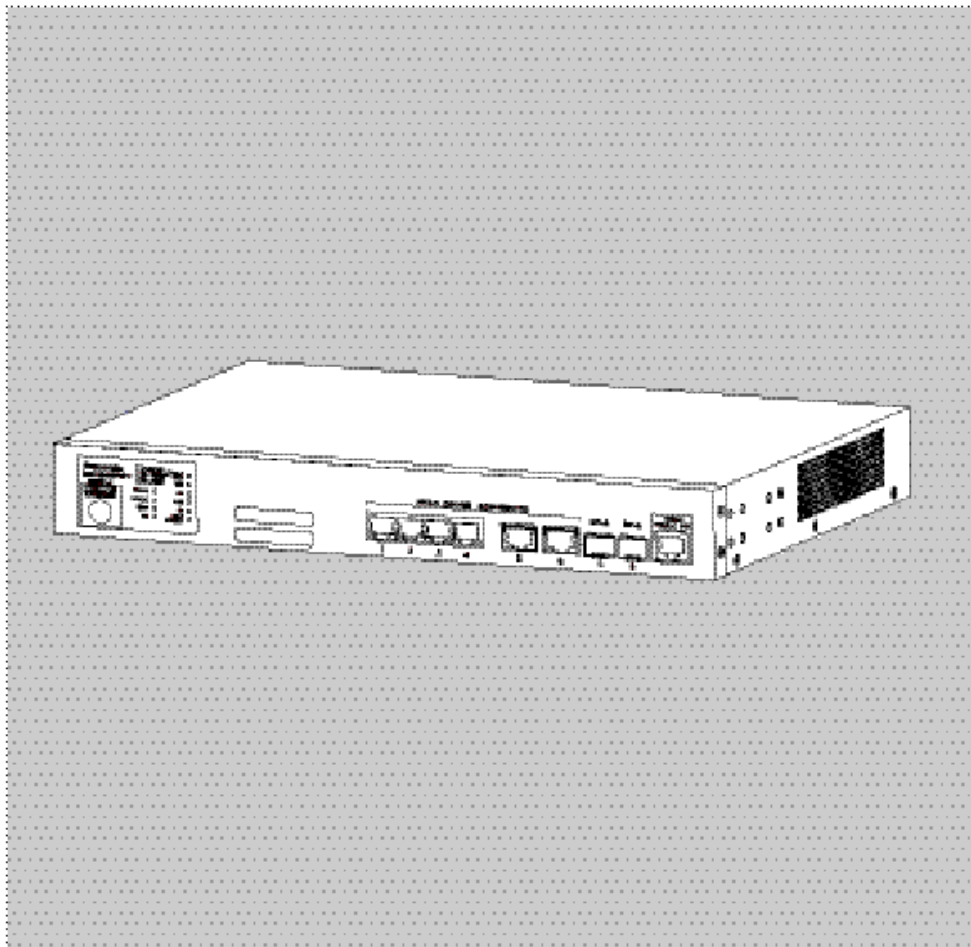




PoE Power Supply Switching Hub

WEB Reference

Model Number PN290496



The target model for this reference is as follows.

Model Name	Model Number	Firmware Version
MGA-ML4TWPoE++	PN290496	1.0.1.00 or higher

Regarding the function compatible with each model, see its specification.

Table of Contents

1 Introduction	9
2 (Reserve)	10
3 System	11
3.1 Device Information	11
3.2 System Information Settings	12
3.3 Peripheral Settings	13
3.4 Port Settings	14
3.4.1 Port Settings	14
3.4.2 Port Status	17
3.4.3 Port GBIC	18
3.4.4 Port Auto Negotiation	19
3.4.5 Error Disable Settings	20
3.4.6 Jumbo Frame	21
3.5 PoE Settings	22
3.5.1 PoE Global Settings	22
3.5.2 PoE Port Settings	24
3.5.3 PoE Schedule Port List Settings	25
3.5.4 PoE Schedule Date List Settings	26
3.5.5 PoE Schedule Settings	27
3.5.6 PoE Schedule Port Configuration	28
3.5.7 PoE LLDP Auto Reboot Settings	29
3.5.8 PoE Ping Auto Reboot Settings	30
3.5.9 PoE Traffic Auto Reboot Settings	31
3.5.10 PoE Auto Reboot SMTP Settings	32
3.5.11 PoE Interface Auto Reboot Settings	33
3.6 System Log	34
3.6.1 System Log Settings	34
3.6.2 System Log Discriminator Settings	37
3.6.3 System Log Server Settings	38
3.6.4 System Log	40
3.6.5 System Attack Log	41
3.6.6 System Authentication Log	42
3.7 Time and SNTP (Simple Network Time Protocol)	43
3.7.1 Clock Settings	43
3.7.2 Time Zone Settings	44
3.7.3 SNTP Settings	46
3.8 Time Range	47
4 Management	49
4.1 Command Logging	49
4.2 User Accounts Settings	50
4.3 User Accounts Encryption	51
4.4 Login Method	52
4.5 SNMP (Simple Network Management Protocol)	54
4.5.1 SNMP Global Settings	54
4.5.2 SNMP Linkchange Trap Settings	56
4.5.3 SNMP View Table Settings	57

4.5.4 SNMP Community Table Settings	58
4.5.5 SNMP Group Table Settings	60
4.5.6 SNMP Engine ID Local Settings	62
4.5.7 SNMP User Table Settings	63
4.5.8 SNMP Host Table Settings	66
4.6 RMON (Remote Monitoring)	68
4.6.1 RMON Global Settings	68
4.6.2 RMON Statistics Settings	69
4.6.3 RMON History Settings	71
4.6.4 RMON Alarm Settings	73
4.6.5 RMON Event Settings	74
4.7 Telnet/Web	76
4.8 Session Time-out	77
4.9 DHCP Auto Configuration	78
4.10 DNS (Domain Name System)	79
4.10.1 DNS Global Settings	79
4.10.2 DNS Name Server Settings	80
4.10.3 DNS Host Settings	81
4.11 File System	82
4.12 SMTP Settings	84
4.13 NLB FDB Settings	86
4.14 IP Setup	87
4.3.1 IP Setup Protocol Settings	87
5 L2 Features	88
5.1 FDB (Forwarding Database)	88
5.1.1 Static FDB	88
5.1.1.1 Unicast Static FDB	88
5.1.1.2 Multicast Static FDB	90
5.1.2 MAC Address Table Settings	91
5.1.3 MAC Address Table	94
5.1.4 MAC Notification	96
5.2 VLAN (Virtual Local Area Network)	98
5.2.1 802.1Q VLAN	98
5.2.2 802.1v Protocol VLAN	100
5.2.2.1 Protocol VLAN Profile	100
5.2.2.2 Protocol VLAN Profile Interface	102
5.2.3 GVRP	103
5.2.3.1 GVRP Global	103
5.2.3.2 GVRP Port	104
5.2.3.3 GVRP Advertise VLAN	105
5.2.3.4 GVRP Forbidden VLAN	106
5.2.3.5 GVRP Statistics Table	107
5.2.4 Asymmetric VLAN	108
5.2.5 MAC VLAN	109
5.2.6 VLAN Interface	110
5.2.7 Subnet VLAN	115
5.2.8 Voice VLAN	116
5.2.8.1 Voice VLAN Global	116
5.2.8.2 Voice VLAN Port	118
5.2.8.3 Voice VLAN OUI	120
5.2.8.4 Voice LAN Device	121
5.2.8.5 Voice VLAN LLDP-MED Device	122

5.2.9 Private VLAN	123
5.3 STP (Spanning Tree Protocol)	126
5.3.1 STP Global Settings	126
5.3.2 STP Port Settings	129
5.3.3 MST Configuration Identification	131
5.3.4 STP Instance	133
5.3.5 MSTP Port Information	134
5.4 Loop Detection Configuration	135
5.4.1 Detecting and Blocking the Loop Settings	135
5.4.2 Loop History Log	136
5.5 Link Aggregation	137
5.6 L2 Protocol Tunnel	139
5.7 L2 Multicast Control	142
5.7.1 IGMP Snooping	142
5.7.1.1 IGMP Snooping Settings	142
5.7.1.2 IGMP Snooping Group Settings	145
5.7.1.3 IGMP Snooping Filter Settings	147
5.7.1.4 IGMP Snooping Multicast Router Information	151
5.7.1.5 IGMP Snooping Statistics Settings	153
5.7.2 MLD Snooping	155
5.7.2.1 MLD Snooping Settings	155
5.7.2.2 MLD Snooping Group Settings	159
5.7.2.3 MLD Snooping Filter Settings	161
5.7.2.4 MLD Snooping Multicast Router Information	164
5.7.2.5 MLD Snooping Statistics Settings	166
5.7.3 Multicast Filtering Mode	168
5.8 LLDP (Link Layer Discovery Protocol)	169
5.8.1 LLDP Global Settings	169
5.8.2 LLDP Port Settings	171
5.8.3 LLDP Management Address List	173
5.8.4 LLDP Basic TLVs Settings	174
5.8.5 LLDP Dot1 TLV Settings	175
5.8.6 LLDP Dot3 TLV Settings	176
5.8.7 LLDP-MED Port Settings	177
5.8.8 LLDP Statistics Information	178
5.8.9 LLDP Local Port Information	179
5.8.10 LLDP Neighbor Port Information	181
5.9 UDLD (Unidirectional Link Detection)	182
5.10 RRP (Ring Redundant Protocol)	183
6 L3 Features	186
6.1 ARP (Address Resolution Protocol)	186
6.1.1 ARP Aging Time	186
6.1.2 Static ARP	187
6.1.3 ARP Table	189
6.2 Gratuitous ARP	190
6.3 IPv6 Neighbor	192
6.4 Interface	193
6.4.1 IPv4 Interface	193
6.4.2 IPv6 Interface	197
6.5 IPv4 Default Route	202
6.6 IPv6 Default Route	203
6.7 IPv6 General Prefix	204

7 QoS (Quality of Service)	205
7.1 Basic Settings	205
7.1.1 Port Default CoS	205
7.1.2 Port Scheduler Method	206
7.1.3 Queue Settings	208
7.1.4 CoS to Queue Mapping	209
7.1.5 Port Rate Limiting	210
7.1.6 Queue Rate Limiting	212
7.2 Advanced Settings	214
7.2.1 DSCP Mutation Map	214
7.2.2 Port Trust State and Mutation Binding	215
7.2.3 DSCP CoS Mapping	216
7.2.4 CoS Color Mapping	217
7.2.5 DSCP Color Mapping	218
7.2.6 Class Map	219
7.2.7 Aggregate Policer	221
7.2.8 Policy Map	227
7.2.9 Policy Binding	235
8 ACL (Access Control List)	236
8.1 ACL Configuration Wizard	236
8.1.1 MAC ACL	238
8.1.2 IPv4	241
8.1.3 IPv6	246
8.2 ACL Access List	251
8.2.1 Standard IP ACL	253
8.2.2 Extended IP ACL	256
8.2.3 Standard IPv6 ACL	261
8.2.4 Extended IPv6 ACL	264
8.2.5 Extended MAC ACL	269
8.2.6 Extended Expert ACL	272
8.3 ACL Interface Access Group	278
8.4 ACL VLAN Access Map	280
8.5 ACL VLAN Filter	283
9 Security	284
9.1 Port Security	284
9.1.1 Port Security Global Settings	284
9.1.2 Port Security Port Settings	286
9.1.3 Port Security Address Entries	288
9.2 802.1X	289
9.2.1 802.1X Global Settings	289
9.2.2 802.1X Forced Authorized MAC Settings	291
9.2.3 802.1X Unauthorized MAC Settings	292
9.2.4 802.1X Ports Settings	293
9.2.5 EAP Port Config	298
9.2.6 802.1X Authenticator Statistics Information	299
9.2.7 802.1X Supplicant Global Settings	300
9.2.8 802.1X Supplicant Port Settings	301
9.2.9 802.1X Supplicant Statistics Information	303
9.3 AAA (Authentication, Authorization, and Accounting)	304
9.3.1 AAA Global Settings	304

9.3.2 AAA Authentication Settings	305
9.3.3 AAA Authentication User Settings	308
9.3.4 AAA Authentication MAC Settings	310
9.3.5 Application Authentication Settings	312
9.3.6 Application Accounting Settings	313
9.3.7 Authentication EXEC Settings	315
9.3.8 Accounting Settings	317
9.4 Authentication	320
9.4.1 Authentication Dynamic VLAN Settings	320
9.4.2 Authentication Status Table	321
9.4.3 2-Step Authentication Settings	322
9.5 RADIUS (Remote Authentication Dial-In User Service)	323
9.5.1 RADIUS Global Settings	323
9.5.2 RADIUS Server Settings	325
9.5.3 RADIUS Group Server Settings	326
9.5.4 RADIUS Statistic	328
9.6 TACACS+ (Terminal Access Controller Access-Control System Plus)	329
9.6.1 TACACS+ Global Settings	329
9.6.2 TACACS+ Group Server Settings	330
9.6.3 TACACS+ Statistic	332
9.7 SAVI (Source Address Validation Improvements)	333
9.7.1 IPv4	333
9.7.1.1 DHCPv4 Snooping	333
9.7.1.1.1 DHCP Snooping Global Settings	333
9.7.1.1.2 DHCP Snooping Port Settings	334
9.7.1.1.3 DHCP Snooping VLAN Settings	335
9.7.1.1.4 DHCP Snooping Database	336
9.7.1.1.5 DHCP Snooping Binding Entry	338
9.7.1.2 Dynamic ARP Inspection	339
9.7.1.2.1 ARP Access List	339
9.7.1.2.2 ARP Inspection Settings	341
9.7.1.2.3 ARP Inspection Port Settings	344
9.7.1.2.4 ARP Inspection Statistics Information	345
9.7.1.2.5 ARP Inspection Log	346
9.7.1.3 IP Source Guard	347
9.7.1.3.1 IP Source Guard Port Settings	347
9.7.1.3.2 IP Source Guard Binding	348
9.7.1.3.3 IP Source Guard HW Entry	350
9.8 DHCP Server Protection	351
9.8.1 Global Settings on Protecting a DHCP Server	351
9.8.2 DHCP Server Protect Global Settings	352
9.8.3 DHCP Server Protect Port Settings	353
9.9 BPDU Guard	354
9.10 NetBIOS Filtering	356
9.11 MAC Authentication	357
9.12 Web Authentication	359
9.12.1 Web Authentication Settings	359
9.12.2 Web Page Contents Settings	360
9.12.3 Temporary DHCP Server Settings	361
9.13 Trusted Host	363
9.14 Traffic Segmentation Settings	364
9.15 Storm Control	365
9.16 SSH (Secure Shell)	369

9.16.1 SSH Global Settings	369
9.16.2 Host Key	370
9.16.3 SSH Server Connection	371
9.16.4 SSH User Settings	372
9.17 SSL (Secure Sockets Layer)	373
9.17.1 SSL Global Settings	373
9.17.2 Crypto PKI Trustpoint	374
9.17.3 SSL Service Policy	375
10 OAM (Operations, Administration & Management)	377
10.1 Cable Diagnostics	377
10.2 DDM (Digital Diagnostic Monitoring)	378
10.2.1 DDM Settings	378
10.2.2 DDM Temperature Threshold Settings	380
10.2.3 DDM Voltage Threshold Settings	381
10.2.4 DDM Bias Current Threshold Settings	382
10.2.5 DDM TX Power Threshold Settings	383
10.2.6 DDM RX Power Threshold Settings	384
10.2.7 DDM Status Table	385
11 Monitoring	386
11.1 Utilization	386
11.1.1 Port Utilization	386
11.2 Statistics	387
11.2.1 Port	387
11.2.2 Interface Counters	389
11.2.3 Counters	391
11.3 Mirror Settings	393
11.4 Device	396
12 ECO Mode	397
12.1 Power-Saving	397
12.2 EEE (Energy Efficient Ethernet)	398
13 Tool Bar	399
13.1 Save	399
13.1.1 Save Configuration	399
13.2 Tool	399
13.2.1 Firmware Upgrade & Backup	399
13.2.1.1 Firmware Upgrade from HTTP (Servers)	399
13.2.1.2 Firmware Upgrade from TFTP	401
13.2.1.3 Firmware Upgrade from FTP Servers	402
13.2.1.4 Firmware Upgrade from RCP	403
13.2.1.5 Firmware Backup to HTTP	404
13.2.1.6 Firmware Backup to TFTP	405
13.2.1.7 Firmware Backup to FTP Servers	406
13.2.1.8 Firmware Backup to RCP	407
13.2.2 Configuration Restore & Backup	408
13.2.2.1 Configuration Restore from HTTP	408
13.2.2.2 Configuration Restore from TFTP	409
13.2.2.3 Configuration Recovery from FTP Servers	410
13.2.2.4 Configuration Restore from RCP	411
13.2.2.5 Configuration Backup to HTTP	412

13.2.2.6 Configuration Backup to TFTP	413
13.2.2.7 Configuration Backup to FTP Servers	414
13.2.2.8 Configuration Backup to RCP	415
13.2.3 Log Backup	416
13.2.3.1 Log Backup to HTTP	416
13.2.3.2 Log-backup to TFTP	417
13.2.3.3 Log Backup to RCP	418
13.2.4 Ping	419
13.2.5 Trace Route	422
13.2.6 Reset	424
13.2.7 Reboot System	425
13.3 Language	426
14.4 Log Out	427
15 Appendix - System Log Entries	428
15.1 802.1X	428
15.2 AAA	429
15.3 ARP	432
15.4 Authentication (2 Steps)	433
15.5 BPDU Guard	435
15.6 Command	436
15.7 Configuration/Firmware	437
15.8 DAD	440
15.9 DDM	441
15.10 Debug Error	442
15.11 DHCPv6 Client	443
15.12 Dynamic ARP	445
15.13 Interface	446
15.14 PoE	447
15.15 PoE Scheduler	448
15.16 PoE Auto Reboot	449
15.17 Verifying IP Source Guard	450
15.18 LLDP-MED	451
15.19 LACP	453
15.20 Detecting Loops	454
15.21 MAC-based Access Control	455
15.22 MSTP Debug Extension	456
15.23 Port Security	458
15.24 RADIUS	459
15.25 RRP	460
15.26 SNMP	461
15.27 System	462
15.28 Telnet	463
15.29 Temperature	464
15.30 Traffic Control	465
15.31 Voice VLAN	466
15.32 WAC	467
15.33 Web	468
16 Appendix - System Trap Entries	469
16.1 BPDU Guard	469
16.2 DDM	470
16.3 DHCP Server Protect	471

16.4 Gratuitous ARP	472
16.5 LLDP-MED	473
16.6 Detecting Loops	474
16.7 MAC Based Access Control	475
16.8 MAC Notification	476
16.9 MSTP	477
16.10 Port Security	478
16.11 Port	479
16.12 RMON	480
16.13 SNMP Authentication	481
16.14 System	482
16.15 Temperature	483
16.16 Traffic Control	484

1 Introduction

The MGA-ML can be programmed using the web.

- To enable the web, you need to program ① and ② using the CLI.
① Assign an IP address to this system. (192.168.0.101 is an example.)
MGA-ML#configure terminal
MGA-ML(config)#interface vlan 1
MGA-ML(config-if)#ip address 192.168.0.101 255.255.255.0
② Enable the http server function.
MGA-ML(config)#ip http server
- To log in to this device, enter the IP address on the web browser, and then enter the user name and password. The default username and password is "manager".



The screenshot shows a web browser window with the title "MGA-ML4TWPoE++". The login form has three input fields: "User Name" with the text "manager", "Password" with masked characters "*****", and "Language" with a dropdown menu showing "English". Below the fields are two buttons: "Login" and "Reset".

- The example settings screens used in this reference may differ from the actual screens.
- Some screens are not described in this reference. It can be used according to the actual screen display.

2 (Reserve)

3 System

3.1 Device Information

Use the following window to display general switch information and utilization (or usage). As you log-into the Web UI of the switch, the window is displayed from the beginning.

Click the **GA-MLxxT** link (in Frame A) to display the following window.

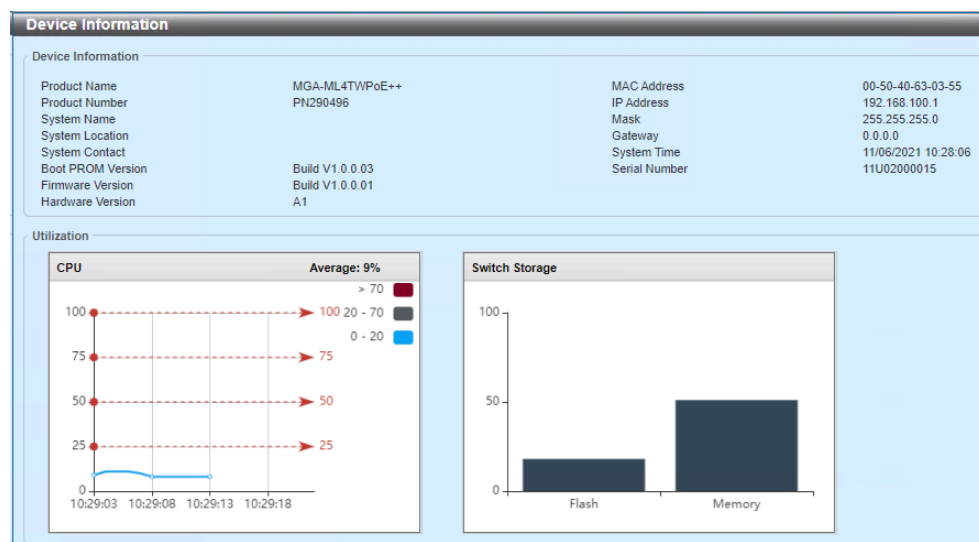


Figure 3-1 Device Information

3.2 System Information Settings

Use the following window to implement the system information settings and display its settings.

Choose **System > System Information Settings** to display the following window.

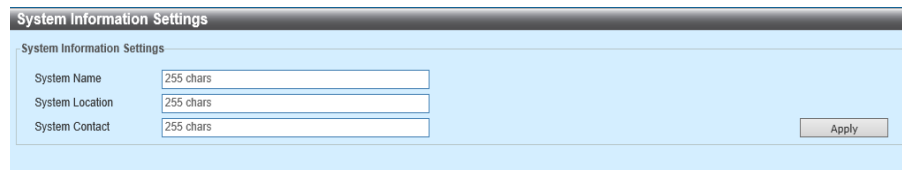


Figure 3-2 System Information Settings

In the section of **System Information Settings**, you can configure the following parameters.

Parameter	Overview
System Name	Enter the system name of a switch. Use the name to identify the switch in the network.
System Location	Enter and describe an overview of the switch location.
System Contact	Enter the name of the PIC for a switch. In general, this means the name of the person or company in charge of configuring and maintaining the switch.

Click **Apply** to reflect the change made.

3.3 Peripheral Settings

Use the following window to configure and display the peripheral settings.

Choose **System > Peripheral Settings** to display the following window.

Port Status								
Port Status								
Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
Fi1/0/1	Connected	00-50-40-63-03-56	1	OFF	OFF	Auto-Full	Auto-1000M	5GBASE-T
Fi1/0/2	Not-Connected	00-50-40-63-03-57	1	OFF	OFF	Auto	Auto	5GBASE-T
Fi1/0/3	Not-Connected	00-50-40-63-03-58	1	OFF	OFF	Auto	Auto	5GBASE-T
Fi1/0/4	Not-Connected	00-50-40-63-03-59	1	OFF	OFF	Auto	Auto	5GBASE-T
Te1/0/5(c)	Not-Connected	00-50-40-63-03-5A	1	OFF	OFF	Auto	Auto	10GBASE-T
Te1/0/5(f)	Not-Connected	00-50-40-63-03-5A	1	OFF	OFF	Auto	Auto	10GBASE-R
Te1/0/6(c)	Not-Connected	00-50-40-63-03-5B	1	OFF	OFF	Auto	Auto	10GBASE-T
Te1/0/6(f)	Not-Connected	00-50-40-63-03-5B	1	OFF	OFF	Auto	Auto	10GBASE-R

Figure 3-3 Peripheral Settings

The following parameters can be configured in the **Environment Temperature Threshold Settings** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Thermal	Select the thermal sensor ID.
High Threshold	Enter the high threshold value of the warning temperature setting. The range is from -100 to 200 degrees Celsius. Tick the Default check box to return to the default value.
Low Threshold	Enter the low threshold value of the warning temperature setting. The range is from -100 to 200 degrees Celsius. Tick the Default check box to return to the default value.

