log Message: VRRP-5-MACL3DEL: Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table</p> <p>Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address</p>	Notice
<p>Event description: Failed when adding a virtual MAC into switch chip L2 table.</p> <p>Log Message: VRRP-3-MACADDFAIL:Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode></p> <p>Parameters description: vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Errcode of VRRP protocol behavior.</p>	Error
<p>Event description: Failed when deleting a virtual MAC from switch chip L2 table.</p> <p>Log Message: VRRP-3-MACDELFAIL:Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode></p> <p>Parameters description: vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Errcode of VRRP protocol behaviour.</p>	Error
<p>Event description: Failed when adding a virtual MAC into switch L3 table. The L3 table is full.</p> <p>Log Message: VRRP-3-MACL3FULL: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full</p> <p>Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address</p>	Error

<p>Event description: Failed when adding a virtual MAC into switch L3 table. The port where the MAC is learned from is invalid.</p> <p>Log Message: VRRP-3-BADMAC: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-port: port number of VRRP virtual MAC. 	Error
<p>Event description: Failed when adding a virtual MAC into switch L3 table. The interface where the MAC is learned from is invalid.</p> <p>Log Message: VRRP-3-BADINTF: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-intf: interface id on which VRRP virtual MAC address is based. 	Error
<p>Event description: Failed when adding a virtual MAC into switch L3 table. The box where the MAC is learned from is invalid.</p> <p>Log Message: VRRP-3-BADUNIT: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid</p> <p>Parameters description:</p> <ul style="list-style-type: none"> vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-box: stacking box number of VRRP virtual MAC. 	Error
<p>Event description: Failed when adding a virtual MAC into switch chip's L3 table.</p> <p>Log Message: VRRP-3-MACL3ADDFAIL: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode></p> <p>Parameters description:</p> <ul style="list-style-type: none"> vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Err code of VRRP protocol behavior. 	Error
<p>Event description: Failed when deleting a virtual MAC from switch chip's L3 table.</p> <p>Log Message: VRRP-3-MACL3DELFAIL: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode></p> <p>Parameters description:</p> <ul style="list-style-type: none"> vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Err code of VRRP protocol behavior. 	Error

Web

Log Description	Severity
<p>Event description: Successful login through Web.</p> <p>Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>).</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client. 	Informational

Event description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning
Event description: Web session timed out. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event description: Logout through Web. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event description: Successful login through Web (SSL). Log Message: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event description: Login failed through Web (SSL). Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Warning
Event description: Web (SSL) session timed out. Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event description: Logout through Web(SSL). Log Message: Logout through Web(SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Informational

Web-Authentication

Log Description	Severity
Event description: The log message occurs when a host passed the authentication. Log Message: Web-Authentication host login success (Username: <username>, IP: <ipaddr >, MAC: <mac-address>, <interface-id>, VID: <vlan-id>). Parameters description:	Informational

username: The host username.
ipaddr: The host IP address, either an IPv4 or IPv6 address.
mac-address: The host MAC addresses.
interface-id: The interface on which the host is authenticated.
vlan-id: The VLAN ID on which the host exists.

Event description: The log message occurs when a host failed to pass the authentication. Critical

Log Message: Web-Authentication host login fail (Username: <username>, IP: <ipaddr >, MAC: <mac-address>, <interface-id>, VID: <vlan-id>).

Parameters description:

username: The host username.
ipaddr: The host IP address, either an IPv4 or IPv6 address.
mac-address: The host MAC addresses.
interface-id: The interface on which the host is authenticated.
vlan-id: The VLAN ID on which the host exists.

Appendix C - Trap Entries

The following table lists all possible trap log entries and their corresponding meanings that will appear in the switch.

Authentication Fail

Trap Name	Description	OID
authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5

CFM

Trap Name	Description	OID
dot1agCfmFaultAlarm	This trap is initiated when a connectivity defect is detected. Binding objects: (1) dot1agCfmMepHighestPrDefect	1.3.111.2.802.1.1.8.0.1

CFM Extension

Trap Name	Description	OID
swCFMExtAISOccurred	A notification is generated when local MEP enters AIS status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.17.1.12.86.100.0.1
swCFMExtAISCleared	A notification is generated when local MEP exits AIS status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.17.1.12.86.100.0.2
swCFMExtLockOccurred	A notification is generated when local MEP enters lock status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.17.1.12.86.100.0.3
swCFMExtLockCleared	A notification is generated when local MEP exits lock status.	1.3.6.1.4.1.17.1.12.86.100.0

Binding objects:	.4
(1) dot1agCfmMdIndex	
(2) dot1agCfmMaIndex	
(3) dot1agCfmMeplIdentifier	

LACP

Trap Name	Description	OID
linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3

LDP

Trap Name	Description	OID
mplsLdpInitSessionThresholdExceeded	This notification is generated when the backoff is enabled, and the number of Session Initialization messages exceeds the value of the 'mplsLdpEntityInitSessionThreshold'	1.3.6.1.2.1.10.166.4.0.1
mplsLdpPathVectorLimitMismatch	This notification is sent when the 'mplsLdpEntityPathVectorLimit' does NOT match the value of the 'mplsLdpPeerPathVectorLimit' for a specific Entity.	1.3.6.1.2.1.10.166.4.0.2
mplsLdpSessionUp	If this notification is sent when the value of 'mplsLdpSessionState' enters the 'operational(5)' state	1.3.6.1.2.1.10.166.4.0.3
mplsLdpSessionDown	This notification is sent when the value of 'mplsLdpSessionState' leaves the 'operational(5)' state	1.3.6.1.2.1.10.166.4.0.4