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

3.4 Port Settings

3.4.1 Port Settings

Use the following window, and then implement the port settings on the switch to display its settings.

Choose **System > Port Configuration > Port Settings** to display the following window.

Port	Link Status	Medium	State	MDIX	Flow Control		Duplex	Speed	Description
					Send	Receive			
F11/0/1	Up	Enabled	Enabled	Normal	OFF	OFF	Auto	Auto	
F11/0/2	Down	Enabled	Enabled	Normal	OFF	OFF	Auto	Auto	
F11/0/3	Down	Enabled	Enabled	Normal	OFF	OFF	Auto	Auto	
F11/0/4	Down	Enabled	Enabled	Normal	OFF	OFF	Auto	Auto	
Te1/0/5(C)	Down	Enabled	Enabled	Auto	OFF	OFF	Auto	Auto	
Te1/0/5(F)	Down	Enabled	Enabled	Auto	OFF	OFF	Auto	Auto	
Te1/0/6(C)	Down	Enabled	Enabled	Auto	OFF	OFF	Auto	Auto	
Te1/0/6(F)	Down	Enabled	Enabled	Auto	OFF	OFF	Auto	Auto	

Figure 3-4 Port Settings

In the **Port Settings** section, you can configure the following parameters.

Parameter	Overview
From port - To Port	Choose the port you use.
Selecting a Media	Choose a media type for ports. The options available are Automatic , RJ45 and SFP . SFP stands for Small Form-Factor Pluggable.
Media Type	Choose a media type for ports. The options available are RJ45 and SFP .
State	This parameter enables or disables a physical port.

Parameter	Overview
MDIX	<p>Choose an object of MDIX (Medium Dependent Interface Crossover). The options available are as follows.</p> <ul style="list-style-type: none"> • Auto - This value automatically senses an optimum type of cables. • Normal - Choose this for normal cables. Selecting it makes a port to become the MDIX mode, and that allows a straight-through cable to connect to a PC LAN adapter. Or, employ a cross-over cable to connect it to a port of a different switch (MDI mode). • Cross - Choose this for employing a cross-over cable. Selecting this option allows a port to become the MDI mode, and that allows a straight-cable to connect to a port of the different switch (MDIX mode).
Flow Control	<p>Set the flow control to ON or OFF. On the port where it is set to full duplex, use the flow control of 802.3x, and use the one (of two), which is automatically selected on an Automatic port.</p>
Duplex	<p>Choose the duplex mode you use. The options available are Automatic and Full.</p>
Speed	<p>Choose the option of a port speed. This option allows you to implement the forced settings manually for the connection-speed on the port, which is selected for connecting with the speed specified. If Master Configurations are implemented, you can advertise the functions, which are related to types of duplex communication, the speed and physical layer, on ports. Also, this action determines the relationship between a master and a slave on the joint where two physical layers exist (or contact each other). The relationship is necessary for establishing a timing-control between the two physical layers above. The timing-control is configured on a physical layer of the master by a local source. A loop timing is used for the slave settings. In this case, the timing is obtained from the data stream received from the master. If one connection is set to the master, the other connection must be set to the slave. If other configurations are implemented, the condition of a "link-down" occurs on both ports.</p>

Parameter	Overview
Speed	<p>The following options are available to choose.</p> <ul style="list-style-type: none"> • Automatic - In the case of a copper-port, an auto negotiation starts, and then it allows the speed and flow control to negotiate with its link-partner. In the case of fiber-ports, the auto negotiation starts, and then it allows the clock and full-control to negotiate with its link-partner. • 100M - This value sets to the port speed to 100Mbps, forcefully. This option is available for 100Mbps copper-cable connection, only. • 1000M - This value sets the port speed to 1Gbps, forcefully. This option is available for 1Gbps fiber-connection, only. • 1000M Master - This value sets the port speed to 1Gbps forcefully, and functions as the master, and facilitates the timing of an operation for sending and receiving. This option is available for 1Gbps copper-cable connection, only. • 1000M Slave - This value sets the port speed to 1Gbps forcefully, and also functions as the slave to facilitate the timing of an operation for sending and receiving. This option is only available for 1Gbps copper-cable connection. • 2500M - This value sets the port speed to 2.5Gbps, forcefully. This option is available for 2.5Gbps fiber-connection, only. • 5000M - This value sets the port speed to 5Gbps, forcefully. This option is available for 5Gbps fiber-connection, only. • 10G - This value sets the port speed to 10Gbps, forcefully. This option is available for 10Gbps fiber-connection, only.
Capability Advertised	If you set the Speed to Auto , these functions are advertised during the Auto Negotiation .
Description	Describe an overview of the corresponding ports. The number of characters can be up to 64.

Click **Apply** to reflect the change made.

3.4.2 Port Status

Use the following window to display the physical port-status and settings of the switch.

Choose **System > Port Configuration > Port Status** to display the following window.

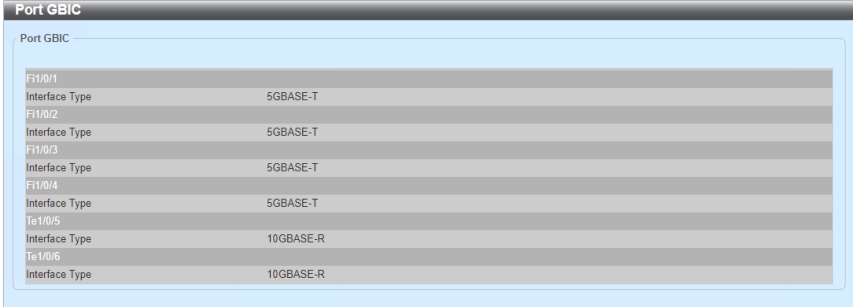
Port Status								
Port Status								
Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
Fi1/0/1	Connected	00-50-40-63-03-56	1	OFF	OFF	Auto-Full	Auto-1000M	5GBASE-T
Fi1/0/2	Connected	00-50-40-63-03-57	1	OFF	OFF	Auto-Full	Auto-1000M	5GBASE-T
Fi1/0/3	Not-Connected	00-50-40-63-03-58	1	OFF	OFF	Auto	Auto	5GBASE-T
Fi1/0/4	Not-Connected	00-50-40-63-03-59	1	OFF	OFF	Auto	Auto	5GBASE-T
Te1/0/5(c)	Not-Connected	00-50-40-63-03-5A	1	OFF	OFF	Auto	Auto	10GBASE-T
Te1/0/5(f)	Not-Connected	00-50-40-63-03-5A	1	OFF	OFF	Auto	Auto	10GBASE-R
Te1/0/6(c)	Not-Connected	00-50-40-63-03-5B	1	OFF	OFF	Auto	Auto	10GBASE-T
Te1/0/6(f)	Not-Connected	00-50-40-63-03-5B	1	OFF	OFF	Auto	Auto	10GBASE-R

Figure 3-5 Port Status

3.4.3 Port GBIC

Use the following window to display the information about the transceiver plugged into a physical port of the switch. GBIC stands for Gigabit Interface Converter.

Choose **System > Port Settings > Port GBIC** to display the following window.



The screenshot shows a window titled "Port GBIC" with a sub-header "Port GBIC". Below this is a table with two columns: "Interface" and "Interface Type". The table lists eight entries, alternating between fiber and copper interfaces.

Interface	Interface Type
Fi1/0/1	5GBASE-T
Fi1/0/2	5GBASE-T
Fi1/0/3	5GBASE-T
Fi1/0/4	5GBASE-T
Te1/0/5	10GBASE-R
Te1/0/6	10GBASE-R

Figure 3-6 Port GBIC

3.4.4 Port Auto Negotiation

Use the following window to display an Auto Negotiation table of a port and its information.

Choose **System > Port Configuration > Port Auto Negotiation** to display the following window.

Port Auto Negotiation								
Port Auto Negotiation								
Note: AN: Auto Negotiation; RS: Remote Signaling; CS: Config Status; CB: Capability Bits; CAB: Capability Advertised Bits; CRB: Capability Received Bits; RFA: Remote Fault Advertised; RFR: Remote Fault Received								
Port	AN	RS	CS	CB	CAB	CRB	RFA	RFR
Fi1/0/1	Enabled	Detected	Complete	100M_Full,...	100M_Full,...	10M_Half, ...	Disabled	NoError
Fi1/0/2	Enabled	Not Detected	Configuring	100M_Full,...	100M_Full,...	-	Disabled	NoError
Fi1/0/3	Enabled	Not Detected	Configuring	100M_Full,...	100M_Full,...	-	Disabled	NoError
Fi1/0/4	Enabled	Not Detected	Configuring	100M_Full,...	100M_Full,...	-	Disabled	NoError
Te1/0/5	Enabled	Not Detected	Configuring	100M_Full,...	100M_Full,...	-	Disabled	NoError
Te1/0/6	Enabled	Not Detected	Configuring	100M_Full,...	100M_Full,...	-	Disabled	NoError

Figure 3-7 Port Auto Negotiation

3.4.5 Error Disable Settings

Use the following window, and then implement the settings on the error disable feature to display its settings.

Choose **System > Port Configuration > Error Disable Settings** to display the following window.

Figure 3-8 Error Disable Settings

In the section of the configuration of **Error Disable Recovery**, you can configure the following parameters.

Parameter	Overview
ErrDisable Cause	Choose the cause of the error-disabled condition. The options available are All , Port Security , Storm Control , BPDU Attack Protection , Dynamic ARP Inspection , DHCP Snooping and L2PT Guard .
Condition	This parameter enables or disables the function of the error-disable recovery.
Interval	Enter the time (seconds) needed for recovering ports from the error condition, which is caused by the module specified; the range is from 5 to 86,400.

Click **Apply** to reflect the change.

3.4.6 Jumbo Frame

Use the following window, and then configure the jumbo frame to display its settings. The jumbo frame is the Ethernet frame, which consists of the payload, and its size is more than 1,518 (bytes).

Choose **System > Port Configuration > Jumbo Frame** to display the following window.

Jumbo Frame

Jumbo Frame

From Port

To Port

Maximum Receive Frame Size (64-9216)

Fi1/0/1

Fi1/0/1

1518 bytes

Apply

Port	Maximum Receive Frame Size (bytes)
Fi1/0/1	1518
Fi1/0/2	1518
Fi1/0/3	1518
Fi1/0/4	1518
Te1/0/5	1518
Te1/0/6	1518

Figure 3-9 Jumbo Frame

In the **Jumbo Frame** section, you can configure the following parameters.

Parameter	Overview
From Port - To Port	Choose the port you use.
Maximum Receive Frame Size	Enter the maximum value of a frame size for receiving. The range is from 64 to 9,216 (bytes). By default, the value is 1,518 (bytes).

Click **Apply** to reflect the change.

3.5 PoE Settings

3.5.1 PoE Global Settings

Use the following window to configure the common settings on a device regarding the PoE.

Choose **System > PoE Settings > PoE Global Settings** to display the following window.

Figure 3-10 PoE Global Settings

In the section of the **PoE Global Settings**, you can configure the following parameters.

Parameter	Overview	
Power Management Method	This parameter displays the method of power-supply if the power supply exceeds the Power Budget . The factory default settings is NextPort .	
	NextPort	Stops the power supply for the port connected right before exceeding the power budget.
	Low Priority	Stops the power-supply of the port whose priority is the lowest. If the priority is the same, the power-supply for the port with the larger port-number becomes stopped.
Threshold for Sending SNMP Traps	Displays the threshold of power supply for sending traps. The factory default settings is 50 (%).	
PoE SNMP Traps	Configures the PoE power-supply traps. The factory default settings is disabled (%).	

Fan Speed	Selects the power-supply and fan-speed, which can be supplied by this device.
------------------	---

Click **Apply** to reflect the change.

3.5.2 PoE Port Settings

Use the following window to implement the settings on the power-supply per port.

Choose **System > PoE > PoE Port Settings** to display the following window.

Port	Admin	Schedule	Status	Layer	Class	Priority	Limit (mW)	Power (mW)	Voltage (V)	Current (mA)
F11/0/1	UP	-	Not Power	-	-	low	Auto	0	0	0
F11/0/2	UP	-	Not Power	-	-	low	Auto	0	0	0
F11/0/3	UP	-	Not Power	-	-	low	Auto	0	0	0
F11/0/4	UP	-	Not Power	-	-	low	Auto	0	0	0

Figure 3-11 PoE Port Settings

In the section of the **PoE Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port - To Port	Select the port to be configured.
Status	Configures to enable or disable the power-supply of the port. The options (or numbers) available are Enable , and the table is Up , and Disable indicates Down . The factory default settings is Up .
Power Limit (1000- 95000)	Configures the upper limit of the power-supply. The factory default settings is Auto .
Priority	Configures the priority of the power-supply. The options available are Crit. , High and Low . The factory default settings is Low .

Click **Apply** to reflect the change.

3.5.3 PoE Schedule Port List Settings

Use the following window to display the settings information regarding the PoE schedulee port-list.

Choose **System > PoE Settings > PoE Scheduler Port List Settings** to display the following window.

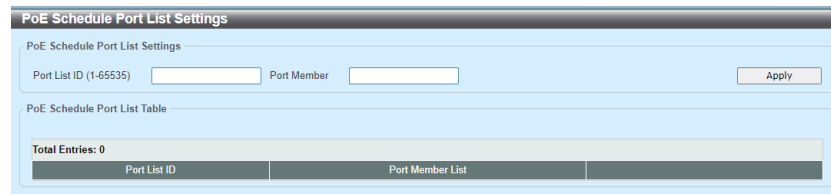


Figure 3-12 PoE Scheduler Port List Settings

In the section of **PoE Schedule Settings**, you can configure the following parameter.

Parameter	Overview
Port List ID	Configures the index number of the PoE scheduler port list.
Port Member	Configures the port on which the PoE scheduler operates. Specify the specified range for each port number by separating them with commas (1, 3) or hyphenating (1-4).

Click **Apply** to reflect the change.

3.5.4 PoE Schedule Date List Settings

Use the following window, and then configure the date list of the PoE scheduler to display the information of the date list.

Choose **System > PoE Settings > PoE Schedule Date List Settings** to display the following window.

Figure 3-13 PoE Scheduler Date List Settings

In the section of the **PoE Date List Settings**, you can configure the following parameters.

Parameter	Overview
Date List Number	Configures the index-number of the port-list of the PoE scheduler.
Date List Name	Configures the name of the date list of the PoE Scheduler.
Year (2000-2099)	Configures the year when the date list is executed.
Month Date (MM/DD)	Configures the date when the date list is executed.

Click **Apply** to reflect the change.

3.5.5 PoE Schedule Settings

Use the following window, and then configure the PoE schedule to display the schedule information.

Choose **System > PoE > PoE Schedule Settings** to display the following window.

Figure 3-14 PoE Schedule Settings

In the section of **PoE schedule Settings**, you can configure the following parameters.

Parameter	Overview
PoE Schedule Global Status	Enables or disables the global settings on the PoE schedule.
Schedule Index	Configures the index-number of the PoE scheduler.
Schedule Name	Configures the name of the PoE schedule.
Schedule Classifier	Configures the class of the PoE schedule. The options available are Daily , Weekly , Monthly and Datelist .
Scheduled Time	Configures the time when the PoE schedule is executed.
Port-List Number	Configures the port-list number where the PoE schedule is executed.
PoE Action	Displays the action of the PoE schedule. The options available are OFF-Port , ON-Port and OFF/ON-Port .
Order to Display	Configures the order to display the PoE schedule. The options available are Index and Next Execution Time .

Click **Apply** to reflect the change.

3.5.6 PoE Schedule Port Configuration

Use the following window, and then configure the settings on the port-list of the PoE scheduler to display the port configuration.

Choose **System > PoE Settings > PoE Schedule Port Configuration** to display the following window.

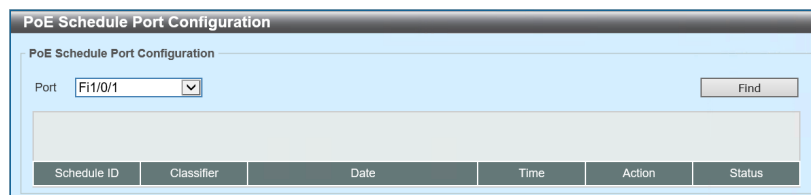


Figure 3-15 PoE Schedule Port Configuration

In the section of the **PoE Schedule Port Configuration**, you can configure the following parameters.

Parameter	Overview
Schedule ID	Index-number of the PoE scheduler.
Classifier	Class of the PoE schedule. The options available are Daily , Weekly , Monthly and Datelist .
Date	Date when the PoE schedule is executed.
Time	Time when the PoE schedule is executed.
Action	Action of the PoE schedule. The options available are OFF-Port , ON-Port and OFF/ON-Port .
Status	Status of PoE Schedule Settings on port. The options available are Enabled and Disabled .

Click **Apply** to reflect the change.

3.5.7 PoE LLDP Auto Reboot Settings

Use the following window, and then implement the settings to monitor the PoE auto-reboot LLDP.

Choose **System > PoE Settings > PoE LLDP Auto Reboot Settings** to display the following window.

PoE LLDP Auto Reboot Global		
LLDP Timeout (1-180)	65	sec <input type="checkbox"/> Default
LLDP Error Retry Times (1-10)	3	<input type="checkbox"/> Default
Apply		
PoE LLDP Auto Reboot Interface		
From Port	To Port	Status
F1/0/1	F1/0/1	Disabled <input type="checkbox"/> Default
Apply		
Port	Status	
F1/0/1	Disabled	
F1/0/2	Disabled	
F1/0/3	Disabled	
F1/0/4	Disabled	

Figure 3-16 PoE LLDP Auto Reboot Settings

In the section of **PoE LLDP Auto Reboot Settings**, you can configure the following parameters.

Parameter	Overview
LLDP Timeout (1- 180)	Configures the time-out with seconds for monitoring the auto-reboot LLDP, which is used for the PoE auto-reboot (factory default settings: 65).
LLDP Error Retry Times (1-10)	Configures the number of retries when monitoring errors of the auto-reboot, which is used for the PoE auto-reboot (factory default settings: 3).
Average Traffics (1-60)	Configures the interval for calculating the average value of traffics existing in the device (factory default settings: 5).
From Port - To Port	The port-number, which configures the PoE auto-reboot LLDP.
Status	Configures to enable or disable to monitor the PoE auto-reboot LLDP.

Click **Apply** to reflect the change.

3.5.8 PoE Ping Auto Reboot Settings

Use the following window to implement the settings for monitoring the PoE ping auto reboot.

Choose **System > PoE > PoE Ping Auto Reboot Settings** to display the following window.

Figure 3-17 PoE Ping Auto Reboot Settings

In the section of **PoE Ping Auto Reboot Settings**, you can configure the following parameters.

Parameter	Overview
Ping Interval	Configures the interval of monitoring Ping, which is used for the PoE auto-reboot (factory default settings: 60).
Ping Time-out (1-30)	Configures the time-out with seconds (as unit) for monitoring Ping, which is used for the PoE auto-reboot (factory default settings: 5).
Ping Error Retry Times (1-10)	Configures the number of retries during the error of monitoring Ping, which is used for the PoE auto-reboot (factory default settings: 3).
From Port/ To Port	Select the range of the port-number.
Ping IP Address	Configures the IP address of the Ping, which is used for the PoE auto-reboot.
Ping IPv6 Address	Configures the IPv6 address of the Ping, which is used for the PoE auto-reboot.

Click **Apply** to reflect the change.

3.5.9 PoE Traffic Auto Reboot Settings

Use the following window to implement the settings on the PoE traffic auto reboot.

Choose **System > PoE Settings > PoE Traffic Auto Reboot Settings** to display the following window.

Figure 3-18 PoE Traffic Auto-reboot Settings

In the section of the **PoE Traffic Auto Reboot Settings**, you can configure the following parameters.

Parameter	Overview
Traffic Interval (1-60)	Configures the interval of monitoring traffics in seconds (factory default setting: 5).
Traffic Error Retry Times (1-10)	Configures the number of retries during traffic errors (factory default setting: 3).
From Port - To Port	Select the range of the port-number.
Condition (of Determining Traffics)	Configures the evaluation of PoE terminal abnormality due to the communication charges. The options available are None , Below and Over .
Threshold (0-5368709119)	Configures the threshold of traffics.

Click **Apply** to reflect the change.

3.5.10 PoE Auto Reboot SMTP Settings

Use the following window to implement the settings on the PoE auto-reboot SMTP.

Choose **System > PoE Settings > PoE Auto Reboot SMTP Settings** to display the following window.

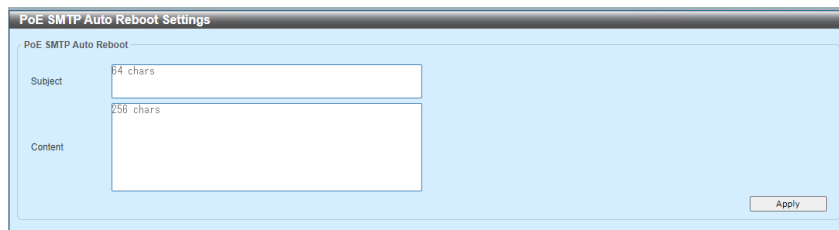


Figure 3-19 PoE Auto-reboot SMTP Settings

In the section of **PoE Auto Reboot SMTP Settings**, you can configure the following parameters.

Parameter	Overview
Subject	Configures the subject when sending the mail notification, which is done by the PoE auto-reboot SMTP.
Content	Configures the content when sending the mail-notification, which is done by the PoE auto-reboot SMTP.

Click **Apply** to reflect the change.

3.5.11 PoE Interface Auto Reboot Settings

Use the following window to implement the settings on **PoE Interface Auto Reboot**.

Choose **System > PoE Settings > PoE Traffic Auto-reboot Interface Settings** to display the following window.

Port	Abnormal Condition	PoE OFF/ON Notify	SMTP Notify	Trap Notify	PoE OFF/ON Interval	PoE OFF/ON Repeat	Repeat Interval
Fi1/0/1	OR	Disabled	Disabled	Disabled	3	Disabled	600
Fi1/0/2	OR	Disabled	Disabled	Disabled	3	Disabled	600
Fi1/0/3	OR	Disabled	Disabled	Disabled	3	Disabled	600
Fi1/0/4	OR	Disabled	Disabled	Disabled	3	Disabled	600

Figure 3-20 PoE Interface Auto Reboot Settings

In the section of **PoE Interface Auto Reboot Settings**, you can configure the following parameters.

Parameter	Overview
From Port - To Port	Select the range of the port-number.
Ping OFF/ON Notification	Configures the condition to evaluate the abnormality regarding the monitoring-method — for example, Ping, LLDP and traffics. The options available are Or and And .
Mail Notification	Configures to enable or disable the SNMP trap settings on the PoE auto-reboot.
SNMP Trap Notification	Enables or disables the SNMP-trap settings on the PoE auto-reboot.
PoE OFF/ON Period	Configures the interval of the PoE power-supply OFF/ON when evaluating the PoE auto-reboot abnormality.
PoE OFF/ON Repeat	PoE auto-reboot enables or disables the repeating execution of the PoE power supply OFF/ON when determining an error.
PoE OFF/ON Repeat Interval	Configures the PoE OFF/ON repeat-interval when evaluating the PoE auto-reboot abnormality.

Click **Apply** to reflect the change.

3.6 System Log

3.6.1 System Log Settings

Use the following window to implement the settings on system logs and display its settings.

Choose **System > System Log > System Log Settings** to display the following window.

Figure 3-21 System Log Settings

In the section of the **Log State**, you can configure the following parameter.

Parameter	Overview
Log State	This parameter enables or disables the status of a global system log.

Click **Apply** to reflect the change.

In the section of **Buffer-log Settings**, you can configure the following parameters.

Parameter	Overview
Buffer Log State	This parameter enables or disables the state of a global buffer-log. The options available are enable, disable and default. If you choose Default , the state of a global buffer log complies with the default operation.

Parameter	Overview
Severity	Choose the severity of the information type to be logged. The values to choose are these: 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Information), and 7 (Debugging).
Identification Name	Enter the identification name you use. The number of characters can be used up to 15. Specify the name of a discriminator profile. Based on the filtering standard stipulated on this profile, buffer-log messages become filtered.
Write Delay	Enter the delay value of a log. The range is from 0 to 65,535 (seconds). By default, the value is set to 300 (seconds). If you click Infinite , the function of write-delay (or delayed writing) becomes disabled.

Click **Apply** to reflect the change.

In the section of the **Console Log** settings, you can configure the following parameters.

Parameter	Overview
Console-log State	This parameter enables or disables the state of a global console-log.
Severity	Choose the severity of the information type, which is logged. The values to choose are these: 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Information) and 7 (Debugging).
Identification Name	Enter the identification name you use. The number of characters can be used up to 15. Specify the name of a discriminator profile. Based on the filtering standard stipulated on this profile, console-log messages become filtered.

Click **Apply** to reflect the change.

In the section of the **SMTP Log** settings, you can configure the following parameters.

Parameter	Overview
SMTP Log State	This parameter enables or disables the log state of a global SMTP (Simple Mail Transfer Protocol).

Parameter	Overview
Severity	Choose the severity of the information type, which is logged. The values to choose are these: 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Information), and 7 (Debugging).
Identification Name	Enter the identification name you use. The number of characters can be used up to 15. Specify the name of a discriminator profile. Based on the filtering standard stipulated on this profile, SMTP log messages become filtered.

Click **Apply** to reflect the change made.

The following parameters can be configured in the **Log Trap Link Change Delay Settings** section:

Parameter	Description
Log Trap Link Change	Enables issuance delays for system logs and SNMP traps related to the link state of physical ports. The range is from 1 to 30 (seconds). When using the link aggregation on your device, if the system logs and SNMP traps regarding the link status of the physical port cannot be normally transmitted to the SYSLOG server or SNMP server, you may be able to solve issue by using this function. The recommendation value is 5 seconds when using this function.

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

3.6.2 System Log Discriminator Settings

Use the following window to implement the settings on a discriminator and display its settings.

Choose **System > System Log > System Log Discriminator Settings** to display the following window.

Figure 3-22 System Log Discriminator Settings

In the section of the **Discriminator Log Settings**, you can configure the following parameters.

Parameter	Overview
Discriminator Name	Enter the name of a discriminator profile. The number of characters can be up to 15.
Action	Choose the facility operation option and a facility type to associate them with an operation selected. The options available as an operation are dispose (or discard) and include.
Severity	Choose the operation option and the severity of the information type, which is logged. The options available as an operation are dispose and include. The values to choose severity: 0(Emergencies) , 1(Alerts) , 2(Critical) , 3(Errors) , 4(Warnings) , 5(Notification) , 6(Information) and 7(Debugging) .

Click **Apply** to add a new entry based on the information specified.

Click **Delete** to delete the entry.

3.6.3 System Log Server Settings

Use the following window to implement the settings on the server, which is used on the system-log, and to display its settings.

Choose **System > System Log > System Log Server Settings** to display the following window.

Figure 3-23 System Log Server Settings

In the section of **Log Server**, you can configure the following parameters.

Parameter	Overview
Host IPv4 Address	Enter an IPv4 address of a system-log server.
Host IPv6 Address	Enter an IPv6 address of a system-log server.
UDP Port	Enter the port-number of UDP (User Datagram Protocol) of a system-log server. Set the number (or value) to 514, or specify the value within the range from 1,024 to 65,535. By default, the value is set to 514.
Severity	Choose the severity of the information type, which is logged. The values to choose are these: 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Information) and 7 (Debugging).

Parameter	Overview		
Facility	Choose the facility number that are logged. The range is from 0 to 23. Each facility-number is associated with the specific facility below. See the following table.		
	Facility-Number	Facility Name	Facility Description
	1	user	User-level messages
	2	mail	Mail System
	3	daemon	System daemons
	4	auth1	Security/ Authentication messages
	5	syslog	Messages generated by the SYSLOG, internally
	6	lpr	Line printer sub-system
	7	news	Network news sub-system
	8	uucp	UUCP sub-system
	9	clock1	Clock daemon
	10	auth2	Security / Authentication messages
	11	ftp	FTP daemon
	12	ntp	NTP sub-system
	13	logaudit	Log audit
	14	logalert	Log alert
	15	clock2	Clock daemon
	16	local0	Local use 0 (local0)
	17	local1	Local use 1 (local1)
	18	local2	Local use 2 (local2)
	19	local3	Local use 3 (local3)
	20	local4	Local use 4 (local4)
	21	local5	Local use 5 (local5)
	22	local6	Local use 6 (local6)
	23	local7	Local use 7 (local7)
Discriminator Name	Enter a discriminator-name to be used for filtering messages that are sent to a log-server. The number of characters for the name can be up to 15.		

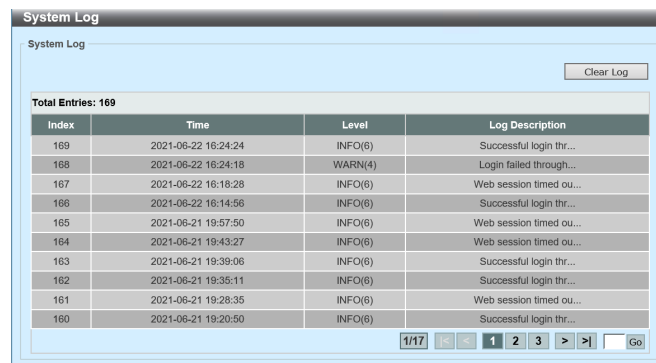
Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete the entry.

3.6.4 System Log

Use the following window to display and clear system logs.

Choose **System > System Log > System Log Settings** to display the following window.



The screenshot shows a window titled "System Log". Inside, there is a "Clear Log" button in the top right corner. Below it, a text label reads "Total Entries: 169". A table displays log entries with the following columns: Index, Time, Level, and Log Description. The table contains 10 rows of data. At the bottom of the window, there is a pagination control showing "1/17" and buttons for navigating between pages (1, 2, 3, etc.) and a "Go" button.

Index	Time	Level	Log Description
169	2021-06-22 16:24:24	INFO(6)	Successful login thr...
168	2021-06-22 16:24:18	WARN(4)	Login failed through...
167	2021-06-22 16:18:28	INFO(6)	Web session timed ou...
166	2021-06-22 16:14:56	INFO(6)	Successful login thr...
165	2021-06-21 19:57:50	INFO(6)	Web session timed ou...
164	2021-06-21 19:43:27	INFO(6)	Web session timed ou...
163	2021-06-21 19:39:06	INFO(6)	Successful login thr...
162	2021-06-21 19:35:11	INFO(6)	Successful login thr...
161	2021-06-21 19:28:35	INFO(6)	Web session timed ou...
160	2021-06-21 19:20:50	INFO(6)	Successful login thr...

Figure 3-24 System Log

Click the **Clear Log** button to clear the log-entry from the table above.

If two or more pages exist, enter their page number. Then click **Go** to move to a specific page.

3.6.5 System Attack Log

Use the following window to display and clear the system attack log.

Choose **System > System Log > System Attack Log** to display the following window.

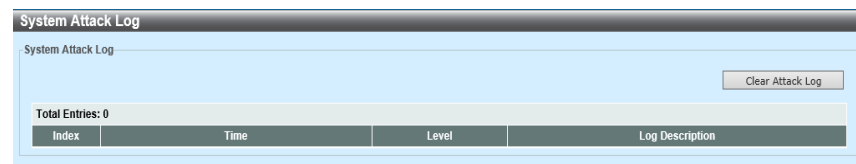


Figure 3-25 System Attack Log

Click the **Clear Attack Log** button to clear the entry of attack logs from a table.

3.6.6 System Authentication Log

Use the following window to implement the settings on a system authentication log and display its settings.

Choose **System > System Log > System Authentication Log** to display the following window.

The screenshot shows the 'System Authentication Log' configuration window. It includes settings for the log's state (Enabled), write delay (60 minutes), and tail size (1-256). There are buttons for 'Apply', 'Find', 'Show All', and 'Clear Log'. A summary bar indicates 'Total Entries: 0'. The bottom section is a table header with columns: ID, Date/Time, Level, and Authentication Event.

Figure 3-26 System Authentication Log

In the section of **System Authentication Log**, you can configure the following parameters.

Parameter	Overview
Authentication Log State	This parameter enables or disables an authentication log.
Write Delay for Authentication Logs	Enter the write-delay value of the authentication log. The range is from 1 to 1,440 (minutes).
Tail	Enter the number of the latest authentication log-entries to be displayed. The range is from 1 to 256.

Click **Apply** to reflect the change.

Click **Find** to search the entry in a table based on the search condition specified.

Click **Show All** to search all the entries available for displaying them.

Click the **Clear Log** button to clear the log entry from a table.

3.7 Time and SNTP (Simple Network Time Protocol)

3.7.1 Clock Settings

Use the following window to implement the settings on time and date, which is used on the time-dependent features of the switch, and to display its settings.

Choose **System > Time and SNTP > Clock Settings** to display the following window.

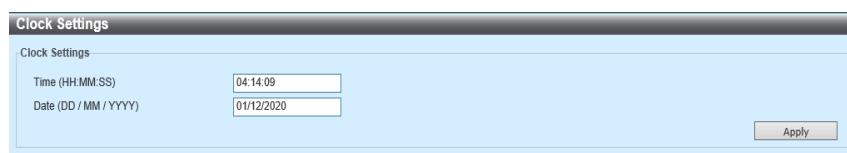


Figure 3-27 Clock Settings

In the section of **Clock Settings**, you can configure the following parameters.

Parameter	Overview
Time	Enter the current time by using (HH), (MM), and (SS) (e.g. 19:20:20).
Date (DD / MM / YYYY)	Enter the current day (DD), month (MM) and year (YY) (e.g. 25/04/2017).

Click **Apply** to reflect the change.

3.7.2 Time Zone Settings

Use the following window to implement the settings on DST (Summer-time) and time zone to display its settings.

Choose **System > Time and SNTP > Time Zone Settings** to display the following window.

Figure 3-28 Time Zone Settings

In the first section, you can configure the following parameters.

Parameter	Overview
Summer-Time State	<p>Choose the summer-time settings. The options available are as follows.</p> <ul style="list-style-type: none"> • Disable - Disables the summer-time settings. • Recurring Setting - Configure so as the summer-time starts and ends on the date and month specified. • Date Settings - Configure so as the summer-time starts and ends on the date and month specified.
Timezone	Specifies the offset of a local time zone from Universal Coordinated Time (UTC).

In the section of **Recurring Settings**, you can configure the following parameters.

Parameter	Overview
From: Week of the Month	Select the week when summer-time starts.
From: Day of the Week	Select the day when summer-time starts.
From: Month	Select the month when summer-time starts.
From: Time	Select the time when summer-time starts.
To: Week of the Month	Select the week when summer-time ends.
To: Week and date	Select the day when summer-time ends.
To: Month	Select the month when summer-time ends.
To: Time	Select the time when summer-time ends.
Offset	Enter the time to add on the summer-time period. The default value is 60, and the range of this offset is 30, 60, 90 and 120.

In the section of **Date Settings**, you can configure the following parameters.

Parameter	Overview
From: Date of Month	Select the date when summer-time starts.
From: Month	Select the month when summer-time starts.
From: Year	Enter the year when summer-time starts.
From: Time	Select the time when summer-time starts.
To: Date of the Month	Select the date when summer-time ends.
To: Month	Select the month when summer-time ends.
To: Year	Enter the year when summer-time ends.
To: Hour	Select the time when summer-time ends.
Offset	Enter the time to add on the summer-time period. The default value is 60, and the range of this offset is 30, 60, 90 and 120.

Click **Apply** to reflect the change.

3.7.3 SNTP Settings

Use the following window to implement the settings on SNTP (Simple Network Time Protocol) and display its settings. Use the SNTP, and then obtain a synchronization automatically and periodically between the configuration of time and date for a switch and the settings hosted by an SNTP server.

Choose **System > Time and SNTP > SNTP Settings** to display the following window.

Figure 3-29 SNTP Settings

In the section of **SNTP Global Settings**, you can configure the following parameters.

Parameter	Overview
SNTP State	This parameter enables or disables SNTP, globally.
Poll Interval	Enter the synchronization-interval, in seconds. The range of values is from 30 and 99,999 (seconds). The default interval is 720 (seconds).

Click **Apply** to reflect the change.

In the section of **SNTP Server Settings**, you can configure the following parameters.

Parameter	Overview
IPv4 Address	Enter an IPv4 address of an SNTP server.
IPv6 Address	Enter an IPv6 address of an SNTP server.

Click **Add** to add the new entry based on the information specified.

Click **Delete** to delete an entry.

3.8 Time Range

Use the following window to implement the settings on a time range profile and display its settings.

Choose **System > Time Range** to display the following window.

Figure 3-30 Time Range

In the section of **Time Range**, you can configure the following parameters.

Parameters	Overview
Range Name	Enter the name of a time range profile. The number of characters for the name can be up to 32.
From Week - To Week	Select the starting and ending days of the week that will be used for this time profile. If you set the Daily option to on, the time profile is used for all days. When the option of a final week is set to ON, this time profile is used from the beginning of a week to the end of it.
From Starting Time (HH:MM) to Ending Time (HH:MM)	Choose the starting and ending time, which is used for this time profile. The first (left-side) drop-down menu allows you to choose the time. You can choose the minute on the second (right-side) drop-down menu.

Click **Apply** to add a new entry based on the information specified.

Click **Find** to search the entry in a table based on the search condition specified for displaying.

Click **Show All** to find and display all the entries available.

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

Click **Delete** to delete the entries.

If two or more pages exist, enter the page number. Then click **Go** to move to the specific page.

4 Management

4.1 Command Logging

This window is used to enable or disable the command logging function. This function is used to log the CLI commands. Commands that did not change the configuration of the switch would not be logged.

Choose **Management > Command Logging** to display the following window.



Figure 4-1 Command Logging

In the **Command Logging Settings** section, you can configure the following parameters.

Parameter	Overview
Command Logging State	Select to enable or disable the command logging function.

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

4.2 User Accounts Settings

This window is used to configure and display the user account settings. These user accounts are used to log into the software configuration of the switch.

Choose **Management > User Accounts Settings** to display the following window.

The screenshot shows the 'User Accounts Settings' window with the 'User Management Settings' tab selected. The form contains the following fields: 'User Name' with a hint '32 chars', 'Privilege (1-15)', 'Password Type' set to 'None', and a 'Password' field. An 'Apply' button is to the right. Below the form, it says 'Total Entries: 1'. A table lists one entry: 'manager' with privilege '15' and a masked password. A 'Delete' button is next to the entry. At the bottom, there are pagination controls showing '1/1' and a 'Go' button.

Figure 4-2 User Accounts Settings (User Management Settings)

You can configure the following parameters in the **User Management Settings** section.

Parameter	Overview
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. The range is from 1 to 15.
Password Type	Select the password type for this user account here. Options to choose from are None , Plain Text , and Encrypted-SHA1 . SHA stands for Secure Hash Algorithms.
Password	After selecting Plain Text or Encrypted-SHA1 as the password type, enter the password for this user account here.

Click the **Apply** button to add a new entry based on the information specified.

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

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Session Table** tab to display the following window.

ID	Type	User Name	Privilege	Login Time	IP Address
0	console	Anonymous	1	4D20H33M53S	
20	* web	manager	15	4M46S	192.168.100.254

Figure 4-3 User Accounts Settings (Session Table)

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

4.3 User Accounts Encryption

Use the following window to enable or disable the user accounts encryption.

Choose **Management > User Accounts Encryption** to display the following window.

Figure 4-4 User Accounts Encryption

In the section of **User Accounts Encryption**, you can configure the following parameter.

Parameter	Overview
User Accounts Encryption State	This parameter enables or disables the user-account encryption.

Click **Apply** to reflect the change.

4.4 Login Method

Use the following window to implement the settings on and display the log-in method for each log-in application, which is supported on the switch.

Choose **Management > Login Method** to display the following window.

Login Method		
Enable Password		
Level	15	
Password Type	Plain Text	
Password	32 chars	
Apply		
Login Method		
Application	Login Method	
Console	Login Local	Edit
Telnet	Login Local	Edit
SSH	Login Local	Edit
Login Password		
Application	Console	
Password Type	Plain Text	
Password	32 chars	
Apply		

Figure 4-5 Login Method

In the section of **Enable Password**, you can configure the following parameters.

Parameter	Overview
Level	Choose the privilege level of user accounts. The range is from 1 to 15.
Password Type	Choose the password type for users. The options available are as follows. <ul style="list-style-type: none">• Plain Text - Choosing this makes a password to become a plain-text form. This is the default option.• Encrypted - Choose this to encrypt a password based on SHA-1.
Password	Enters a password for user accounts. <ul style="list-style-type: none">- The number of characters for a password of the plain-text form can be up to 32. The password can be case-sensitive and include spaces.- In the encrypted form, the number of characters for its password can be up to 35 (maximum byte) and case-sensitive.

Click **Apply** to reflect the change.

Click **Edit** to edit the entry-settings.

In the section of **Login Method**, you can configure the following parameter.

Parameter	Overview
Log-in Method	<p>Click Edit, and then this parameter becomes configurable. Choose the log-in method for the application specified. The options available are as follows.</p> <p>No - Log-in authentication to access the application specified is not needed.</p> <p>Log-in - You need to enter a password when accessing the application specified.</p> <p>Log-in Local - You need to enter a user-name and a password to access the application specified.</p>

In the section of **Login Password**, you can configure the following parameters.

Parameter	Overview
Application	Choose an application to configure. The options available are Console , Telnet and Secure Shell (SSH) .
Password Type	Choose a password-encryption type to use. The options available are Plain Text and Encrypted .
Password	<p>Enter a password of the application selected. This password is used when the login method of the application specified is set to login.</p> <ul style="list-style-type: none"> In the plain-text form, the number of characters for a password can be up to 32. The password is case-sensitive and can contain spaces. In the encrypted form, the number of characters for its password can be up to 35, as the maximum bytes, and be case-sensitive.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete the entry.

4.5 SNMP (Simple Network Management Protocol)

4.5.1 SNMP Global Settings

Use the following window to configure and display the global SNMP settings.

Choose **Management > SNMP > SNMP Global Settings** to display the following window.

Figure 4-6 SNMP Global Settings

You can configure the following parameters in the **SNMP Global Settings** section.

Parameter	Overview
SNMP Global State	Select to globally enable or disable the SNMP feature.
SNMP Response Broadcast Request	Select to enable or disable the server to respond to broadcast SNMP <i>GetRequest</i> packets.
SNMP UDP Port	Enter the SNMP UDP port number. The range is from 1 to 65,535.
Trap Source Interface	Enter the interface whose IP address is used as the source address for sending the SNMP trap packet.

You can configure the following parameters in the **Trap Settings** section.

Parameter	Overview
Trap Global State	Select to globally enable or disable the sending of all or specific SNMP notifications.
SNMP Authentication Trap	Select this option to control the sending of SNMP authentication failure notifications. An <i>authenticationFailuretrap</i> trap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.
Port Link Up	Select this option to control the sending of port link up notifications. A <i>linkUp</i> trap is generated when the device recognizes that one of the communication links has come up.
Port Link Down	Select this option to control the sending of port link down notifications. A <i>linkDown</i> trap is generated when the device recognizes that a one of the communication links is down.
Coldstart	Select this option to control the sending of SNMP <i>coldStart</i> notifications.
Warmstart	Select this option to control the sending of SNMP <i>warmStart</i> notifications.

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

The following parameters can be configured in the **Log Trap Link Change Delay Settings** section:

Parameter	Description
Log Trap Link Change	Enables issuance delays for system logs and SNMP traps related to the link state of physical ports. The range is from 1 to 30 (seconds). When using the link aggregation on your device, if the system logs and SNMP traps regarding the link status of the physical port cannot be normally transmitted to the SYSLOG server or SNMP server, you may be able to solve issue by using this function. The recommendation value is 5 seconds when using this function.

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

4.5.2 SNMP Linkchange Trap Settings

Use the following window to configure and display the SNMP Linkchange trap settings.

Choose **Management > SNMP > SNMP Linkchange Trap Settings** to display the following window.

The screenshot shows the 'SNMP Linkchange Trap Settings' window. It includes four dropdown menus: 'From Port' (Fi1/0/1), 'To Port' (Fi1/0/1), 'Trap Sending' (Disabled), and 'Trap State' (Disabled). An 'Apply' button is located to the right of these settings. Below the settings is a table with three columns: 'Port', 'Trap Sending', and 'Trap State'.

Port	Trap Sending	Trap State
Fi1/0/1	Enabled	Enabled
Fi1/0/2	Enabled	Enabled
Fi1/0/3	Enabled	Enabled
Fi1/0/4	Enabled	Enabled
Te1/0/5	Enabled	Enabled
Te1/0/6	Enabled	Enabled

Figure 4-7 SNMP Linkchange Trap Settings

You can configure the following parameters in the **SNMP Linkchange Trap Settings** section.

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
From Port - To Port	Select the port(s) that will be used here.
Trap Sending	Select to enable or disable the sending of the SNMP notification traps that are generated by the system.
Trap State	Select to enable or disable the SNMP <i>linkChange</i> trap.

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

4.5.3 SNMP View Table Settings

Use the following window to configure and display the SNMP view table settings. These SNMP view entries define which Management Information Base (MIB) objects can be accessed by a remote SNMP manager. The SNMP Subtree Object Identifier (OID) maps SNMP users to the SNMP views.

Choose **Management > SNMP > SNMP View Table Settings** to display the following window.

The screenshot shows the 'SNMP View Table Settings' window. It has three input fields: 'View Name *' with a '32 chars' hint, 'Subtree OID *' with a 'N.N.N...N' hint, and 'View Type' with a dropdown menu set to 'Included'. An 'Add' button is to the right. Below these is a table with 8 entries. The table has columns for View Name, Subtree OID, View Type, and a Delete button.

View Name	Subtree OID	View Type	
restricted	1.3.6.1.2.1.1	Included	Delete
restricted	1.3.6.1.2.1.11	Included	Delete
restricted	1.3.6.1.6.3.10.2.1	Included	Delete
restricted	1.3.6.1.6.3.11.2.1	Included	Delete
restricted	1.3.6.1.6.3.15.1.1	Included	Delete
CommunityView	1	Included	Delete
CommunityView	1.3.6.1.6.3	Excluded	Delete
CommunityView	1.3.6.1.6.3.1	Included	Delete

Figure 4-8 SNMP View Table Settings

You can configure the following parameters in the **SNMP View Settings** section.

Parameter	Overview
View Name	Enter the SNMP view name. This is used to identify the new SNMP view being created. This can be up to 32 characters long.
Subtree OID	Enter the OID sub-tree for the view . The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select the view type . Options available are: <ul style="list-style-type: none"> • Included - Select to include this object in the list of objects that an SNMP manager can access. • Excluded - Select to exclude this object from the list of objects that an SNMP manager can access.

Click the **Add** button to add a new entry based on the information specified.

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

4.5.4 SNMP Community Table Settings

This window is used to configure and display SNMP community strings that define the relationship between SNMP managers and SNMP agents. The SNMP community string acts like a password to permit access to the SNMP agent on the switch.

The following characteristics can be associated with the community string:

- An access list containing IP addresses of SNMP managers that are permitted to use the community string to gain access to the SNMP agent of the switch.
- MIB views that define the subset of MIB objects that are accessible to the SNMP community.
- Read-Write or Read-Only permissions for MIB objects accessible to the SNMP community.

Choose **Management > SNMP > SNMP Community Table Settings** to display the following window.

Figure 4-9 SNMP Community Table Settings

You can configure the following parameters in the **SNMP Community Settings** section.

Parameter	Overview
Key Type	Select the key type for the SNMP community. Options available are Plain Text and Encrypted .
Community Name	Enter the SNMP community name here. You can use this to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. This can be up to 32 characters long.
View Name	Enter the SNMP view name here. You can use this to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table. This can be up to 32 characters long.

Parameter	Overview
Access Right	Select the access right here. Options available are: <ul style="list-style-type: none">• Read Only - SNMP community members using the community string created can only read the contents of the MIBs on the Switch.• Read Write - SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.
IP Access-List Name	Enter the name of the standard access list to restrict the users that can use this community string to access to the SNMP agent.

Click the **Add** button to add a new entry based on the information specified.

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

4.5.5 SNMP Group Table Settings

Use the following window to configure and display the SNMP group table settings. SNMP groups map SNMP users to SNMP views.