LLDP

Trap Name	Description	OID
IldpRemTablesChange	A IldpRemTablesChange notification is sent when the value of IldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Binding 1. IldpStatsRemTablesInserts 2. IldpStatsRemTablesDeletes 3. IldpStatsRemTablesDrops 4. IldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
IldpXMedTopologyChangeDetected	A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding 1. IldpRemChassisIdSubtype 2. IldpRemChassisId 3. IldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1

MPLS

Trap Name	Description	OID
mplsXCUp	This notification is generated when the mplsXCOperStatus object for one or more contiguous entries in the mplsXCTable is about to enter the up state from another state.	1.3.6.1.2.1.10.166.2.0.1
mplsXCDown	This notification is generated when the mplsXCOperStatus object for one or more contiguous entries in the mplsXCTable is about to enter the up state from another state.	1.3.6.1.2.1.10.166.2.0.2

MSTP

Trap Name	Description	OID
newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.2

Port

Trap Name	Description	OID
-----------	-------------	-----

linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1. 1.5.4
linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1. 1.5.3

RMON

Trap Name	Description	OID
risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1)alarmIndex (2)alarmVariable (3)alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16 .0.1
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1)alarmIndex (2) alarmVariable (3)alarmSampleType (4)alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16 .0.2

Start

Trap Name	Description	OID
coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1. 1.5.1
warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1. 1.5.2

VPWS

Trap Name	Description	OID
-----------	-------------	-----

pwDown	This notification is generated when the pwOperStatus object for one or more contiguous entries in the pwTable which are about to enter the down(2) or lowerLayerDown(6) state from any other state, except for transition from the notPresent(5) state.	1.3.6.1.2.1.10 .246.0.1
pwUp	This notification is generated when the pwOperStatus object for one or more contiguous entries in the pwTable which are about to enter the up(1) state from some other state except the notPresent(5) state and given that the pwDown notification issued for these entries.	1.3.6.1.2.1.10 .246.0.2
pwDeleted	This notification is generated when the PW has been deleted, i.e., when the pwRowStatus has been set destroy(6) or the PW has been deleted by a non-MIB application or due to an auto-discovery process.	1.3.6.1.2.1.10 .246.0.3

VRRP

Trap Name	Description	OID
vrrpTrapNewMaster	The newMaster trap indicates that the sending agent has transitioned to 'Master' state. Binding objects: (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.68 .0.1
vrrpTrapAuthFailure	A vrrpAuthFailure trap signifies that a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional. Binding objects: (1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	1.3.6.1.2.1.68 .0.2

Appendix D - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the DXS-3600 is used in the following modules: Console, Telnet, SSH, Web, 802.1X, MAC-based Access Control, and WAC.

The description that follows explains the following RADIUS Attributes Assignment types:

- Privilege Level
- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign the **Privilege Level** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for the bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	1	Required
Attribute-Specific Field	Used to assign the privilege level of the user to operate the switch.	Range (1-15)	Required

If the user has configured the privilege level attribute of the RADIUS server (for example, level 15) and the Console, Telnet, SSH, and Web authentication is successful, the device will assign the privilege level (according to the RADIUS server) to this access user. However, if the user does not configure the privilege level attribute and authenticates successfully, the device will not assign any privilege level to the access user. If the privilege level is configured less than the minimum supported value or greater than the maximum supported value, the privilege level will be ignored.

To assign the **Ingress/Egress Bandwidth** by the RADIUS server, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and

authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of "0", the effective bandwidth will be set "no_limited", and if the bandwidth is configured less than "0" or greater than maximum supported value, the bandwidth will be ignored.

To assign the **802.1p Default Priority** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0 to 7	Required

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or MAC based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign the **VLAN** by the RADIUS server, the proper parameters should be configured on the RADIUS server. To use VLAN assignment, RFC 3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      | Length |      Tag      | String...
+-----+-----+-----+-----+-----+-----+-----+

```

The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format
0x01	VLAN name (ASCII)
0x02	VLAN ID (ASCII)
Others (0x00, 0x03 ~ 0x1F, >0x1F)	When the switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the switch will check all existing VLAN IDs and check if there is one matched. If the switch can find one matched, it will move to that VLAN. If the switch cannot find the matched VLAN ID, it will think the VLAN setting string as a "VLAN Name". Then it will check that it can find out a matched VLAN Name.

Note: A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC based Access Control, or WAC authentication is successful, the port will be assigned to VLAN 3. However if the user does not configure the VLAN attributes, when the port is not guest VLAN member, it will be kept in its current authentication VLAN, and when the port is guest VLAN member, it will be assigned to its original VLAN.

To assign the **ACL** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for an ACL.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	14 (for ACL script)	Required
Attribute-Specific Field	Used to assign the ACL script. The format is based on Access Control List (ACL) Commands .	ACL Script For example: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL script: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;), and the 802.1X or MAC-based Access Control WAC is successful, the device will assign the ACL script according to the RADIUS server. The enter **Access-List Configuration Mode** and exit **Access-List Configuration Mode** must be a pair, otherwise the ACP script will be reject. For more information about the ACL module, please refer to **Access Control List (ACL) Commands** chapter.

Appendix E - IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, information and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute. For more information about D-Link VSA, refer to the **RADIUS Attributes Assignment** Appendix.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF RADIUS attributes supported by the D-Link switch.

RADIUS Authentication Attributes:

Number	IETF Attribute
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message

80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address

RADIUS Accounting Attributes:

Number	IETF Attribute
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address