Choose **Management > SNMP > SNMP Group Table Settings** to display the following window.

The screenshot shows the 'SNMP Group Table Settings' window. It has a title bar 'SNMP Group Table Settings' and a subtitle 'SNMP Group Settings'. The configuration area includes:

- Group Name ***: A text field with a '32 chars' limit.
- User-based Security Model**: A dropdown menu currently set to 'SNMPv1'.
- Security Level**: A dropdown menu currently set to 'NoAuthNoPriv'.
- IP Address-List Name**: A text field with a '32 chars' limit.
- Read View Name**: A text field with a '32 chars' limit.
- Write View Name**: A text field with a '32 chars' limit.
- Notify View Name**: A text field with a '32 chars' limit.

 A note indicates '* Mandatory Field'. An 'Add' button is located to the right of the configuration fields. Below the configuration area is a table titled 'Total Entries: 5'.

Group Name	Read View Name	Write View Name	Notify View Name	Security Model	Security Level	IP Address-List Name	
public	CommunityV...		CommunityV...	v1			Delete
public	CommunityV...		CommunityV...	v2c			Delete
initial	restricted		restricted	v3	NoAuthNoPriv		Delete
private	CommunityV...	CommunityV...	CommunityV...	v1			Delete
private	CommunityV...	CommunityV...	CommunityV...	v2c			Delete

Figure 4-10 SNMP Group Table Settings

You can configure the following parameters in the **SNMP Group Settings** section.

Parameter	Overview
Group Name	Enter the SNMP group name here. This name can be up to 32 characters long. Spaces are not allowed.
Read View Name	Enter the read view name that users of the group can access.
User-based Security Model	Select the security model here. Options available are: <ul style="list-style-type: none"> • SNMPv1 - Select to allow the group to use the SNMPv1 security model. • SNMPv2c - Select to allow the group to use the SNMPv2c security model. • SNMPv3 - Select to allow the group to use the SNMPv3 security model.
Write View Name	Enter the write view name that the users of the group can access.

Parameter	Overview
Security Level	After selecting to use SNMPv3 as the User-based Security Model , select the security level here. Options available are: <ul style="list-style-type: none">• NoAuthNoPriv - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.• AuthNoPriv - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.• AuthPriv - Specifies that authorization will be
Notify View Name	Enter the notify view name that users of the group can access. The notify view describes the object that can be reported its status via trap packets to the group user.
IP Address-List Name	Enter the standard IP Access Control List (ACL) to associate with the group.

Click the **Add** button to add a new entry based on the information specified.

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

4.5.6 SNMP Engine ID Local Settings

This window is used to configure and display the local SNMP engine ID. The engine ID is unique per switch and is used in SNMPv3 (SNMP version 3) implementations.

Choose **Management > SNMP > SNMP Engine ID Local Settings** to display the following window.

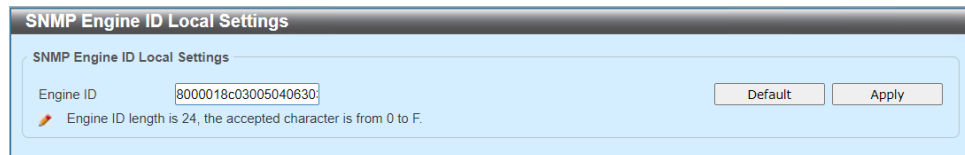
The image shows a web-based configuration window titled "SNMP Engine ID Local Settings". Inside the window, there is a sub-header "SNMP Engine ID Local Settings". Below this, there is a label "Engine ID" followed by a text input field containing the hexadecimal string "8000018c03005040630". To the right of the input field are two buttons: "Default" and "Apply". Below the input field, there is a small orange icon and a note: "Engine ID length is 24, the accepted character is from 0 to F."

Figure 4-11 SNMP Engine ID Local Settings

You can configure the following parameters in the **SNMP Engine ID Local Settings** section.

Parameter	Overview
Engine ID	Enter the SNMP engine ID string here. This string can be up to 24 characters long.

Click the **Default** button to use the default engine ID.

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

4.5.7 SNMP User Table Settings

This window is used to configure and display SNMP user settings.

Choose **Management > SNMP > SNMP User Table Settings** to display the following window.

Figure 4-12 SNMP User Table Settings

You can configure the following parameters in the **SNMP User Settings** section.

Parameter	Overview
User Name	Enter the SNMP user name here. This is used to identify the SNMP user. This name can be up to 32 characters long.
Group Name	Enter the SNMP group name for the user here. This name can be up to 32 characters long. Spaces are not allowed.
SNMP Version	Select the SNMP version. Options available are v1 , v2c , and v3 .
SNMP V3 Encryption	After selecting v3 as the SNMP Version , select the SNMPv3 encryption here. Options available are None , Password , and Key .
Auth-Protocol by Password	After selecting v3 as the SNMP Version and Password for SNMP V3 Encryption , select the authentication protocol for the password here. Options available are: <ul style="list-style-type: none"> MD5 - Specifies to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or key. SHA - Specifies to use the HMAC-SHA authentication protocol. This field will require the user to enter a password or key.

Parameter	Overview
Password	Enter the authentication protocol password here. <ul style="list-style-type: none"> For MD5, this password must be between 8 and 16 characters long. For SHA, this password must be between 8 and 20 characters long.
Priv-Protocol by Password	After selecting v3 as the SNMP Version and Password for SNMP V3 Encryption , select the private protocol for the password here. Options available are: <ul style="list-style-type: none"> None - Specifies that no authorization protocol will be used. DES56 - Specifies to use Data Encryption Standard (DES) 56-bit encryption, based on the CBC-DES (DES-56) standard. This field requires the user to enter a password or a key.
Password	Enter the private protocol password here. <ul style="list-style-type: none"> For none, this field will be disabled. For DES56, this password must be between 8 and 16 characters long.
Auth-Protocol by Key	After selecting v3 as the SNMP Version and Key for SNMP V3 Encryption select the authentication protocol for the key here. Options available are: <ul style="list-style-type: none"> MD5 - Specifies to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or a key. SHA - Specifies to use the HMAC-SHA authentication protocol. This field will require the user to enter a password or a key.
Key	Enter the authentication protocol key here. <ul style="list-style-type: none"> For MD5, this key must be 32 characters long. For SHA, this key must be 40 characters long.
Priv-Protocol by Key	After selecting v3 as the SNMP Version and Key for SNMP V3 Encryption select the private protocol for the key here. Options available are: <ul style="list-style-type: none"> None - Specifies that no authorization protocol will be used. DES56 - Specifies to use Data Encryption Standard (DES) 56-bit encryption, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key.
Key	Enter the private protocol key here. <ul style="list-style-type: none"> For none, this field will be disabled. For DES56, this key must be 32 characters long.
IP Address-List Name	Enter the standard IP ACL to associate with the user.

Click the **Add** button to add a new entry based on the information specified.

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

4.5.8 SNMP Host Table Settings

This window is used to configure and display SNMP host settings.

Choose **Management > SNMP > SNMP Host Table Settings** to display the following window.

Figure 4-13 SNMP Host Table Settings

You can configure the following parameters in the **SNMP Host Settings** section.

Parameter	Overview
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
Host IPv6 Address	Enter the IPv6 address of the SNMP notification host.
User-based Security Model	Select the security model here. Options available are: <ul style="list-style-type: none"> • SNMPv1 - Select to allow the group user to use the SNMPv1 security model. • SNMPv2c - Select to allow the group user to use the SNMPv2c security model. • SNMPv3 - Select to allow the group user to use the SNMPv3 security model.
Security Level	After selecting SNMPv3 as the User-based Security Model , select the security level here. Options available are: <ul style="list-style-type: none"> • NoAuthNoPriv - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. • AuthNoPriv - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. • AuthPriv - Specifies that authorization will be
UDP Port	Enter the UDP port number here. The default port number is 162. The range is from 1 to 65535. Some port numbers may conflict with other protocols.

Parameter	Overview
Community String / SNMPv3 User Name	Enter the community string to be sent with the notification packet.

Click the **Add** button to add a new entry based on the information specified.

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

4.6 RMON (Remote Monitoring)

4.6.1 RMON Global Settings

Use the following window to enable or disable the trap state on RMON rising alarm and RMON falling alarm.

Choose **Management > RMON > RMON Global Settings** to display the following window.

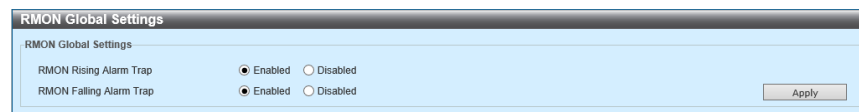


Figure 4-14 RMON Global Settings

In the section of **RMON Global Settings**, you can configure the following parameters.

Parameter	Overview
RMON Rising Alarm Trap	This parameter enables or disables the function of an RMON rising alarm trap.
RMON Falling Alarm Trap	This parameter enables or disables the function of an RMON falling alarm trap.

Click **Apply** to reflect the change.

4.6.2 RMON Statistics Settings

Use the following window to implement the settings on the RMON statistics for the port specified and display its settings.

Choose **Management > RMON > RMON Statistics Settings** to display the following window.

Figure 4-15 RMON Statistics Settings

In the section of **RMON Statistics Settings**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
Index	Enter the RMON table index. The range of value is from 1 to 65,535.
Owner	Enter the owner character strings; the number of character strings can be up to 127.

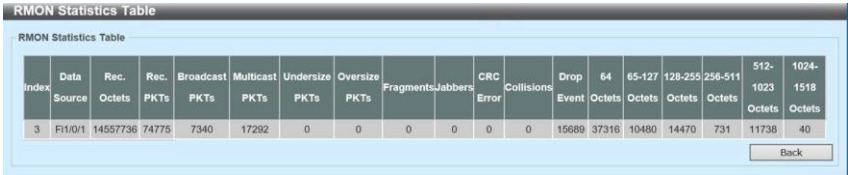
Click **Add** to add a new entry based on the information specified.

Click **Delete** to delete the entry.

Click **Show Detail** to display details on the entry.

If two or more pages exist, enter the page-numbers. Then click **Go** to move to a specific page.

Click **Show Detail** to display the following window.



The screenshot shows a window titled "RMON Statistics Table". Inside, there is a table with 20 columns representing different network statistics. The first row shows the interface "Fi1/0/1" and various counts for received packets, broadcasts, multicasts, errors, and drops. A "Back" button is located at the bottom right of the table.

Index	Data Source	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets
3	Fi1/0/1	14557736	74775	7340	17292	0	0	0	0	0	0	15689	37316	10480	14470	731	11738	40

Figure 4-16 RMON Statistics Settings (Show Detail.)

Click **Back** to return to the previous window.

4.6.3 RMON History Settings

Use the following window to implement the RMON history settings on the port specified and display its settings.

Choose **Management > RMON > RMON History Settings** to display the following window.

Figure 4-17 RMON History Settings

In the section of **RMON History Settings**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
Index	Enter the index number of entries for a history group table. The range is from 1 to 65,535.
Number of Buckets	Enter the number of packets, which are specified for a RMON collecting history group of the statistics. The range is from 1 to 65,535. The default value is 50.
Interval	Enter the interval-time for the cycle of each polling. The range is from 1 to 3,600 (seconds).
Owner	Enter the owner character strings; the number of characters for the strings can be up to 127.

Click **Add** to add a new entry based on the information specified.

Click **Delete** to delete the entry.

Click **Show Detail** to display details on the entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Show Detail** to display the following window.

RMON History Table													
RMON History Table													
Index	Sample	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Utilization	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event
													Back

Figure 4-18 RMON History Table (Show Detail.)

Click **Back** to return to the previous window.

4.6.4 RMON Alarm Settings

Choose **Management > RMON > RMON Alarm Settings** to display the following window.

Figure 4-19 RMON Alarm Settings

In the section of **RMON Alarm Settings**, you can configure the following parameters.

Parameter	Overview
Index	Enter the alarm index. The range is from 1 to 65,535.
Interval	Enter the interval of the cross-checking between a variable sampling and the threshold as the second-unit. The valid range is from 1 to 2,147,483,648.
Variables	Enter an object ID of variables for sampling.
Type	Choose a monitoring type. The options available are Absolute and Delta .
Rising Threshold	Enter the rising threshold within the range from 0 to 2,147,483,647.
Falling Threshold	Enter the falling threshold within the range from 0 to 2,147,483,647.
Rising Event Number	Enter the index of an event entry to use for notifying the events, which exceed the rising threshold. The valid range is from 1 to 65,535. If not specified, no actions are necessary when the value exceeds the rising threshold.
Falling Event Number	Enter the event-entry index to use for notifying the events, which exceed the falling threshold. The valid range is from 1 to 65,535. If not specified, no actions are necessary when the value exceeds the falling threshold.
Owner	Enter the owner character strings; the maximum number of the strings can be up to 127.

Click **Add** to add a new entry based on the information specified.

Click **Delete** to delete the entry.

4.6.5 RMON Event Settings

Use the following window to implement the RMON event settings and display its settings.

Choose **Management > RMON > RMON Event Settings** to display the following window.

Figure 4-20 RMON Event Settings

In the section of **RMON Event Settings**, you can configure the following parameters.

Parameter	Overview
Index	Enter the index value of an alarm entry. The range is from 1 to 65,535.
Description	Enter the overview and description of the RMON event entries. The number of characters in character strings can be up to 127.
Type	Choose the type of the RMON event entries. The options available are None , Logs , Traps and Logs and Traps .
Community	Enter the community character strings. The number of characters for the character strings can be up to 127.
Owner	Enter the owner character strings. The number of characters for the character strings can be up to 127.

Click **Add** to add a new entry based on the information specified.

Click **Delete** to delete the entry.

Click **View Log** to display the log entry, which is associated with the entry specified.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **View-log** to display the following window.

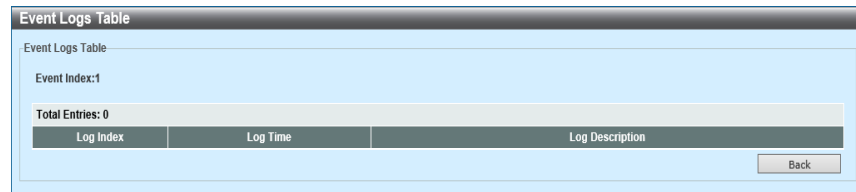


Figure 4-21 RMON Event Settings (View Log)

Click **Back** to return to the previous window.

4.7 Telnet/Web

Use the following window to implement the settings on Telnet and Web of the switch and display its settings.

Choose **Management > Telnet/Web** to display the following window.

Figure 4-22 Telnet/Web

In the section of the **Telnet Settings**, you can configure the following parameters.

Parameter	Overview
Telnet State	This parameter enables or disables the function of a Telnet server.
Port	Enter the TCP port-number to use for Telnet management of a device. (TCP stands for Transmission Control Protocol.) The TCP port, which is typically used for Telnet protocol is 23.

Click **Apply** to reflect the change.

In the section of the **Web Settings**, you can configure the following parameters.

Parameter	Overview
Web State	This parameter enables or disables the configuration via (or on the) Web.
Port	Enter the TCP port-number to use for Telnet management of a device. The TCP port typically used for Telnet protocol is 80.

Click **Apply** to reflect the change.

4.8 Session Time-out

Use the following window to implement the settings on Web, Console, Telnet and the session time-out of the SSH connection and to display its settings.

Choose **Management > Session Time-out** to display the following window.

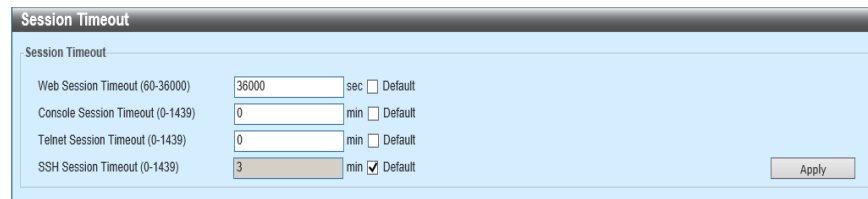


Figure 4-23 Session Time-out

In the section of **Session Time-out**, you can configure the following parameters.

Parameter	Overview
Web Session Time-out	Enter the time for Web session time-out with the second-unit. If the default check-box is set to on, the value is returned to the default value. The range of values is from 60 to 36,000 (seconds), and the default value is set to 3 (minutes).
Console Session Time-out	Enter the time for console session time-out with the minute-unit. If the default check-box is set to on, the value returns to the default value. The range of values is from 0 to 1,439 (minutes). If you enter 0, the time-out becomes disabled. The default value is set to 3 (minutes).
Telnet Session Time-out	Enter the time for Telnet session time-out with the minute-unit. If the default check-box is set to on, the value returns to the default value. The range of values is from 0 to 1,439 (minutes). If you enter 0, the time-out becomes disabled. The default value is set to 3 (minutes).
SSH Session Time-out	Enter the time for SSH session time-out with the minute-unit. If the default check-box is set to on, the value returns to the default value. The range of values is from 0 to 1,439 (minutes). If you enter 0, the time-out becomes disabled. The default value is set to 3 (minutes).

Click **Apply** to reflect the change.

4.9 DHCP Auto Configuration

Use the following window to enable or disable the function of the DHCP auto configuration.

Choose **Management > DHCP Auto Configuration** to display the following window.



Figure 4-24 DHCP Auto Configuration

In the section of **DHCP Auto Configuration**, you can configure the following parameter.

Parameter	Overview
Auto Configuration State	This parameter enables or disables the function of the DHCP auto configuration.

Click **Apply** to reflect the change.

4.10 DNS (Domain Name System)

4.10.1 DNS Global Settings

Use the following window to implement the global DNS settings and display its settings.

Choose **Management> DNS> DNS Global Settings** to display the following window.

DNS Global Settings	
IP DNS Lookup Static State	Enabled
IP DNS Lookup Cache State	Enabled
IP Domain Lookup	Disabled
IP Name Server Timeout (1-60)	3 sec
IP DNS Server	Disabled

Figure 4-25 DNS Global Settings

In the section of **DNS Global Settings**, you can configure the following parameters.

Parameter	Overview
Static State for Searching IP DNS	This parameter enables or disables the static state for searching IP DNS.
Cache Condition for Searching IP DNS	This parameter enables or disables the cache condition for searching IP DNS.
Searching IP Domains	This parameter enables or disables the condition for searching IP domains.
IP-name Server Timeout	Enter the maximum time (value) to wait for the response from the name-server specified. Specify the value within the range from 1 to 60.
IP DNS Servers	This parameter enables or disables to set the DNS-server function to global.

Click **Apply** to reflect the change.

4.10.2 DNS Name Server Settings

Use the following window to implement the settings on a DNS name server and display its settings.

Choose **Management > DNS > DNS Name Server Settings** to display the following window.

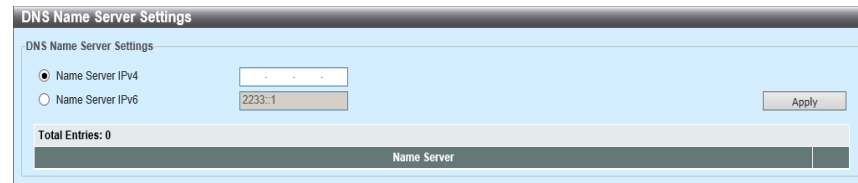


Figure 4-26 DNS Name Server Settings

In the section of the **DNS Name Server Settings**, you can configure the following parameters.

Parameter	Overview
IPv4 Name Server	Choose and enter an IPv4 address of a DNS server.
IPv6 Name Server	Choose and enter an IPv6 address of a DNS server.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete the entry.

4.10.3 DNS Host Settings

Use the following window to implement the DNS host settings and display its settings.

Choose **Management > DNS > DNS Host Settings** to display the following window.

Figure 4-27 DNS Host Settings

In the section of **Static Host Settings**, you can configure the following parameters.

Parameter	Overview
Host Name	Enter the name of a DNS host.
IP Address	Choose and enter an IPv4 address of a DNS host.
IPv6 Address	Choose and enter an IPv6 address of a DNS host.

Click **Apply** to add new entries based on the information specified.

Click **Clear All** to clear all the dynamic entries from a table.

Click **Delete** to delete the entry.

If two or more pages exist, enter the page-numbers. Then click **Go** to move to a specific page.

4.11 File System

Use the following window to implement the settings on a file system of a switch and display its settings.

Choose **Management > File System** to display the following window.

Drive	Media Type	Size (MB)	File System Type	Label
c:	Flash	88	UBIFS	

Figure 4-28 File System

You can configure the following parameter.

Parameter	Overview
Path	Enter the character strings of a path.

Click **Go** to move to the path entered.

Click **Copy** to copy a specific file on the **File System**.

Click **c:** (the drive-link above) to move to C: drive.

Click **c:** (the drive-link) to display the following window.

Index	Info	Attr	Size (byte)	Update Time	Name	Boot Up	Rename	Delete
1	CFG(*)	-rw	1116	Apr. 04 2021 17:14:49	config.cfg	Boot Up	Rename	Delete
2	RUN(*)	-rw	12077624	Feb. 10 2021 19:48:28	runtime.had	Boot Up	Rename	Delete
3		d--	0	Apr. 04 2021 08:03:44	system			Delete

Total 64192000 bytes (Free 51964416 bytes)
(*) : Boot Up File

Figure 4-29 File System (c:)

Click **Back** to return to the previous window.

Click **Create a Directory** to create a new directory on the **File System**.

Click **Boot Up** to use the files in the boot-up sequence.

Only a configuration file and a firmware file can be used in the boot-up sequence.

Click **Rename** to rename a specific file-name.

Click **Delete** to delete a file or folder from the file system.

Click **Copy** to display the following window.

Figure 4-30 File System (Copy)

You can configure the following parameters.

Parameter	Overview
Source	Choose the file type of a source. The options available are startup-config and Source File . Only when you choose the Source File option, you can the source file path and filename be entered in the space provided.
Destination	Choose the file type of a destination (of a copy). The options available are startup-config , running-config and Destination File . Only when you choose the Destination File option, you can enter the destination-path and file-name in the entry-field displayed. Select the Replace check-box to replace the current running configuration with the configuration file, which is displayed.

Click **Apply** to copy to copy the source configuration/file to the destination configuration/file.

Click **Cancel** to cancel the copy.

4.12 SMTP Settings

Use the following window to implement the SMTP (Simple Mail Transfer Protocol) settings and display its settings.

Choose **Management > SMTP Settings** to display the following window.

Figure 4-31 SMTP Settings

In the section of the **SMTP Global Settings**, you can configure the following parameters.

Parameter	Overview
SMTP IP	Choose an IP address type of an SMTP server. The options available are IPv4 and IPv6 .
SMTP IPv4 Server Address	Choose IPv4 from SMTP IP , and then enter an IPv4 address of an SMTP server.
SMTP IPv6 Server Address	Choose IPv6 from SMTP IP , and then enter an IPv6 address of an SMTP server.
SMTP IPv4 Server Port	Choose IPv4 from SMTP IP , and then enter the port-number (value) of an SMTP server. The range is from 1 to 65,535. By default, the value is set to 25.
SMTP IPv6 Server Port	Choose IPv6 from SMTP IP , and then enter the port-number (value) of an SMTP server. The range is from 1 to 65,535. By default, the value is set to 25.
Your Email Address	Enter the email address, which indicates a switch. The number of characters for this character strings can be up to 254.
Transmission Interval	Enter the value of a transmission interval. The range is from 0 to 65,535 (minutes). By default, the value is set to 30 minutes.

Click **Apply** to reflect the change.

In the section of **SMTP Email Receiver Address**, you can configure the following parameter.

Parameter	Overview
Adding an Email Receiver	Enter the email address of a receiver. The number of characters for this character strings can be up to 254.

In the section of **Send a Test-mail to All**, you can configure the following parameters.

Parameter	Overview
Subject	Enter the subject of an email. The number of characters for this character strings can be up to 128.
Contents	Enter the text of an email. The number of characters for this character strings can be up to 512.

Click **Add** to add a new entry based on the information specified.

Click **Apply** to reflect the change.

Click **Delete All** to delete every receiver email address from all the entries.

Click **Delete** to delete a receiver email address from the entry specified.

4.13 NLB FDB Settings

Use the following window to implement the settings on NLB (Network Load Balancing) and FDB (File Database) of the port specified and to display its settings.

Choose **Management > NLB FDB Settings** to display the following window.

Figure 4-32 NLB FDB Settings

In the section of **NLB FDB Settings**, you can configure the following parameters.

Parameter	Overview
NLB Type	Choose the NLB type. The options available are Unicast and Multicast .
VID	Choose Multicast from NLB type , and then enter the VLAN ID you use. The range is from 1 to 4,094.
MAC Address	Enter the Unicast of entries or Multicast MAC address. If the destination MAC address of packets, which are received, corresponds with the MAC address specified, the packets are transferred to the interface specified.
From Port/ To Port	Choose the port you use.

Click **Apply** to reflect the change.

Click **Delete All** to delete all the entries.

Click **Delete** to delete the entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

4.14 IP Setup

4.3.1 IP Setup Protocol Settings

Use the following window to enable or disable the function of an IP setup interface.

Choose **Management > IP Setup > IP Setup Protocol Settings** to display the following window.

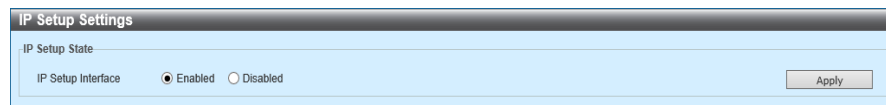


Figure 4-33 IP Setup Protocol Settings

In the section of **IP Setup Protocol State**, you can configure the following parameter.

Parameter	Overview
IP Setup Interface	This parameter enables or disables an IP setup interface.

Click **Apply** to reflect the change.

5 L2 Features

5.1 FDB (Forwarding Database)

5.1.1 Static FDB

5.1.1.1 Unicast Static FDB

Use the following window to implement the settings on a static-unicast forwarding and display its settings.

Choose **L2 Features > FDB > Static FDB > Unicast Static FDB** to display the following window.

Figure 5-1 Unicast Static FDB

In the section of **Unicast Static FDB**, you can configure the following parameters.

Parameter	Overview
Port/Disposal	When choosing Port , apply the port where a MAC address entered exists. When choosing Disposal , drop the MAC address from Unicast Static FDB .
Port Number	Choose the port you use.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
MAC Address	Enter the MAC address where packets are transferred to static. Specify a Unicast MAC address for this address.

Click **Apply** to add new entries based on the information specified.

Click **Delete All** to delete all the entries.

Click **Delete** to delete the entry.

If two or more pages exist, enter the page-numbers. Then click **Go** to move to a specific page.

5.1.1.2 Multicast Static FDB

Use the following window to implement the settings on Multicast static FDB and display its settings.

Choose **L2 Features > FDB > Static FDB > Multicast Static FDB** to display the following window.

Figure 5-2 Multicast Static FDB

In the section of **Multicast Static FDB**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
MAC Address	Enter a MAC address of the static destination for Multicast packets. Specify the Multicast MAC address for this address.

Click **Apply** to add new entries based on the information specified.

Click **Delete** all to delete all the entries.

Click **Delete** to delete the entry.

If two or more pages exist, enter the page-numbers. Then click **Go** to move to a specific page.

5.1.2 MAC Address Table Settings

Use the following window to implement the settings on a MAC address table and display its settings.

Choose **L2 Features > FDB > MAC Address Table Settings** to display the following window.

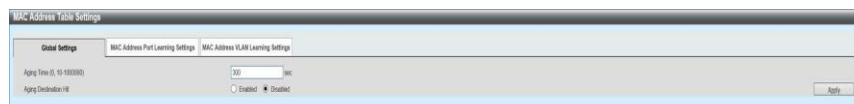


Figure 5-3 MAC Address Table Settings (Global Settings)

In the section of the **Global Settings**, you can configure the following parameters.

Parameter	Overview
Aging Time	Enter the aging time (value) of a MAC address table. The range is from 10 to 1,000,000 (seconds). If you enter 0, the MAC address aging becomes disabled. By default, the value is set to 300 (seconds).
Aging Destination Hit	This parameter enables or disables the function of the aging destination hit.

Click **Apply** to reflect the change.

Click the tab of **MAC Address Port Learning Settings** to display the following window.

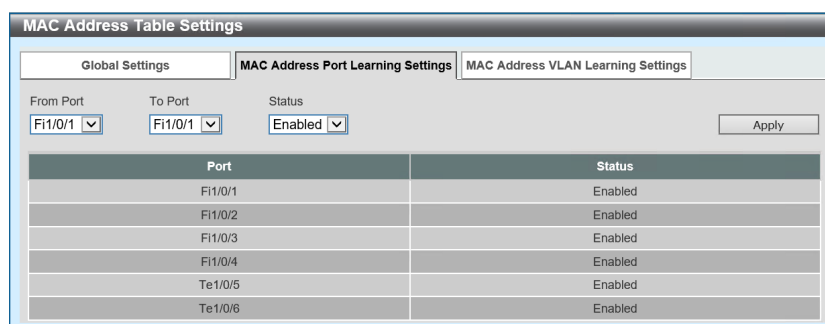


Figure 5-4 MAC Address Table Settings (MAC Address Port Learning Settings)

In the section of **MAC Address Port Learning Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
State	This parameter enables or disables the function of a learning MAC address of the port specified.

Click **Apply** to reflect the change.

Click the tab of **MAC Address Port Learning Settings** to display the following window.

Figure 5-5 MAC Address Table Settings (MAC Address VLAN Learning Settings)

In the section of **MAC Address VLAN Learning Settings**, you can configure the following parameters.

Parameter	Overview
VID List	Enter the VLAN ID you use. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.
State	This parameter enables or disables the function of learning a MAC address of the VLAN specified.

Click **Apply** to add new entries based on the information specified.

In the section of a **MAC Address for Searching VLAN Learning**, you can configure the following parameter.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

If two or more pages exist, enter the page numbers.
Then click **Go** to move to a specific page.

5.1.3 MAC Address Table

Use the following window to display and clear the entry of a MAC address table.

Choose **L2 Features > FDB > MAC Address Table** to display the following window.

VID	MAC Address	Type	Port
1	00-50-40-63-03-55	Static	CPU
1	58-27-8C-BE-62-B6	Dynamic	Fi1/0/2
1	58-27-8C-BF-26-4C	Dynamic	Fi1/0/1

Figure 5-6 MAC Address Table

In the section of the **MAC Address Table**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port-number to configure.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
MAC Address	Enter a MAC address to use for this settings.

Click the **Clear Dynamic by Port** button to clear all the dynamic MAC addresses associated with the port specified.

Click the **Clear Dynamic by VLAN** button to clear all the dynamic MAC addresses associated with the VLAN specified.

Click the **Clear Dynamic by MAC** button to clear the dynamic MAC address specified from a table.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **Clear All** to clear all the entries from a table.

Click **See All** to search and display all the entries available.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

5.1.4 MAC Notification

Use the following window to implement the settings on a global MAC notification and MAC notification of the port specified and display its settings.

Choose **L2 Features > FDB > MAC Notification** to display the following window.

Figure 5-7 MAC Notification (MAC Notification Settings)

In the section of **MAC Notification Global-Settings**, you can configure the following parameters.

Parameter	Overview
MAC Address Notification	This parameter enables or disables to set the MAC notification to global, on the switch.
Interval	Enter the time (value) needed for the notification interval whose range is from 1 to 2,147,483,647 (seconds). By default, the value is set to 1 (second).
History Size	Enter the maximum number (value) of the entries to display a list for the history-log, which is used for the notification. The range is from 0 to 500. By default, the value is set to 1.
State of MAC Notification Trap	This parameter enables or disables the state of MAC notification-traps.
From Port/ To Port	Choose the port you use.
Adding Traps	This parameter enables or disables to add traps on the port selected.
Removing Traps	This parameter enables or disables to remove traps from the port selected.

Click **Apply** to reflect the change.

Choose the **MAC Notification History** tab to display the following window.



Figure 5-8 MAC Notification (MAC Notification History)

5.2 VLAN (Virtual Local Area Network)

5.2.1 802.1Q VLAN

Use the following window to implement the settings on IEEE 802.1Q VLAN and display its settings.

Choose **L2 Features > VLAN > 802.1Q VLAN** to display the following window.

Figure 5-9 802.1Q VLAN

In the section of **802.1Q VLAN**, you can configure the following parameter.

Parameter	Overview
VID List	Enter a VLAN ID to create or delete it. You can enter its consecutive VLAN IDs, which are delimited by a comma. Or you can enter the range of VLAN IDs, which are delimited by a hyphen. The range is from 1 to 4,094.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete entries based on the information specified.

In the section of **Searching VLAN**, you can configure the following parameter.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Find** to search and display the entries in the table based on the search condition specified.

Click **See All** to search and display all the entries available.

Click **Edit** to edit the entry-settings.

Click **Delete** to delete the entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

5.2.2 802.1v Protocol VLAN

5.2.2.1 Protocol VLAN Profile

Use the following window to implement the settings on IEEE 802.1v protocol VLAN and display its settings. Two or more VLANs are supported on each protocol. Untagged-ports can be configured for different protocols on the same physical port.

Choose **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile** to display the following window.

Figure 5-10 Protocol VLAN Profile

In the section of **Adding Protocol VLAN Profile**, you can configure the following parameters.

Parameter	Overview
Profile ID	Enter the profile ID for 802.1v protocol VLAN. The range is from 1 to 16.
Frame Type	Choose an option of a frame type. This function allows you to investigate a type-octet in the packet header, and searches for the protocol type, which is associated. Doing so maps packets to VLAN for the protocol definition. The options available are Ethernet 2, SNAP and LLC . SNAP stands for Sub-network Access Protocol, and LLC for Logical Link Control.

Parameter	Overview
Ether-type	<p>Enter the Ethernet-type value of a group. Use the protocol value to identify a protocol of the frame-type specified. The range is from 0x0 to 0xFFFF. The octet character strings includes one of the following values, depending on a frame-type.</p> <ul style="list-style-type: none">• Regarding Ethernet 2, it is the hex value (or hexadecimal number) of 16 bits (2 octets).• Set IPv4 to 0800, IPv6 to 86DD, and ARP to 0806.• Regarding IEEE802.3 SNAP, it is the hex value of 16 bits (2 octets).• Regarding IEEE802.3 LLC, it is a pair of IEEE 802.2 LSAP (Link Service Access Point) of 2 octets.• The first octet is DSAP (Destination Service Access Point) and the second octet is source.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete the entry.

5.2.2.2 Protocol VLAN Profile Interface

Use the following window to implement the settings on an interface of a protocol VLAN profile and display its settings.

Choose **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface** to display the following window.

Figure 5-11 Protocol VLAN Profile Interface

In the section of **Adding a New Protocol VLAN Interface**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port-number of a switch you configure.
Profile ID	Choose the profile ID of 802.1v protocol VLAN.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
Priority	Choose the priority value you use. Specify the value within the range from 0 to 7. Specify this parameter to rewrite (or transcribe) 802.1p default-priority, which is configured on the switch beforehand. This priority determines the CoS (Class of Service) queue, which is the destination of transferring packets. After specifying this field, if a switch receives packets, which correspond to this priority, the packets are transferred to the CoS queue configured in advance.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete the entry.

5.2.3 GVRP

5.2.3.1 GVRP Global

Use the following window to implement the global settings on GVRP (GARP VLAN Registration Protocol) and display its settings. GARP stands for Generic Attribute Registration Protocol.

Choose **L2 Features > VLAN > GVRP > GVRP Global** to display the following window.

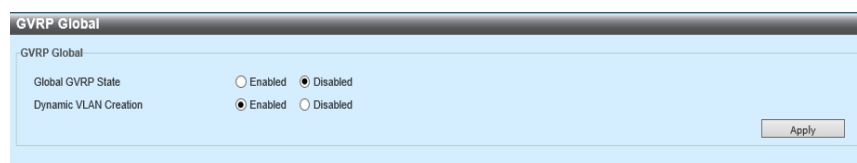


Figure 5-12 GVRP Global

In the section of **GVRP Global**, you can configure the following parameters.

Parameter	Overview
Global GVRP State	This parameter enables or disables the global GVRP state.
Creating Dynamic VLAN	This parameter enables or disables the function of creating a dynamic VLAN.

Click **Apply** to reflect the change.

5.2.3.2 GVRP Port

Use the following window to implement the settings on GVRP Port and display its settings.

Choose **L2 Features > VLAN > GVRP > GVRP Port** to display the following window.

Port	GVRP Status	Join Time	Leave Time	Leave All Time
F11/0/1	Disabled	20	60	1000
F11/0/2	Disabled	20	60	1000
F11/0/3	Disabled	20	60	1000
F11/0/4	Disabled	20	60	1000
Te1/0/5	Disabled	20	60	1000
Te1/0/6	Disabled	20	60	1000

Figure 5-13 GVRP Port

In the section of **GVRP Port**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
GVRP State	This parameter enables or disables the GVRP port state. Doing so allows a port to become a VLAN member, dynamically. By default, this option is disabled.
Join Time	Enter the value of a join-time. The range is from 10 to 10,000 (centiseconds). By default, the value is set to 20 centiseconds.
Leave Time	Enter the value for leave time; the range is from 10 to 10,000 centi-seconds. Enter the value of leave time. The range is from10 to 10,000 (centiseconds). By default, the value is set to 60 centiseconds.
Leave All Time	Enter the value for Leave All time. The range is from 10 to 10,000 (centiseconds). By default, the value is set to 1,000 (centiseconds).

Click **Apply** to reflect the change.

5.2.3.3 GVRP Advertise VLAN

Use the following window to implement the settings on GVRP advertise VLAN and display its settings.

Choose **L2 Features > VLAN > GVRP > GVRP Advertise VLAN** to display the following window.

Figure 5-14 GVRP Advertise VLAN

In the section of **GVRP Advertise VLAN**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Action	Choose the advertise VLAN to use for a port mapping action. The options available are All , Add , Delete and Replace . If you choose All , all the advertise VLANs are used.
Advertise VID List	Enter a VLAN ID to advertise it. You can enter its consecutive VLAN IDs by delimiting with a comma. Or, you can enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.

Click **Apply** to reflect the change.

5.2.3.4 GVRP Forbidden VLAN

Use the following window to implement the settings on GVRP forbidden VLAN and display its settings.

Choose **L2 Features > VLAN > GVRP > GVRP Forbidden VLAN** to display the following window.

Figure 5-15 GVRP Forbidden VLAN

In the section of **GVRP Forbidden VLAN**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Action	Choose the forbidden VLAN to use for a port mapping action. The value to choose are All , Add , Delete and Replace . Click All , and then all the forbidden VLANs are used.
Forbidden VID List	Enter a VLAN ID to forbid it. You can enter its consecutive VLAN IDs, by delimiting with a comma, or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.

Click **Apply** to reflect the change.

5.2.3.5 GVRP Statistics Table

Use the following window to display and clear the GVRP statistics.

Choose **L2 Features > VLAN > GVRP > GVRP Statistics Table** to display the following window.

Port		JoinEmpty	JoinIn	LeaveEmpty	LeaveIn	LeaveAll	Empty
F11/0/1	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
F11/0/2	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
F11/0/3	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
F11/0/4	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
Te11/0/5	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
Te11/0/6	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0

Figure 5-16 GVRP Statistics Table

In the section of **GVRP Statistics Table**, you can configure the following parameter.

Parameter	Overview
Port	Choose the port you use.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **Clear** to clear the statistics information from the port specified.

Click **See All** to search and display all the entries available.

Click **Clear All** to clear all the statistics information from all the ports.

5.2.4 Asymmetric VLAN

Use the following window to implement the settings on an asymmetric VLAN and display its settings.

Choose **L2 Features > VLAN > Asymmetric VLAN** to display the following window.

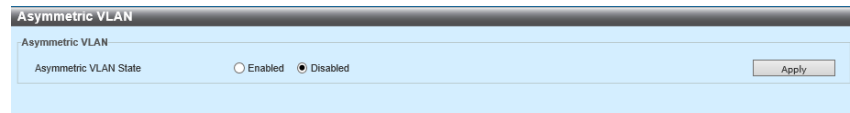


Figure 5-17 Asymmetric VLAN

In the section of the **Asymmetric VLAN**, you can configure the following parameter.

Parameter	Overview
Asymmetric VLAN State	This parameter enables or disables the function of the asymmetric VLAN.

Click **Apply** to reflect the change.

5.2.5 MAC VLAN

Use the following window to implement the settings on a MAC based VLAN. Then, a static MAC based VLAN entry is configured. If this is associated with a port, the VLAN operating on the port becomes changed.

Choose **L2 Features > VLAN > MAC VLAN** to display the following window.

Figure 5-18 MAC VLAN

In the section of **MAC VLAN**, you can configure the following parameters.

Parameter	Overview
MAC Address	Enter the Unicast MAC address.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
Priority	Choose the priority (value) to allocate for untagged-packets. You can specify the value within the range from 0 to 7.

Click **Apply** to add new entries based on the information specified.

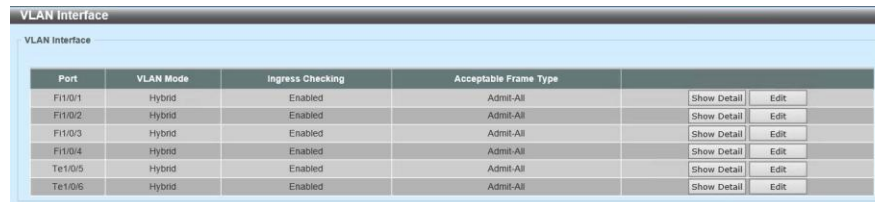
Click **Delete** to delete the entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

5.2.6 VLAN Interface

Use the following window to implement the settings on the VLAN interface and display its settings.

Choose **L2 Features > VLAN > VLAN Interface** to display the following window.



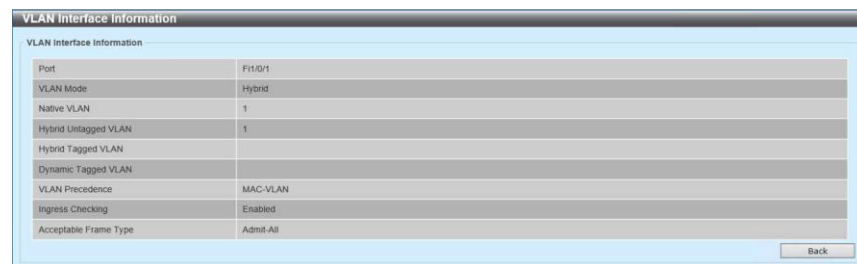
Port	VLAN Mode	Ingress Checking	Acceptable Frame Type	Show Detail	Edit
F11/0/1	Hybrid	Enabled	Admit-All	Show Detail	Edit
F11/0/2	Hybrid	Enabled	Admit-All	Show Detail	Edit
F11/0/3	Hybrid	Enabled	Admit-All	Show Detail	Edit
F11/0/4	Hybrid	Enabled	Admit-All	Show Detail	Edit
Te1/0/5	Hybrid	Enabled	Admit-All	Show Detail	Edit
Te1/0/6	Hybrid	Enabled	Admit-All	Show Detail	Edit

Figure 5-19 VLAN Interface

Click **Show Detail** to display details on the entry.

Click **Edit** to edit the entry-settings.

Click **Show Detail** to display the following window.



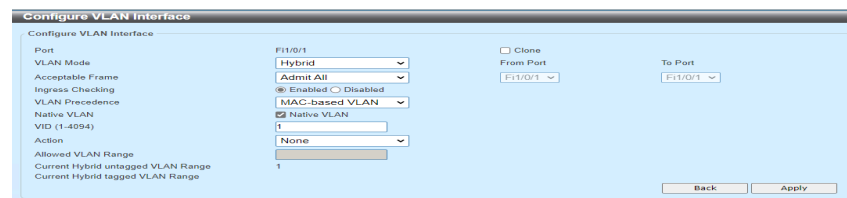
VLAN Interface Information	
Port	F11/0/1
VLAN Mode	Hybrid
Native VLAN	1
Hybrid Untagged VLAN	1
Hybrid Tagged VLAN	
Dynamic Tagged VLAN	
VLAN Precedence	MAC-VLAN
Ingress Checking	Enabled
Acceptable Frame Type	Admit-All

Back

Figure 5-20 VLAN Interface (Show Detail.)

Click **Back** to return to the previous window.

Click **Edit** to display the following window.



Configure VLAN Interface	
Port	F11/0/1
VLAN Mode	Hybrid
Acceptable Frame	Admit All
Ingress Checking	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
VLAN Precedence	MAC-based VLAN
Native VLAN	<input checked="" type="checkbox"/> Native VLAN
VID (1-4094)	1
Action	None
Allowed VLAN Range	
Current Hybrid untagged VLAN Range	1
Current Hybrid tagged VLAN Range	

Back Apply

Figure 5-21 VLAN Interface (Edit and Access)

In the section of **VLAN Interface Settings**, you can configure the following parameters.

Parameter	Overview
VLAN Mode	Choose the option of VLAN mode. The options available are Access , Hybrid , Trunk , Promiscuous and Host .
Acceptable Frames	Choose an operating option for acceptable frames. The options available are Tagged only , Untagged only and Admit All .
Checking Ingress	This parameter enables or disables the function of checking ingress.
VLAN ID	Enter the VLAN ID you use for this configuration. The range is from 1 to 4,094.
Clone	If you choose this option, you need to enable a clone function.
From Port/ To Port	Choose the port you use.

Click **Apply** to reflect the change.

Click **Back** to return to the previous window.

Choose **Hybrid** from **VLAN Mode** to display the following window.

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

- Port:** F11/0/2
- VLAN Mode:** Hybrid
- Acceptable Frame:** Admit All
- Ingress Checking:** Enabled (radio button selected)
- VLAN Precedence:** MAC-based VLAN
- Native VLAN:** ☒ Native VLAN
- VID (1-4094):** 1
- Action:** None
- Allowed VLAN Range:** 1
- Current Hybrid untagged VLAN Range:** 1
- Current Hybrid tagged VLAN Range:** 1
- Clone:** ☐ Clone
- From Port:** F11/0/1
- To Port:** F11/0/1

Buttons at the bottom: Back, Apply

Figure 5-22 VLAN Interface (Edit and Hybrid)

In the section of **VLAN Interface Settings**, you can configure the following parameters.

Parameter	Overview
VLAN Mode	Choose the option of VLAN mode. The options available are Access , Hybrid , Trunk , Promiscuous and Host .
Acceptable Frames	Choose an operating option for acceptable frames. The options available are Tagged only , Untagged only and Admit All .
Checking Ingress	This parameter enables or disables the function of checking Ingress.
VLAN Precedence	Choose an option for VLAN Precedence. The options available are MAC based VLAN and Subnet based VLAN .
Native VLAN	If you set this option to on, the native VLAN function becomes enabled.
VID	This parameter becomes available if Native VLAN option is set to on. Enter the VLAN ID you use. The range is from 1 to 4,094.
Action	Choose the action you perform (or execute). The options available are Nothing , Add , Delete , Tag and Untag .
Adding Mode	Choose to add one of these parameters: untagged and tagged.
VLAN Range Allowed	Enter the VLAN range allowed.
Clone	If you choose this option, you need to enable the clone function.
From Port/ To Port	Choose the port you use.

Click **Apply** to reflect the change.

Click **Back** to return to the previous window.

Choose **Trunk** on the **VLAN Mode** to display the following window.

Figure 5-23 VLAN Interface (Edit and Trunk)

In the section of **VLAN Interface Settings**, you can configure the following parameters.

Parameter	Overview
VLAN Mode	Choose the option of VLAN mode. The options available are Access , Hybrid , Trunk , Promiscuous and Host .
Acceptable Frames	Choose an operating option for acceptable frames. The options available are Tagged only , Untagged only and Admit All .
Checking Ingress	This parameter becomes available if you choose Trunk from VLAN Mode . This action enables or disables the function of checking Ingress.
Native VLAN	If you set this option to on, the native VLAN function becomes enabled. In addition, choose Untagged or Tagged as the frame to support on this VLAN.
VID	This parameter will be available if the Native VLAN option is set to on. Enter the VLAN ID you use. The range is from 1 to 4,094.
Action	Choose the action you perform. The options available are Nothing , All , Add , Delete , Except and Replace .
VLAN Range Allowed	Enter the VLAN range allowed.
Clone	If you choose this option, you need to enable the clone function.
From Port/ To Port	Choose the port you use.

Click **Apply** to reflect the change.

Click **Back** to return to the previous window.

Choose **Promiscuous** from **VLAN Mode** to display the following window.

Figure 5-24 VLAN Interface (Edit and Promiscuous)

In the section of **VLAN Interface Settings**, you can configure the following parameters.

Parameter	Overview
VLAN Mode	Choose an option of VLAN mode. The options available are Access , Hybrid , Trunk , Promiscuous and Host .

Parameter	Overview
Acceptable Frames	Choose an operating option for acceptable frames. The options available are Tagged only , Untagged only and Admit All .
Checking Ingress	This parameter enables or disables the function of checking ingress.
Clone	If you choose this option, you need to enable the clone function.
From Port/ To Port	Choose the port you use.

Click **Apply** to reflect the change.

Click **Back** to return to the previous window.

Choose **Host** from **VLAN Mode** to display the following window.

Figure 5-25 VLAN Interface (Edit and Host)

In the section of **VLAN Interface Settings**, you can configure the following parameters.

Parameter	Overview
VLAN Mode	Choose the option of VLAN mode. The options available are Access , Hybrid , Trunk , Promiscuous and Host .
Acceptable Frames	Choose an operating option for acceptable frames. The options available are Tagged only , Untagged only and Admit All .
Checking Ingress	This parameter enables or disables the function of checking ingress.
Clone	If you choose this option, you need to enable a clone function.
From Port/ To Port	Choose the port you use.

Click **Apply** to reflect the change.

Click **Back** to return to the previous window.

5.2.7 Subnet VLAN

Use the following window to implement the settings on a subnet VLAN and display its settings. Configure the subnet VLAN. If you receive untagged IP packets or priority tag IP packets through a port, both of them are cross-checked (along) with the subnet VLAN entry by using the source IP address. If the source IP is included in the entry subnet, the packets are grouped (or classified) into the VLAN, which is defined on the subnet.

Choose **L2 Features > VLAN > Subnet VLAN** to display the following window.

Subnet VLAN

Subnet VLAN

☒ IPv4 Network Prefix/Prefix Length 20.0.1.0/8 ☐ IPv6 Network Prefix/Prefix Length 8FEE::/64

Length

VID (1-4094) Priority 0 Apply

Total Entries: 0

Subnet	VID	Priority
--------	-----	----------

Figure 5-26 Subnet VLAN

In the section of the **Subnet VLAN**, you can configure the following parameters.

Parameter	Overview
IPv4 Network Prefix / Prefix Length	Choose and enter the value of an IPv4 address of the subnet VLAN and its prefix-length.
IPv6 Network Prefix / Prefix Length	Choose and enter the value of an IPv6 address of the subnet VLAN and its prefix length.
VID	Enter a subnet VLAN ID to use. The range is from 1 to 4,094.
Priority	Choose the priority value to use. You can specify the value within the range from 0 to 7. The lower the value, the higher its priority will be.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete the entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

5.2.8 Voice VLAN

5.2.8.1 Voice VLAN Global

Use the following window to implement the settings on a global voice VLAN. Enable or disable to set a voice VLAN function to global, and then specify the voice VLAN of a switch. The number of voice VLANs to specify for the switch is one, only.

Choose **L2 Features > VLAN > Voice VLAN > Voice VLAN Global** to display the following window.

Figure 5-27 Voice VLAN Global

In the section of the **Voice VLAN Global**, you can configure the following parameters.

Parameter	Overview
Voice VLAN State	This parameter enables or disables to set the voice VLAN function to global.
Voice VLAN ID	Enter a VLAN ID for the voice VLAN. Before the settings, the VLAN specified as the voice VLAN must exist beforehand, and the range is from 2 to 4,094.
Voice VLAN CoS	Enter CoS of the voice VLAN. The range is from 0 to 7. The voice packets arriving at the voice VLAN corresponding-ports are marked as the CoS specified. You can distinguish between voice VLAN traffics and data traffics of QoS (Quality of Service) by including annotations for CoS packets.
Aging-Time	Enter the aging-time. This parameter configures the aging-time and voice VLAN information to age out the voice device, which automatically learned. If the last voice device, which is connected to a port, stops transmitting traffics and a MAC address of the voice device ages out from FDB, the aging-timer of the voice VLAN activates. If the deadline of the voice VLAN aging-timer expires, ports are removed from the voice VLAN. If the voice traffics restart during the aging-time, the aging-timer is canceled. The range is from 1 to 65,535 (minutes). The port becomes removed from the voice VLAN after the expiration of the voice VLAN aging-timer.

Click **Apply** to reflect the change.

5.2.8.2 Voice VLAN Port

Use the following window to implement the settings on a voice VLAN interface and display its settings.

Choose **L2 Features > VLAN > Voice VLAN > Voice VLAN Port** to display the following window.

Port	State	Mode
F11/0/1	Disabled	Auto/Untag
F11/0/2	Disabled	Auto/Untag
F11/0/3	Disabled	Auto/Untag
F11/0/4	Disabled	Auto/Untag
Te1/0/5	Disabled	Auto/Untag
Te1/0/6	Disabled	Auto/Untag

Figure 5-28 Voice VLAN Port

In the section of **Audio VLAN Port**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
State	This parameter enables or disables a voice VLAN function of the port specified. If you enable a voice LAN on the port, the voice packets received are transferred by the voice VLAN. Packets received are determined (or evaluated) as voice packets when a source MAC address of the packets complies with an OUI address.

Parameter	Overview
Mode	<p>Chooses a mode. The options available are as follows.</p> <ul style="list-style-type: none">• Auto Untagged - the untagged membership of the voice VLAN is automatically learned.• Auto-Tag - the tagged membership regarding the voice VLAN is learned automatically.• Manual - This configures the voice VLAN membership, manually. <p>If the automatic learning is enabled, ports are automatically learned as the voice VLAN member. This membership ages out, automatically. If a port operates as the auto-tagged mode and captures the voice device through the device OUI, the port automatically participates in the voice VLAN as the tagged member. If the voice device transmits tagged packets, the switch changes its priority. If the voice device transmits untagged packets, they are transferred by PVID (Port VLAN ID). If a port operates as the auto-untagged mode and captures the voice device through the device OUI, the port automatically participates in the voice VLAN as the untagged member. If the voice device transmits tagged packets, the switch changes its priority. If the voice device transmits untagged packets, they are transferred through the voice VLAN. If the switch receives LLDP-MED (LLDP Media Endpoint Discovery) packets, it checks the priority-flag. Switches follow the tagged flag and the priority settings.</p>

Click **Apply** to reflect the change.

5.2.8.3 Voice VLAN OUI

Use the following window to implement the settings on voice VLAN OUI and display its settings. You can associate the OUI of a user definition with the voice VLAN. If a source MAC address of packets received corresponds with an optional OUI pattern, the packets received are evaluated as voice packets. The default OUI cannot be either deleted or specified because of the duplication.

Choose **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI** to display the following window.

Figure 5-29 Voice VLAN OUI

In the section of **Voice VLAN OUI**, you can configure the following parameters.

Parameter	Overview
OUI Address	Enter one MAC address for voice VLAN OUI.
Mask	Enter the bit mask, which corresponds with a MAC address of voice VLAN OUI.
Description	Fill out an overview for describing a MAC address of user-definition OUI. The number of character strings can be up to 32.

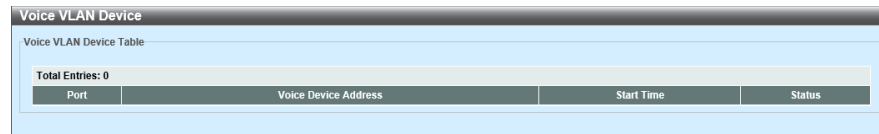
Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete the entry.

5.2.8.4 Voice LAN Device

Use the following window to display a table of the voice VLAN device and its information.

Choose **L2 Features > VLAN > Voice VLAN > Voice VLAN Device** to display the following window.



The screenshot shows a window titled "Voice VLAN Device". Inside, there is a section labeled "Voice VLAN Device Table". Below this, it says "Total Entries: 0". A table with four columns is shown: "Port", "Voice Device Address", "Start Time", and "Status". The table is currently empty.

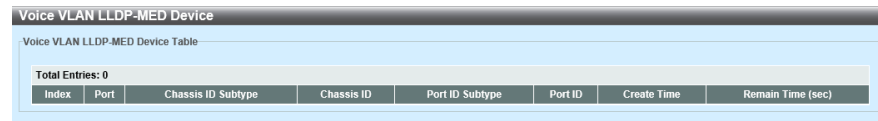
Port	Voice Device Address	Start Time	Status
------	----------------------	------------	--------

Figure 5-30 Voice VLAN Device

5.2.8.5 Voice VLAN LLDP-MED Device

Use the following window to display a table of the voice VLAN LLDP-MED device and its information.

Choose **L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device** to display the following window.



Index	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Create Time	Remain Time (sec)
-------	------	--------------------	------------	-----------------	---------	-------------	-------------------

Figure 5-31 Voice VLAN LLDP-MED Device

5.2.9 Private VLAN

Use the following window to implement the settings on a private VLAN and display its settings.

Choose **L2 Features > VLAN > Private VLAN** to display the following window.

Figure 5-32 Private VLAN

In the section of the **Private VLAN**, you can configure the following parameters.

Parameter	Overview
VID List	Enter a private VLAN ID to use. You can enter its consecutive VLAN IDs, by delimiting with a comma, or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.
State	This parameter enables or disables the private VLAN state.
Type	Choose a private VLAN type to create. The options available are Community , Isolated and Primary .

Click **Apply** to reflect the change.

In the section of **Private VLAN Association**, you can configure the following parameters.

Parameter	Overview
VID List	Enter the private VLAN ID you use. You can enter its consecutive VLAN IDs, by delimiting with a comma, or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.
Action	Choose an action to execute on the private VLAN. The options available are Add , Delete and Disable .
Secondary VID List	Enter a secondary private VLAN ID to use it. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.

Click **Apply** to reflect the change.

In the section of the **Private VLAN Host Association**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Primary VID	Enter the primary VLAN ID you use. The range is from 1 to 4,094.
Secondary VID	Enter the secondary VLAN ID you use. The range is from 1 to 4,094. If the option of Remove Association is set to on, this settings does not become enabled.

Click **Apply** to reflect the change.

In the section of the **Private VLAN Mapping**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Primary VID	Enter the primary VLAN ID you use. The range is from 1 to 4,094.
Action	Click Add to add a new entry based on the information entered. Click Remove to remove an entry based on the information entered.
Secondary VID List	Enter the secondary VLAN ID you use. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094. If an option of Remove Mapping is set to on, this configuration does not become enabled.

Click **Apply** to reflect the change.

5.3 STP (Spanning Tree Protocol)

5.3.1 STP Global Settings

Use the following window to implement the settings on global STP and display its settings.

Choose **L2 Features > STP > STP Global Settings** to display the following window.

The screenshot shows the 'STP Global Settings' window. It is divided into four main sections. The first section, 'STP State', has a radio button for 'Disabled' which is selected, and an 'Apply' button. The second section, 'STP Mode', has a dropdown menu showing 'RSTP' and an 'Apply' button. The third section, 'STP Priority', has a dropdown menu showing '32768' and an 'Apply' button. The fourth section, 'STP Configuration', contains four input fields: 'Bridge Max Age (6-40)' with value '20', 'Bridge Hello Time (1-2)' with value '2', 'Bridge Forward Time (4-30)' with value '15', and 'Max Hops (1-40)' with value '20'. There is also a 'TX Hold Count (1-10)' field with value '6'. An 'Apply' button is located at the bottom right of this section.

Figure 5-33 STP Global Settings

In the section of the **STP State**, you can configure the following parameter.

Parameter	Overview
STP State	This parameter enables or disables the global STP state.

Click **Apply** to reflect the change.

In the section of an **STP Mode**, you can configure the following parameter.

Parameter	Overview
STP Mode	Choose the STP mode you use. The options available are MSTP , RSTP and STP . MSTP stands for Multiple Spanning Tree Protocol, RSTP for Rapid Spanning Tree Protocol, and STP for Spanning Tree Protocol.

Click **Apply** to reflect the change.

In the section of an **STP Priority**, you can configure the following parameter.

Parameter	Overview
Priority	Choose the value of an STP priority. You can specify the value within the range from 0 to 61,440. By default, the value is 32,768. The lower the value, the higher priority will be.

Click **Apply** to reflect the change.

In the section of an **STP Configuration**, you can configure the following parameters.

Parameter	Overview
Bridge Max Age	Enter the value of bridge-maximum age. The range is from 6 to 40 (seconds). By default, the value is 20 (seconds). Set the value of the maximum age to ensure that old information does not circulate limitlessly through redundant paths in the network; the effective propagation of new information is not prevented. As the value is set to a root bridge, it is useful to evaluate that the settings of a spanning tree of the switch is the same with other devices of a bridge VLAN.
Bridge Hello Time	This parameter becomes available if you choose RSTP or STP on the STP Mode . Enter the value of hello time for a bridge. The range is from 1 to 2 (seconds). By default, the value is 2 (seconds). This is the interval for transmitting BPDU (Bridge Protocol Data Unit) packets whose root bridge is twice, to inform that it is a root bridge on all of other switches. This field is displayed when you choose an STP or RSTP (Rapid Spanning Tree Protocol) as the STP version. In the case of an MSTP, the hello-time needs to be configured as a port-unit.
Bridge Forward Time	Enter the value of bridge-forward time. The range is from 4 to 30 (seconds). By default, the value is 15 (seconds). This means the time for listening condition when all the ports of a switch migrate (or move) from the blocking state to a forwarding state.
TX Hold Count	Enter the value of a transmission hold count. The range is from 1 to 10 (times). By default, the value is 6 (times). Use the value to configure the maximum number of hello packets, which are transmitted with the predetermined interval.

Parameter	Overview
Max Hops	Enter the maximum number (value) of hops to allow. The range is from 6 to 40 (hops). By default, the value is equal to 20 (hops). Use the value to configure the number of hops between devices existing in a domain of a spanning tree before removing BPDU packets, which are transmitted by a switch. Hop-counting decreases one by one every time a switch passes until the value reaches 0. After that, the switch deletes the BPDU packets, and then the information (or data) retained in the port ages out.

Click **Apply** to reflect the change.

5.3.2 STP Port Settings

Use the following window to implement the settings on STP ports and display its settings.

Choose **L2 Features > STP > STP Port Settings** to display the following window.

Port	State	Cost	Guard Root	Link Type	Port Fast	TCN Filter	BPDU Forward	Priority
F1/0/1	Enabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Disabled	128
F1/0/2	Enabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Disabled	128
F1/0/3	Enabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Disabled	128
F1/0/4	Enabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Disabled	128
Te1/0/5	Enabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Disabled	128
Te1/0/6	Enabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Disabled	128

Figure 5-34 STP Port Settings

In the section of **STP Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port Ports to apply	Choose the port you use.
Cost	Enter the cost value. The range is from 1 to 200,000,000. the value defines the metric, which indicates a relative cost of a forwarding packets to the port list specified. The port cost can be set as the metric value or automatically. The default value is [0] (automatic). If you set 0 to the external cost, the speed of forwarding packets to the specified port is automatically set on a list of the optimal efficiency. The default port of 100Mbps port costs 200,000, and it costs 20,000 for a Gigabit port. The lower the numerical value, the higher possibility of transferring packets (from the port) will be.
State	This parameter enables or disables an STP port state.
Guard Route	This parameter enables or disables a guard route function.
Link Type	Choose the link type option. The options available are Auto , P2P and Share . A full-duplex port is considered to have a Point-to-Point (P2P) connection. On the other hand, a half-duplex port is considered to have a shared connection. The port cannot migrate to the forwarding state promptly by setting the link type to Shared . By default, this option is set to Auto .

Parameter	Overview
Port-Fast	<p>Choose the port-fast option. The options available are as follows.</p> <ul style="list-style-type: none"> • Network - The port keeps remained in the non-port-fast state for three seconds. If no BPDU is received, the port becomes the port-fast state, and then its state becomes changed to the forwarding state. If the port receives the BPDU later, the port becomes changed to the non-port-fast state. • Disabled - Always, the port keeps the non-port-fast state. Always, it waits until the forwarding state. After that, the forward-time delay occurs. • Edge - If a link-up occurs, the port directly transits to the state of spanning-tree forwarding without waiting for the forward time delay. • If the interface receives the BPDU later, its operation state changes to the non-port-fast state. By default, this option is set to Network.
TCN Filtering	<p>This parameter enables or disables an option of Topology Change Notification (TCN) filtering. If a port is set to the TCN filtering mode, TC events received by a port are ignored. By default, this option is set to disabled.</p>
BPDU Forwarding	<p>This parameter enables or disables BPDU forwarding. If enabled, the STP BPDU received are transferred to all the VLAN member ports with the untagged form. By default, this option is set to disabled.</p>
Priority	<p>Choose the priority value. The range of values to choose is from 0 to 240. By default, this option is set to 128. The lower the value, the higher priority will be.</p>
Hello Time	<p>Enter the value of hello time. The range is from 1 to 2 (seconds). the value specifies an interval for a representative port to wait during periodic transmissions of each configuration message.</p>

Click **Apply** to reflect the change.

5.3.3 MST Configuration Identification

Use the following window to implement the settings on an MST configuration ID and display its settings. This configuration allows you to identify the Multiple Spanning Tree Instance (MSTI), which is configured on a switch.

The default of Common Internal Spanning Tree (CIST) can be changed, but cannot be deleted. In addition, the MSTI ID cannot be changed.

Choose **L2 Features > STP > MST Configuration Identification** to display the following window.

Figure 5-35 MST Configuration Identification

In the section of **MST Configuration Identification**, you can configure the following parameters.

Parameter	Overview
Configuration Name	Enter an MST. This name identifies an MSTI uniquely. If you do not configure a configuration name, a MAC address for the device, which executes an MSTP, is displayed in this field.
Revision Level	Enter the value of a revision level. The range is from 0 to 65,535. By default, the value is set to 0. The value identifies the MSTP domain, which is configured on a switch along with the configuration name.

Click **Apply** to reflect the change.

In the section of the **Instance ID Settings**, you can configure the following parameters.

Parameter	Overview
Instance ID	Enter an Instance ID. The range is from 1 to 64.
Action	Choose the action you perform. The options available are Adding VID and Deleting VID .
VID List	Enter the VLAN ID you use. You can enter its consecutive VLAN IDs by delimiting with a comma. Or, you can enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.

Click **Apply** to reflect the change.

Click **Edit** to edit the entry-settings.

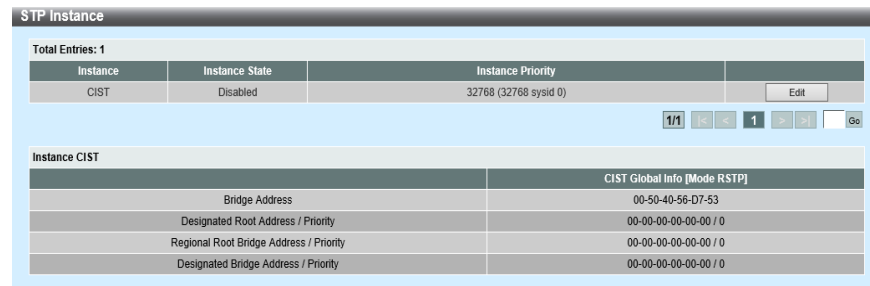
Click **Delete** to delete the entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

5.3.4 STP Instance

Use the following window to implement the settings on an STP instance. and display its settings.

Choose **L2 Features > STP > STP Instance** to display the following window.



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

1/1 < < 1 > > Go

Parameter	CIST Global Info [Mode RSTP]
Bridge Address	00-50-40-56-D7-53
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 5-36 STP Instance

In the section of the **STP Instance**, you can configure the following parameter.

Parameter	Overview
Instance Priority	After you click Edit , enter the value of the instance priority. The range is from 0 to 61,440.

Click **Edit** to edit the entry-settings to move to a specific page

If two or more pages exist, enter the page-numbers. Then click **Go** to move to a specific page.

5.3.5 MSTP Port Information

Use the following window to implement the settings and display MSTP port information.

Choose **L2 Features > STP > MSTP Port Information** to display the following window.

Figure 5-37 MSTP Port Information

In the section of **MSTP Port Information**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
Cost	Click Edit , and then enter the cost value. The range is from 1 to 200,000,000.
Priority	Click Edit , and then enter the priority value. The range of values to choose is from 0 to 240 . By default, this option is set to 128. The lower the value, the higher priority will be.

Click the **Clear Detection Protocol** button to delete the association of the protocol detected from the port specified.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **Edit** to edit the entry-settings.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

5.4 Loop Detection Configuration

5.4.1 Detecting and Blocking the Loop Settings

Use the following window to implement the settings on detecting and blocking loops and display its settings.

Choose **L2 Features > Detecting and Blocking Loops > Detecting and Blocking Loops Settings** to display the following window.

Port	Link	State	Loop Detect	Mode	Recovery	Recovery Time
F11/0/1	Up	Forwarding	Enabled	Block	Enabled	60
F11/0/2	Up	Forwarding	Enabled	Block	Enabled	60
F11/0/3	Down	Forwarding	Enabled	Block	Enabled	60

Figure 5-38 Loop Detection Configuration

In the section of **Detecting and Blocking the Loop Settings**, you can configure the following parameters.

Parameter	Overview
Global State	This parameter enables or disables to set the function of detecting and blocking a loop.
From Port/ To Port	Choose the port you use.
State	This parameter enables or disables the function of a line loop-back of the port specified.
Mode	Choose the mode of detecting and blocking a loop to use on the port specified. The options available are as follows. <ul style="list-style-type: none"> • Shutdown - First, set a port to the shutdown condition when a loop occurs. Then set it to the blocking state. • Block - This allows you to set a port to the blocking state when a loop occurs.
Recovering Loops	This parameter enables or disables the function of recovering loops. If the function is set to enabled, ports become recovered to a normal condition after the value of time-out expires. Enter the entry field where the time-out value is displayed. The range is from 60 to 86,400 (seconds).

Click **Apply** to reflect the change.

5.4.2 Loop History Log

Use the following window to display and clear a loop history log.

Choose **L2 Features > Detecting and Blocking Loops > Loop History Log** to display the following window.



Figure 5-39 Loop History Log

Click the **Clear Log** button to clear log entries from a table.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

5.5 Link Aggregation

Use the following window to implement the settings on a link aggregation and display its settings.

Choose **L2 Features > Link Aggregation** to display the following window.

Figure 5-40 Link Aggregation

In the first section, you can configure the following parameters.

Parameter	Overview
System Priority	Enter the value of a system priority to use. The range is from 1 to 65,535. By default, the value is set to 32,768. The system priority determines the port, which enables a port to participate in a port-channel and to become the standalone mode. The lower the value, the higher priority will be. If there are two or more ports with the same priority, the priority is determined depending on the port-number.
Load Balance Algorithm	Choose a load balance algorithm to use. The value to choose 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 set to Source Destination MAC .

Click **Apply** to reflect the change.

In the section of **Channel Group Information**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Group ID	Enter the channel-group number. The range is from 1 to 32. If a physical port participates in a channel group for the first time, the port-channel is automatically created. One interface can participate in one channel group, only.

Parameter	Overview
Mode	Choose the mode option. The options available are Static , Active and Passive . If the Static mode is specified, the channel group type is static. If the Active or Passive mode is specified, the channel group type is the Link Aggregation Control Protocol (LACP). A channel group consists of static members or LACP members. As the type of channel group is determined, other types of interfaces cannot participate in its channel group.

Click **Add** to add a new entry based on the information specified.

Click **Delete Member Ports** to delete the member ports from the port-channel specified.

Click **Delete Channels** to delete entries.

Click **Show Detail** to display details on the entry.

Click **Show Detail** to display the following window.

The screenshot shows the 'Link Aggregation' configuration window. It has a title bar 'Link Aggregation'. Below the title bar, there are three input fields: 'System Priority (1-65535)' with the value '32768', 'Load Balance Algorithm' with a dropdown menu showing 'Source Destination MAC', and 'System ID' with the value '32768,00-50-40-63-03-55'. There are 'Apply' buttons next to each of these fields. Below these fields is a section titled 'Channel Group Information'. It contains four input fields: 'From Port' with a dropdown menu showing 'Fi1/0/1', 'To Port' with a dropdown menu showing 'Fi1/0/1', 'Group ID (1-6)' with an empty text box, and 'Mode' with a dropdown menu showing 'Static'. There are 'Add' and 'Delete Member Port' buttons to the right of the 'Mode' dropdown. Below the 'Channel Group Information' section is a note: 'Note: Each Channel Group supports up to 8 member ports.' At the bottom, there is a table with the header 'Total Entries: 0' and a table with five columns: 'Channel Group', 'Protocol', 'Max Ports', 'Member Number', and 'Member Ports'. The table is currently empty.

Figure 5-41 Link Aggregation (Show Detail.)

Click **Edit** to edit the entry settings.

Click **Back** to return to the previous window.

5.6 L2 Protocol Tunnel

Use the following window to implement the settings on layer 2 protocol tunnel and display its settings.

Choose **L2 Features > L2 Protocol Tunnel** to display the following window.

Protocol	Drop Counter	Tunneling Address
GVRP	0	00-C0-8F-04-92-C1
STP	0	00-C0-8F-04-92-C0
01-00-0C-CC-CC-CC	0	00-C0-8F-04-92-C2
01-00-0C-CC-CC-CD	0	00-C0-8F-04-92-C3

Figure 5-42 L2 Protocol Tunnel (L2 Protocol Tunnel Global Settings)

In the section of the **L2 Protocol Tunnel Global Settings**, you can configure the following parameters.

Parameter	Overview
CoS for Encapsulated Packets	Choose the CoS value for encapsulated packets. Specify the value within the range from 0 to 7. When you choose Default , use the default value.
Drop Threshold	Enter the drop threshold. The range is from 100 to 20,000. By default, the value is set to 0. The tunneling of the layer 2 protocol packets consumes the throughput (capacity) for encrypting, decoding and transferring packets. Use this option to limit the consumption of CPU processing bandwidth. Specify the threshold for the number of all the layer 2 protocol packets, which can be processed through the system. The protocol packets, which exceed the maximum number of packets, will be removed. When you choose Default , use the default value.
Action	Choose the action you perform. The options available are Add or Delete . This option allows you to add the address of a Layer 2 Protocol Tunneling (L2PT) Multicast on the protocol specified. Or, the option allows you to delete the address above from the protocol specified.

Parameter	Overview
Tunneled Protocol	Choose a tunneled protocol. The options available are as follows. <ul style="list-style-type: none"> • GVRP - GVRP packets are tunneled to the address, which is configured already. • STP - STP packets are tunneled to the address, which is configured already. • MAC - Protocol packets with the specific destination address are tunneled to the address configured. • All - All packets are tunneled to the address, which is configured already.
Protocol MAC	After choosing the MAC option as a Tunneled Protocol , choose the destination address, which is tunneled on the address configured. The options available are 01-00-0C-CC-CC-CC and 01-00-0C-CC-CC-CD .
MAC Address	Enter a MAC address as the tunneling destination for the protocol specified. For this MAC address, you cannot specify the address, which is reserved or used by other protocols.

Click **Apply** to reflect the change.

Choose the **L2 Protocol Tunnel Port Settings** tab to display the following window.

Figure 5-43 L2 Protocol Tunnel (L2 Protocol Tunnel Port Settings)

In the section of **L2 Protocol Tunnel Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Action	Click Add to add a new entry based on the information entered. Click Delete to delete an entry based on the information entered.
Type	Choose the type option. The options available are None , Shutdown and Drop .
Tunneled Protocol	Choose the tunneled protocol option. The options available are GVRP , STP , Protocol MAC and ALL .

Parameter	Overview
Protocol MAC	After choosing Protocol MAC as the Tunneled Protocol , the following options are available. Choose Protocol MAC from it. The options available are 01-00-0C-CC-CC-CC and 01-00-0C-CC-CC-CD .
Threshold	If you choose Shutdown or Removal in the Type field, this parameter becomes available. Enter the threshold value. The range is from 1 to 4,096.

Click **Apply** to add new entries based on the information specified.

Click **Clear All** to clear information from all the entries.

Click **Clear** to clear information from the entry.

5.7 L2 Multicast Control

5.7.1 IGMP Snooping

5.7.1.1 IGMP Snooping Settings

Use the following window to implement the settings on IGMP (Internet Group Management Protocol) Snooping and display its settings.

Choose **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings** to display the following window.

Figure 5-44 IGMP Snooping Settings

In the section of **Global Settings**, you can configure the following parameter.

Parameter	Overview
Global State	This parameter enables or disables to set IGMP Snooping to global.

Click **Apply** to reflect the change.

In the section of **VLAN State Settings**, you can configure the following parameter.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Apply** to add new entries based on the information specified.

In the section of a table of **IGMP Snooping**, you can configure the following parameter.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

Click **Show Detail** to display details on the entry.

Click **Edit** to edit the entry-settings.

If two or more pages exist, enter the page numbers. Click **Go** to move to a specific page.

Click **Show Detail** to display the following window.

IGMP Snooping VLAN Parameters	
VID	1
Status	Enabled
Fast Leave	Disabled (host-based)
Querier State	Disabled
Query Version	v3
Query Interval	125 sec
Max Response Time	10 sec
Robustness Value	2
Last Member Query Interval	1 sec
Proxy Reporting	Disabled
Source Address	0.0.0.0
Rate Limit	0
Unknown Data Learning	Enabled
Unknown Data Expiry Time	Infinity

Modify

Figure 5-45 IGMP Snooping Settings (Show Detail.)

Click **Edit** to edit the settings.

Choose **Edit** or **Revise** to display the following window.

IGMP Snooping VLAN Settings

IGMP Snooping VLAN Settings

VID (1-4094)

Status ☒ Enabled ☐ Disabled

Fast Leave ☐ Enabled ☒ Disabled

Querier State ☐ Enabled ☒ Disabled

Query Version

Query Interval (1-31744) sec

Max Response Time (1-25) sec

Robustness Value (1-7)

Last Member Query Interval (1-25) sec

Proxy Reporting ☐ Enabled ☒ Disabled Source Address

Rate Limit (1-1000) ☒ No Limit

Unknown Data Learning ☒ Enabled ☐ Disabled

Unknown Data Expiry Time (1-65535) sec ☒ Infinity

Apply

Figure 5-46 IGMP Snooping Settings (Edit and Revise)

In the section of **IGMP Snooping VLAN Settings**, you can configure the following parameters.

Parameter	Overview
Fast Leave	This parameter enables or disables the function of the IGMP Snooping fast leave. If it is enabled and the IGMP leave messages are received, that makes members leave immediately.
Querier State	This parameter enables or disables the querier state.
Query Version	Choose the general query-packet version transmitted by an IGMP Snooping querier. The values to choose are 1 , 2 and 3 .
Query Interval	Enter the interval for an IGMP Snooping querier periodically to transmit general query messages of IGMP. The range is from 1 to 31,744.
Maximum Response Time	Enter the maximum response time (in second), which is advertised by an IGMP Snooping query. The range is from 1 to 25.
Robustness Variable	Enter the robustness variable to use it for IGMP Snooping. The range is from 1 to 7.
Final Member Query Interval	Enter the transmission interval of (channel) query messages of IGMP group unique or group source unique. The range is from 1 to 25.
Proxy Reporting	This parameter enables or disables the function of proxy reporting.
Source Address	Enter a source IP address of the proxy reporting. This option becomes enabled if you choose Enabled from Proxy Reporting .
Rate Limiting (or Band Limiting)	Enter the value of a band limiting. The range is from 1 to 1,000. If you set No Limitation to on, a band limiting is not applied for this profile.

Click **Apply** to reflect the change.

5.7.1.2 IGMP Snooping Group Settings

Use the following window to implement the settings on an IGMP Snooping group and display its settings.

Choose **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Group Settings** to display the following window.

Figure 5-47 IGMP Snooping Group Settings

In the section of **Static Group Settings on IGMP Snooping**, you can configure the following parameters.

Parameter	Overview
VID	Enter VLAN IDs to use. The range is from 1 to 4,094.
Group Address	Enter a group address of IP Multicast.
From Port/ To Port	Choose the port you use.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete the entries based on the information specified.

In the section of **IGMP Snooping Static Group Table**, you can configure the following parameters.

Parameter	Overview
VID	Choose and enter VLAN IDs to use. The range is from 1 to 4,094.
Group Address	Click the radio button, and then enter an address of an IP Multicast group.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

In the section of the **IGMP Snooping Group Table**, you can configure the following parameters.

Parameter	Overview
VID	Choose and enter VLAN IDs to use. The range is from 1 to 4,094.
Group Address	Click the radio button, and then enter an address of an IP Multicast group.
Details	This parameter displays details for an IGMP group.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

5.7.1.3 IGMP Snooping Filter Settings

Use the following window to implement the settings on the IGMP Snooping filtering and display its settings.

Choose **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Filter Settings** to display the following window.

The screenshot shows the 'IGMP Snooping Filter Settings' window. It contains the following sections:

- IGMP Snooping Rate Limit Settings:** Includes 'From Port' (F11/0/1), 'To Port' (F11/0/1), 'Limit Number (1-1000)' (empty), and a 'No Limit' checkbox. An 'Apply' button is present.
- IGMP Snooping Limit Settings:** Includes 'From Port' (F11/0/1), 'To Port' (F11/0/1), 'Limit Number (1-1024)' (empty), 'Exclude Action' (Default), 'Exclude ACL Name' (Please Select), and 'VID (1-4094)' (empty). An 'Apply' button is present.
- Access Group Settings:** Includes 'From Port' (F11/0/1), 'To Port' (F11/0/1), 'Action' (Add), and 'VID (1-4094)' (empty). An 'Apply' button is present.
- IGMP Snooping Filter Table:** Includes 'From Port' (F11/0/1), 'To Port' (F11/0/1), 'Find', and 'Show All' buttons. Below the table, it says 'Total Entries: 0' and 'No data to display'.

Figure 5-48 IGMP Snooping Filter Settings

In the section of the settings on **IGMP Snooping Bandwidth Limit**, you can configure the following parameters.

Parameter	Overview
From Port to Port: from the Beginning to the End	Choose the port you use. This is available only if you choose the port option for the following action.
Number of Limitations	Enter the number of limitations. Configure the rate of IGMP control packets, which can be processed on a specific interface by a switch. The range is from 1 to 1,000 (packets/per second). If you choose No Limitation , the limitation is removed.

Click **Apply** to reflect the change.

In the section of the settings on **IGMP Snooping Limitation**, you can configure the following parameters.

Parameter	Overview
From Port to Port: from the Beginning to the End	Choose the port you use.
Number of Limitations	Enter the number of limitations. Use this parameter to limit the number of IGMP cash-entries, which can be created. The range is from 1 to 4,096.
Exceed Action	Choose an exceed action. Use this parameter to specify the operation to process the group, which is newly recognized when exceeding the limitation. The options available are as follows. <ul style="list-style-type: none"> • Default - The default action is executed. • Drop - A new group is dropped. • Replace - A new group is replaced to the oldest group.
Except ACL Name	Enter the name of the standard IP access-list. The group (*,G) or channel (S,G), which are allowed based on the access list, are excluded from the limitation. To authorize a channel (S,G), specify "S" in the field of source-address of the access-list entry and "G" in the destination-address field. To authorize a group (*,G), specify "any" in the source-address field of the access-list entry and "G" in the destination-address field. The number of characters for the name can be up to 32. Or, click Please Select to search and choose the existing access list, which is configured by a switch, for using this configuration.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete entries based on the information specified.

In the section of the settings on **Access Group**, you can configure the following parameters.

Parameter	Overview
From Port to Port: from the Beginning to the End	Choose the port you use.
Action	Click Add to add a new entry based on the information entered. Click Delete to delete an entry based on the information entered.
ACL Name	Enter the name of the standard IP access-list. Specify "any" in the source-address field of the access-list entry and "G" in the destination-address field. The number of characters for the name can be up to 32. Or, choose Please Select to search and choose the existing access list, which is configured by a switch for using this configuration.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Apply** to reflect the change.

In the section of a table of **IGMP Snooping Filter**, you can configure the following parameter.

Parameter	Overview
From Port to Port: from the Beginning to the End	Choose the port you use.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

Click **Show Detail** to display details on the entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Show Detail** to display the following window.

IGMP Snooping Detail Filter Table		
Total Entries: 1		
Port: Gi1/0/1		
VID	Access Group	Groups/Channel Limit
	Not Configured	Not Configured

1/1 < > 1 > > Go

Back

Figure 5-49 IGMP Snooping Filter Settings (Show Detail.)

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Back** to return to the previous window.

5.7.1.4 IGMP Snooping Multicast Router Information

Use the following window to implement the settings on an IGMP Snooping Multicast router and display its settings.

Choose **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Multicast Router Information** to display the following window.

Figure 5-50 IGMP Snooping Multicast Router Information

In the section of the settings on **IGMP Snooping Multicast Router Port**, you can configure the following parameters.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
Configuration	Choose a port configuration. The options available are as follows. <ul style="list-style-type: none"> • Port - Makes the port configured become a static Multicast router port. • Forbidden-Port - Does not allow the ports configured to become a Multicast router port.
From Port/ To Port	Choose the port you use.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete entries based on the information specified.

In the section of a port table of **IGMP Snooping Multicast Router**, you can configure the following parameter.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

5.7.1.5 IGMP Snooping Statistics Settings

Use the following window to display and clear the IGMP Snooping statistics.

Choose **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings** to display the following window.

Figure 5-51 IGMP Snooping Statistics Settings

In the section of the **IGMP Snooping Statistics Settings**, you can configure the following parameters.

Parameter	Overview
Statistics	Choose an interface. The options available are All , VLAN and Port .
VID	Enter the VLAN ID you use. The range is from 1 to 4,094. This option is available if you choose VLAN from the Statistics drop-down list.
From Port/ To Port	Choose the port you use. This option is available if you choose Port from the Statistics drop-down list.

Click **Clear** to clear the statistics information based on the condition specified.

In the section of a table regarding the **IGMP Snooping Statistics**, you can configure the following parameters.

Parameter	Overview
Search Type	Choose the interface type. The options available are VLAN and Port .
VID	Enter the VLAN ID you use. The range is from 1 to 4,094. This option is available if you choose VLAN from the Search Type drop-down list
From Port/ To Port	Choose the port you use. This option is available if you choose Port from the Search Type drop-down list.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

5.7.2 MLD Snooping

5.7.2.1 MLD Snooping Settings

Use the following window to implement the settings on MLD Snooping (Multicast Listener Discovery Snooping) and display its settings.

Choose **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings** to display the following window.

Figure 5-52 MLD Snooping Settings

In the section of **Global Settings**, you can configure the following parameter.

Parameter	Overview
Global State	This parameter enables or disables the global state of MLD Snooping.

Click **Apply** to reflect the change.

In the section of **VLAN State Settings**, you can configure the following parameter.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Apply** to add new entries based on the information specified.

In the section of **MLD Snooping Table**, you can configure the following parameter.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

Click **Show Detail** to display details on the entry.

Click **Edit** to edit the entry-settings.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Show Detail** to display the following window.



MLD Snooping VLAN Parameters	
VID	1
Status	Enabled
Fast Leave	Disabled (host-based)
Querier State	Disabled
Query Version	v2
Query Interval	125 sec
Max Response Time	10 sec
Robustness Value	2
Last Member Query Interval	1 sec
Proxy Reporting	Disabled Source Address (::)
Rate Limit	0
Unknown Data Learning	Enabled
Unknown Data Expiry Time	Infinity

Modify

Figure 5-53 MLD Snooping Settings (Show Detail.)

Click **Edit** to edit the settings.

Click **Edit** or **Revise** to display the following window.

MLD Snooping VLAN Settings

MLD Snooping VLAN Settings

VID (1-4094)

Status ☒ Enabled ☐ Disabled

Fast Leave ☐ Enabled ☒ Disabled

Querier State ☐ Enabled ☒ Disabled

Query Version ▼

Query Interval (1-31744) sec

Max Response Time (1-25) sec

Robustness Value (1-7)

Last Member Query Interval (1-25) sec

Proxy Reporting ☐ Enabled ☒ Disabled Source Address

Rate Limit (1-1000) ☒ No Limit

Unknown Data Learning ☒ Enabled ☐ Disabled

Unknown Data Expiry Time (1-65535) sec ☒ Infinity

Figure 5-54 MLD Snooping Settings (Edit and Revise)

In the section of **IGMP Snooping VLAN Settings**, you can configure the following parameters.

Parameter	Overview
Fast Leave	This parameter enables or disables the function of the MLD Snooping fast-leave. If enabled, the membership is immediately removed when the system receives the MLD leave messages.
Proxy Reporting	This parameter enables or disables the function of the proxy reporting.
Source Address	Enter one source IP address of a proxy reporting. This option is enabled if you choose Enabled from Proxy Reporting .
Querier State	This parameter enables or disables the querier state.
Query Version	Choose the general query packet version transmitted by the MLD Snooping querier. The values to choose are 1 and 2 .
Query Interval	Enter the interval at which the MLD Snooping querier periodically sends general MLD query messages. The range is from 1 to 31,744.
Maximum Response Time	Enter the maximum response time (in seconds), advertised in MLD Snooping queries. The range is from 1 to 25.
Robustness Value	Enter the robustness variable to use it for MLD Snooping. The range is from 1 to 7.
Final Listener Query Interval	Enter the transmission interval of query-messages which are unique to MLD group or group source (channel) due to the MLD Snooping querier. The range is from 1 to 25.
Band Limitation (or Rate Limitation)	Enter the value of the band limitation (or rate limitation). The range is from 1 to 1,000. If you set No Limitation to on, no band limitation is applied for this profile.

Click **Apply** to reflect the change.

5.7.2.2 MLD Snooping Group Settings

Use the following window to implement the settings on an MLD Snooping group and display its settings.

Choose **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Group Settings** to display the following window.

Figure 5-55 MLD Snooping Group Settings

In the section of the settings on **MLD Snooping Static Group**, you can configure the following parameters.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
Group Address	Enter a group address for IPv6 Multicast.
From Port to Port: from the Beginning to the End	Choose the port you use.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete entries based on the information specified.

In the section of a table of **MLD Snooping Static Group**, you can configure the following parameters.

Parameter	Overview
VID	Choose and enter VLAN IDs to use. The range is from 1 to 4,094.
Group Address	Click the Radio button, and then enter an address of an IPv6 Multicast Group.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

In the section of **MLD Snooping Group Table**, you can configure the following parameters.

Parameter	Overview
VID	Choose and enter VLAN IDs to use. The range is from 1 to 4,094.
Group Address	Click the Radio button, and then enter an address of an IPv6 Multicast Group.
Details	If you choose this option, the details on MLD group are displayed.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

5.7.2.3 MLD Snooping Filter Settings

Use the following window to implement the settings on the MLD Snooping filtering and display its settings.

Choose **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Filtering Settings** to display the following window.

The screenshot shows the 'MLD Snooping Filter Settings' window. It contains the following sections:

- MLD Snooping Rate Limit Settings:** Includes 'From Port' (F1/0/1), 'To Port' (F1/0/1), and 'Limit Number (1-1000)' (No Limit). An 'Apply' button is present.
- MLD Snooping Limit Settings:** Includes 'From Port' (F1/0/1), 'To Port' (F1/0/1), 'Limit Number (1-1024)', 'Enforce ACL Name' (VID (1-4094)), and 'Enforce Action' (Default). An 'Apply' button is present.
- Access Group Settings:** Includes 'From Port' (F1/0/1), 'To Port' (F1/0/1), 'Action' (Add), and 'ACL Name' (VID (1-4094)). An 'Apply' button is present.
- MLD Snooping Filter Table:** Includes 'From Port' (F1/0/1), 'To Port' (F1/0/1), and 'Find' and 'Show All' buttons. Below the table, it says 'Total Entries: 0' and 'No data to display'.

Figure 5-56 MLD Snooping Filter Settings

In the section of the settings on **MLD Snooping Band Limitation**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use. This is available only if you select the Port option as the following action.
Number of Limitations	Enter the number of limitations. Use the number of limitations to configure the rate of MLD control packets, which can be processed by the Switch on a specific interface. The range is from 1 to 1,000 (packets/per second). If you choose No Limitation , the limitation is removed (or deleted).

Click **Apply** to reflect the change.

In the section of the settings on **MLD Snooping Limitation**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Number of Limitations	Enter the number of limitations. Use this parameter to limit the number of MLD cash entries, which can be created. The range is from 1 to 2,048.
Exceed Action	Choose an exceed action. Use this parameter to specify the operation to process the group, which is newly recognized when exceeding the limitation. The options available are as follows. <ul style="list-style-type: none"> • Default - The default action is executed. • Drop - A new group is dropped. • Replace - A new group is replaced to the oldest group.
Except ACL Name	Enter the name of the standard IP access-list. The group (*,G) or channel (S,G), which are allowed based on the access list, are excluded from the limitation. To authorize a channel (S,G), specify "S" in the field of source-address of the access-list entry and "G" in the destination- address field. To authorize a group (*,G), specify "any" in the source-address field of the access-list entry and "G" in the destination-address field. The number of characters for the name can be up to 32. Alternatively, click Please Select to search and choose the existing access list, which is configured on the switch (to be used for this configuration).
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete entries based on the information specified.

In the section of **Access Group Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Action	Click Add to add a new entry based on the information entered. Click Delete to delete an entry based on the information entered.

Parameter	Overview
ACL Name	Enter the name of the standard IP access-list. Use this parameter to allow users to participate in the group (*, G). To authorize a group (*,G), specify "any" in the source-address field of the access-list entry and "G" in the destination-address field. The number of characters for the name can be up to 32. Or, click Please Click to retrieve the existing access list, which is configured by a switch for using this configuration, and then choose the list.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Apply** to reflect the change.

In the section of a table of **MLD Snooping Filter**, you can configure the following parameter.

Parameter	Overview
From Port/ To Port	Choose the port you use.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

Click **Show Detail** to display details on the entry.

If two or more pages exist, enter the page numbers. Click **Go** to move to a specific page.

Click **Show Detail** to display the following window.

VID	Access Group	Port: G1/0/1	Groups/Channel Limit
Not Configured	Not Configured	Not Configured	Not Configured

Figure 5-57 MLD Snooping Filter Settings (Show Detail.)

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Back** to return to the previous window.

5.7.2.4 MLD Snooping Multicast Router Information

Use the following window to implement the settings on an MLD Snooping Multicast router and display its settings.

Choose **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Multicast Router Information** to display the following window.

Figure 5-58 MLD Snooping Multicast Router Information

In the section of the port settings on **MLD Snooping Multicast Router**, you can configure the following parameters.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
Configuration	Choose a port configuration. The options available are as follows. <ul style="list-style-type: none"> • Port - Ports configured are connected to a Multicast corresponding router. • Forbidden Port - Ports, which are configured, are not connected to a Multicast corresponding router.
From Port/ To Port	Choose the port you use.

Click **Apply** to add new entries based on the information specified.

Click **Delete** to delete entries based on the information specified.

In the section of a port table for **MLD Snooping Multicast Router**, you can configure the following parameter.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

5.7.2.5 MLD Snooping Statistics Settings

Use the following window to display and clear the MLD Snooping statistics.

Choose **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings** to display the following window.

Figure 5-59 MLD Snooping Statistics Settings

In the section of **MLD Snooping Statistics Settings**, you can configure the following parameters.

Parameter	Overview
Statistics	Choose an interface. The options available are All , VLAN and Port .
VID	Enter the VLAN ID you use. The range is from 1 to 4,094. This option is available when choosing VLAN from the Statistics drop-down list.
From Port/ To Port	Choose the port you use. This option is available when you choose Port from the Statistics drop-down list.

Click **Clear** to clear the statistics information based on the condition specified.

In the section of **MLD Snooping Statistics Table**, you can configure the following parameters.

Parameter	Overview
Search Type	Choose an interface type. The options available are VLAN and Port .
VID	Enter the VLAN ID you use. The range is from 1 to 4,094. This option is available when you choose VLAN from the Search Type drop-down list.
From Port/ To Port	Choose the port you use. This option is available when you choose Port from the Search Type drop-down list.

Click **Find** to search and display the entries in a table based on the search condition specified.

Click **See All** to search and display all the entries available.

5.7.3 Multicast Filtering Mode

Use the following window to implement the settings on the Multicast filtering mode and display its settings.

Choose **L2 Features > L2 Multicast Control > Multicast Filtering Mode** to display the following window.

Figure 5-60 Multicast Filtering Mode

In the section of the **Multicast Filtering Mode**, you can configure the following parameters.

Parameter	Overview
VID List	Enter the VLAN ID you use. You can enter its consecutive VLAN IDs by delimiting with a comma, or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.
Multicast Filtering Mode	Choose the Multicast filtering mode. The options available are as follows. <ul style="list-style-type: none"> • Forward Unregistered - Registered Multicast packets are forwarded based on a forwarding table, and then all unregistered Multicast packets are flooded based on a VLAN domain. • Forward All - All Multicast packets are flooded based on a VLAN domain. • Filter Unregistered - Registered packets are forwarded based on a forwarding table, and then all unregistered Multicast packets are filtered.

Click **Apply** to add new entries based on the information specified.

5.8 LLDP (Link Layer Discovery Protocol)

5.8.1 LLDP Global Settings

Use the following window to implement the global LLDP settings and display its settings.

Choose **L2 Features > LLDP > LLDP Global Settings** to display the following window.

LLDP Global Settings

LLDP State: ☒ Enabled ☐ Disabled

LLDP Forward State: ☒ Enabled ☐ Disabled

LLDP Trap State: ☒ Enabled ☐ Disabled

LLDP-MED Trap State: ☒ Enabled ☐ Disabled

LLDP-MED Configuration

Fast Start Repeat Count (1-10): times ☐ Default

LLDP Configurations

Message TX Interval (5-32768): sec ☐ Default

Message TX Hold Multiplier (2-10): sec ☐ Default

Retx Delay (1-10): sec ☐ Default

TX Delay (1-6182): sec ☐ Default

LLDP System Information

Chassis ID Subtype: MAC Address

Chassis ID: MAC Address

System Name:

System Description:

System Capabilities Supported:

System Capabilities Enabled:

LLDP-MED System Information

Device Class:

Hardware Revision:

Firmware Revision:

Software Revision:

Serial Number:

Manufacturer Name:

Model Name:

Asset ID:

PoE Device Type:

PoE PoE Power Source:

Figure 5-61 LLDP Global Settings

In the section of **LLDP Global Settings**, you can configure the following parameters.

Parameter	Overview
LLDP State	This parameter enables or disables an LLDP function.
LLDP Forward State	This parameter enables or disables the LLDP forward state. If you disable the LLDP State and enable the LLDP Forward State , the LLDP Data Unit (LLDPDU) Packets, which have been received, are transferred.
LLDP Trap State	This parameter enables or disables the LLDP trap state.
LLDP-MED Trap State	This parameter enables or disables the trap state of LLDP Media Endpoint Discovery (LLDP-MED).

Click **Apply** to reflect the change.

In the section of **LLDP-MED Configuration**, you can configure the following parameter.

Parameter	Overview
Number of Transmissions for Fast Start	Enter the value, which is equal to the number of transmissions regarding the LLDP-MED fast start. The range is from 1 to 10. When you choose Default , use the default value.

Click **Apply** to reflect the change.

In the section of **LLDP Configuration**, you can configure the following parameters.

Parameter	Overview
Transmission Interval for Messages	Enter the transmission-interval for consecutive LLDP advertisements on each physical interface. The range is from 5 to 32,768 (seconds). When you choose Default , use (or apply) the default value.
Message TX Hold Multiplier	Enter the multiplier of the LLDPDU transmission-interval to use for calculating the value of Time-To-Live (TTL) of LLDPDU. The range is from 2 to 10. When you choose Default , use the default value.
Reinit Delay	Enter the lag time (or retarded time) regarding the LLDP initialization of an interface. The range is from 1 to 10 (seconds). When you choose Default , use the default value.
TX Delay	Enter the lag time for the transmission of consecutive LLDPDUs on an interface. The range of valid (or enabled) values is from 1 to 8,192 (seconds). The value above must not exceed one-fourth of the value of the transmission-interval timer. When you choose Default , use the default value.

Click **Apply** to reflect the change.

5.8.2 LLDP Port Settings

Use the following window to implement the settings on an LLDP port and display its settings.

Choose **L2 Features > LLDP > LLDP Port Settings** to display the following window.

Port	Notification	Subtype	Admin State	IPv4/IPv6 Address
F11/0/1	Disabled	Local	TX and RX	
F11/0/2	Disabled	Local	TX and RX	
F11/0/3	Disabled	Local	TX and RX	
F11/0/4	Disabled	Local	TX and RX	
Te11/0/5	Disabled	Local	TX and RX	
Te11/0/6	Disabled	Local	TX and RX	

Figure 5-62 LLDP Port Settings

In the section of **LLDP Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Notification	This enables or disables a notification function.
Sub-type	Choose the sub-type of LLDP TLV (Type-Length-Value). The options available are MAC Address and Local .
Management State	<p>Choose the local LLDP agent to allow you to transmit and receive LLDP frames on the port. The options available are as follows.</p> <ul style="list-style-type: none"> TX - The local LLDP agent can transmit LLDP frames, only. RX - The local LLDP agent can receive LLDP frames, only. TX and RX - The local LLDP agent can transmit and receive LLDP frames. Disabled - The local LLDP agent cannot transmit or receive LLDP frames. <p>The default option is set to TX and RX.</p>
IP Sub-type	Choose the information type for the IP address to transmit. The options available are Default , IPv4 and IPv6 .
Action	Choose the action you perform. The options available are Delete and Add .
Address	Enter an IP address to be transmitted.

Click **Apply** to reflect the change.

5.8.3 LLDP Management Address List

Use the following window to display the LLDP management address list and its information.

Choose **L2 Features > LLDP > LLDP Management Address List** to display the following window.

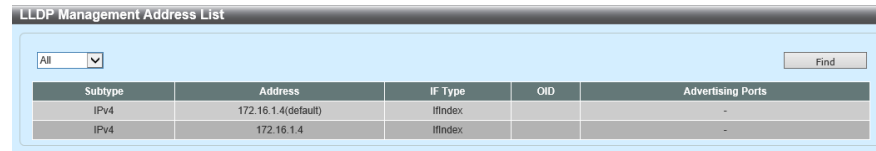


Figure 5-63 LLDP Management Address List

You can configure the following parameter.

Parameter	Overview
Sub-type	<p>Enter a sub type. The options available are All, IPv4 and IPv6.</p> <ul style="list-style-type: none">• After you choose IPv4, enter it in the entry field where an IPv4 address is displayed.• After you choose IPv6, enter it in the entry field where an IPv6 address is displayed.

Click **Find** to search and display the entries in a table based on the search condition specified.

5.8.4 LLDP Basic TLVs Settings

Use the following window to implement the basic settings on LLDP TLV and display its settings.

Choose **L2 Features > LLDP > LLDP Basic TLVs Settings** to display the following window.

Port	Port Description	System Name	System Description	System Capabilities
F1/0/1	Disabled	Disabled	Disabled	Disabled
F1/0/2	Disabled	Disabled	Disabled	Disabled
F1/0/3	Disabled	Disabled	Disabled	Disabled
F1/0/4	Disabled	Disabled	Disabled	Disabled
Te1/0/5	Disabled	Disabled	Disabled	Disabled
Te1/0/6	Disabled	Disabled	Disabled	Disabled

Figure 5-64 LLDP Basic TLVs Settings

In the section of the **LLDP Basic TLVs Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Description of Ports	This parameter enables or disables the transmission of port description TLV.
System Name	This parameter enables or disables the transmission of system name TLV.
Description of Systems	This parameter enables or disables the transmission of system description TLV.
System Capability	This parameter enables or disables the transmission of system capability TLV.

Click **Apply** to reflect the change.

5.8.5 LLDP Dot1 TLV Settings

Use the following window to implement the settings on IEEE 802.1 LLDP TLV and display its settings.

Choose **L2 Features > LLDP > LLDP Dot1 TLV Settings** to display the following window.

Port	Port VLAN ID	Enabled Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity
Fi1/0/1	Disabled			
Fi1/0/2	Disabled			
Fi1/0/3	Disabled			
Fi1/0/4	Disabled			
Te1/0/5	Disabled			
Te1/0/6	Disabled			

Figure 5-65 LLDP Dot1 TLV Settings

In the section of **LLDP Dot1 TLV Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Port VLAN	This parameter enables or disables to transmit Port VLAN ID TLV.
Protocol VLAN	This parameter enables or disables to transmit the port and protocol VLAN ID (PPVID) TLV. Enter the ID in the entry field provided.
VLAN Name	This parameter enables or disables to transmit the TLV of a VLAN name. Enter a VLAN ID in the entry field provided.
Protocol Identity	This parameter enables or disables to transmit the protocol identity TLV. The options available are None , EAPOL , LACP , GVRP , STP and All , as a protocol name

Click **Apply** to reflect the change.

5.8.6 LLDP Dot3 TLV Settings

Use the following window to implement the settings on IEEE 802.3 LLDP TLV and display its settings.

Choose **L2 Features > LLDP > LLDP Dot3 TLV Settings** to display the following window.

Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size	Power Via MDI	Power Via MDI Measurements
Fi1/0/1	Disabled	Disabled	Disabled	Enabled	Enabled
Fi1/0/2	Disabled	Disabled	Disabled	Enabled	Enabled
Fi1/0/3	Disabled	Disabled	Disabled	Enabled	Enabled
Fi1/0/4	Disabled	Disabled	Disabled	Enabled	Enabled
Te1/0/5	Disabled	Disabled	Disabled		
Te1/0/6	Disabled	Disabled	Disabled		

Figure 5-66 LLDP Dot3 TLV Settings

In the section of **LLDP Dot3 TLV Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
MAC/PHY Config./ State	This parameter enables or disables to transmit the MAC/PHY config./state TLV.
Link Aggregation	This parameter enables or disables to transmit the link aggregation TLV.
Maximum Frame Size	This parameter enables or disables to transmit the maximum frame-size TLV.

Click **Apply** to reflect the change.

5.8.7 LLDP-MED Port Settings

Use the following window to implement the settings on an LLDP-MED port and display its settings.

Choose **L2 Features > LLDP > LLDP-MED Port Settings** to display the following window.

Port	Notification	Capabilities	Inventory	Network Policy	PSE
Fi1/0/1	Disabled	Disabled	Disabled	Disabled	Disabled
Fi1/0/2	Disabled	Disabled	Disabled	Disabled	Disabled
Fi1/0/3	Disabled	Disabled	Disabled	Disabled	Disabled
Fi1/0/4	Disabled	Disabled	Disabled	Disabled	Disabled
Te1/0/5	Disabled	Disabled	Disabled	Disabled	Disabled
Te1/0/6	Disabled	Disabled	Disabled	Disabled	Disabled

Figure 5-67 LLDP-MED Port Settings

In the section of the **LLDP-MED Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Notification	This parameter enables or disables the transmission of LLDP-MED notification TLV.
Capability	This parameter enables or disables the transmission of LLDP-MED capability TLV.
Assets	This parameter enables or disables the transmission of LLDP-MED asset management TLV.
Network Policy	This parameter enables or disables the transmission of LLDP-MED network policy TLV.

Click **Apply** to reflect the change.

5.8.8 LLDP Statistics Information

Use the following window to display and clear the LLDP statistics.

Choose **L2 Features > LLDP > LLDP Statistics Information** to display the following window.

LLDP Statistics Information							
LLDP Statistics Information							
Last Change Time	00:00:00:00:00:00						Clear Counter
Total Inserts	0						
Total Deletes	0						
Total Drops	0						
Total Ageouts	0						
LLDP Statistics Ports							
Port	Fi1/0/1						Clear Counter Clear All
Port	Total Transmits	Total Discards	Total Errors	Total Receives	Total TLV Discards	Total TLV Unknowns	Total Ageouts
Fi1/0/1	0	0	0	0	0	0	0
Fi1/0/2	0	0	0	0	0	0	0
Fi1/0/3	0	0	0	0	0	0	0
Fi1/0/4	0	0	0	0	0	0	0
Te1/0/5	0	0	0	0	0	0	0
Te1/0/6	0	0	0	0	0	0	0

Figure 5-68 LLDP Statistics Information

In the section of **LLDP Port Statistics Port Statistics**, you can configure the following parameter.

Parameter	Overview
Port	Choose the port you use.

Click **Clear** to clear the counter information.

Click **Clear All** to clear the counter information on all the ports.

5.8.9 LLDP Local Port Information

Use the following window to display local LLDP port information and its information.

Choose **L2 Features > LLDP > LLDP Local Port Information** to display the following window.

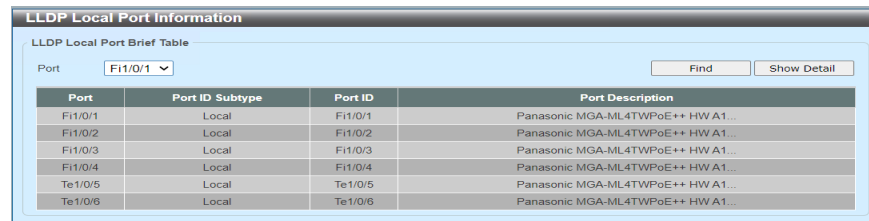


Figure 5-69 LLDP Local Port Information

In the section of the **LLDP Local Port Summary Table**, you can configure the following parameter.

Parameter	Overview
Port	Choose the port you use.

Click **Find** to search the LLDP local port information, which is associated with the port specified.

Click **Show Detail** to display details on the LLDP local port, which is associated with the port specified.

Click **Show Detail** to display the following window.



LLDP Local Information Table	
Port	F1/0/1
Port ID Subtype	Local
Port ID	F1/0/1
Port Description	Panasonic MGA-ML4TWPoE++ HW A1 firmware V1.0.0.01 Port 1 on Unit 1
Port PVID	1
Management Address Count	2
PPVID Entries	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1518
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended power via MDI	Show Detail

Back

Figure 5-70 LLDP Local Port Information (Show Detail.)

Click **Individual Link** to display the details, which are associated with the function specified, on the related table above.

Click **Back** to return to the previous window.

5.8.10 LLDP Neighbor Port Information

Use the following window to display the LLDP port information on neighbor.

Choose **L2 Features > LLDP > LLDP Neighbor Port Information** to display the following window.

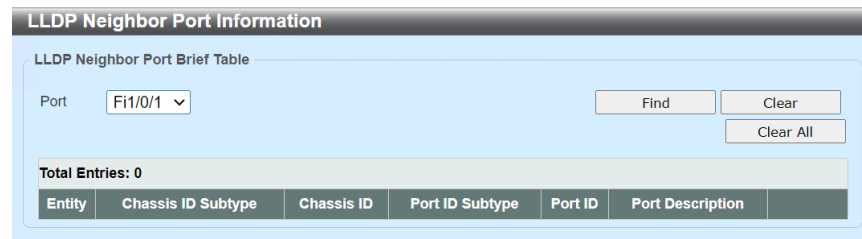


Figure 5-71 LLDP Neighbor Port Information

In the section of a **LLDP Neighbor Port Summary Table**, you can configure the following parameter.

Parameter	Overview
Port	Choose the port you use.

Click **Find** to search the information on the LLDP Neighbor Port, which is associated with the port specified.

Click **Clear** to clear the information on the LLDP Neighbor Port, which is associated with the port specified.

Click **Clear All** to clear information on all the LLDP Neighbor Port.

5.9 UDLD (Unidirectional Link Detection)

Use the following window to implement the UDLD settings and display its settings and state.

Choose **L2 Features > UDLD** to display the following window.

The screenshot shows the 'UDLD' configuration window. At the top, it says 'UDLD Global Settings'. Below this, there is a 'UDLD Detection Time (5-65535)' field set to '5' seconds, with a 'Default' checkbox checked and an 'Apply' button. Below that, there are four dropdown menus: 'From Port' (F11/0/1), 'To Port' (F11/0/1), 'Admin State' (Disabled), and 'Mode' (Normal), each with an 'Apply' button. At the bottom, there is a table with 7 columns: Port, Admin State, Mode, Link State, Neighbor MAC, Neighbor Port, and Neighbor State. The table contains 6 rows of data for ports F11/0/1 through Te1/0/6.

Port	Admin State	Mode	Link State	Neighbor MAC	Neighbor Port	Neighbor State
F11/0/1	Disabled	Normal	Unknown	-	-	-
F11/0/2	Disabled	Normal	Unknown	-	-	-
F11/0/3	Disabled	Normal	Unknown	-	-	-
F11/0/4	Disabled	Normal	Unknown	-	-	-
Te1/0/5	Disabled	Normal	Unknown	-	-	-
Te1/0/6	Disabled	Normal	Unknown	-	-	-

Figure 5-72 UDLD

In the section of **UDLD Global Settings**, you can configure the following parameters.

Parameter	Overview
UDLD Detection Time	This parameter configure the time (in seconds) needed for detecting the unidirectional network (or connection). The configuration range is from 5 to 65,535 (seconds). The factory default settings is 5 (seconds).
From Port/ To Port	Choose the port you use.
Admin State	This parameter enables or disables the UDLD function of the port specified. The factory default settings is Enabled .
Mode	Choose the UDLD mode to be used for the port specified. The factory default settings is Normal . The options available are as follows. <ul style="list-style-type: none"> • Normal - If the unidirectional network is detected, the link of the corresponding port continues to record (or log) an event on a system log. • Shutdown - If the unidirectional network is detected, the corresponding port becomes shut-down to record an event on the system log.

Click **Apply** to reflect the change.

This function can be used between our products, only.

5.10 RRP (Ring Redundant Protocol)

Use the following window to implement the RRP settings and display its settings.

Choose **L2 Features > RRP** to display the following window.

Domain Name	Control VLAN	Data VLAN(s)	Ring Status
rrp			IDLE

Figure 5-73 RRP

In the section of **RRP Global State**, you can configure the following parameter.

Parameter	Overview
RRP State	This parameter enables or disables an RRP function.

Click **Apply** to reflect the change.

In the section of the **RRP Domain State**, you can configure the following parameter.

Parameter	Overview
Domain Name	Enter the name of an RRP domain. The number of the character strings you specify can be up to 25. This domain indicates a physical ring.

Click **Create** to create a new RRP domain.

Click **Show Detail** to display details on the entry.

Click **Delete** to delete the entry.

Click **Show Detail** to display the following window.

The RRP Domain Status window displays the following information:

RRP Domain Status	
RRP Domain Name	RRP1
RRP Domain Status	Disabled
RRP Node Type	
RRP Ring Status	IDLE
Primary Port	-
Primary Port Status	Unknown
Primary Port Role	None
Secondary Port	-
Secondary Port Status	Unknown
Secondary Port Role	None
Polling Interval (1-2)	1
Fail Period (2-5)	2
Ring Guard Port	Disable
Control VLAN (2-4094)	
Data VLAN(s)	

Buttons: Edit, Back

Figure 5-74 RRP (Show Detail.)

Click **Edit** to edit the settings.

Click **Back** to return to the previous window.

Click **Edit** to display the following window.

The RRP Domain Settings window displays the following configuration options:

RRP Domain Settings	
RRP Domain Name	5
RRP Domain Status	Disabled
RRP Node Type	Master
Primary Port	Fi1/0/1 <input checked="" type="checkbox"/> Default
Secondary Port	Fi1/0/1 <input checked="" type="checkbox"/> Default
Polling Interval (1-2)	1
Fail Period (2-5)	2
Ring Guard Port	Disable
Control VLAN (2-4094)	
Data VLAN(s)	3 or 1-5

Buttons: Apply, Cancel, Back

Figure 5-75 RRP (Edition)

In the section of **RRP Domain Settings**, you can configure the following parameters.

Parameter	Overview
RRP Domain State	Choose to enable or disable an RRP domain.

Parameter	Overview
RRP Node Type	Choose the type for RRP-node. The options available are as follows. <ul style="list-style-type: none"> • Master - Specifies the node as the master node in the domain. Only one master-node can be specified in one RRP domain. Roles of the master-node include ring-polling and ring-restoration. • Transit - Specifies the node as a transit node in the domain. Many transit-nodes can be specified in one RRP domain. Responsibilities of a transit-node include link-down alerts.
Primary Port	Choose a primary port. This port will be the first port in the RRP domain. If you choose the Default option, the current settings are cleared.
Secondary Port	Choose a secondary port. This port becomes the second port in the RRP domain. If you choose the default option, the current settings are cleared. If you choose the Default option, the current settings are cleared.
Polling Interval	Enter the polling interval of hello-packets. The range is from 1 to 2 (seconds). The polling interval should be shorter than the failure period.
Failure Period	Enter the disorder period. The range is from 2 to 5 (seconds). The failure period should be longer than the polling interval.
Ring-Guard Port	Choose the port state of RRP ring-guard. The options available are as follows. <ul style="list-style-type: none"> • Primary - This specifies a primary port as the port corresponding with a ring guard. • Secondary - This specifies a secondary port as the port corresponding with a ring-guard. • Both - This specifies for both primary and secondary ports as the port, which corresponds with the ring-guard. • Disabled - Disables this function.
Control VLAN	Enter an ID of the control VLAN. The range is from 2 to 4,094.
Data VLAN	Enter an ID of the data VLAN. The range is from 1 to 4,094.

Click **Apply** to reflect the change.

Click **Cancel** to delete the change.

Click **Back** to return to the previous window.

6 L3 Features

6.1 ARP (Address Resolution Protocol)

6.1.1 ARP Aging Time

Use the following window to implement the settings on ARP aging time and display its settings.

Choose **L3 Features > ARP > ARP Aging Time** to display the following window.

Figure 6-1 ARP Aging Time

In the section of **Searching for ARP Aging Time**, you can configure the following parameters.

Parameter	Overview
Interface VLAN	Enter a VLAN ID. The range is from 1 to 4,094.
Time-out	After you click Edit , enter the time-out value. The range is from 0 to 65,535 (minutes).

Click **Find** to search and display the entries based on the search condition specified.

Click **See All** to search and display all the entries available.

Click **Edit** to edit the entry-settings.

If two or more pages exist, enter the page-numbers. Then click **Go** to move to a specific page.

6.1.2 Static ARP

Use the following window to implement the settings on the static ARP and display its settings.

Choose **L3 Features > ARP > Static ARP** to display the following window.

Figure 6-2 Static ARP

In the section of the **Static ARP Settings**, you can configure the following parameters.

Parameter	Overview
IP Address	Enter an IP address to associate with a MAC address.
Hardware Address	Enter a MAC address to associate with an IP Address.

Click **Apply** to add a new Static ARP entry.

In the section of **Searching for Static ARP**, you can configure the following parameters.

Parameter	Overview
IP Address	Choose and enter an IP address of an entry.
IP Network Mask	Choose and enter a subnet mask of an IP address.
Hardware Address	Choose and enter a MAC address of an entry.
Interface VLAN	Choose and enter a VLAN ID. The range is from 1 to 4,094.

Click **Find** to search and display the entries based on the search condition specified.

Click **See All** to search and display all the entries available.

Click **Edit** to edit the entry-settings.

Click **Delete** to delete the entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

6.1.3 ARP Table

Use the following window to display and clear the ARP entries in a table

Choose **L3 Features > ARP > ARP Table** to display the following window.

ARP Table

ARP Search

☒ Interface VLAN (1-4094) ☐ IP Address Mask ☐ Hardware Address ☐ Type

Total Entries: 2

Interface Name	IP Address	Hardware Address	Aging Time (min)	Type	Clear
vlan1	172.16.1.4	00-50-40-5C-2B-AC	Forever		<input type="button" value="Clear"/>
vlan1	172.16.230.101	34-95-DB-2E-3E-8B	240		<input type="button" value="Clear"/>

1/1

Figure 6-3 ARP Table

In the section of **Searching for ARP**, you can configure the following parameters.

Parameter	Overview
Interface VLAN	Choose and enter a VLAN ID of an interface. The range is from 1 to 4,094.
IP Address	Choose and enter an IP address to be displayed.
Mask	Choose and enter a subnet-mask of an IP address.
Hardware Address	Choose and enter a MAC address to be displayed.
Type	Choose the Type option. The options available are All and Dynamic .

Click **Find** to search and display the entries based on the search condition specified.

Click **Clear All** to clear all the entries from a table.

Click **Clear** to delete entries specified.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

6.2 Gratuitous ARP

Use the following window to implement the settings on gratuitous ARP and display its settings. Gratuitous ARP request packets are the ARP request packets whose destination MAC address is a broadcast address; an IP address of the source and destination for gratuitous ARP packets is configured on an IP address of a transmission device. The device uses ARP request packets to accurately check if the IP address has duplications with other hosts. Alternatively, the device reconfigures or loads the ARP cache entries of the host connected to an interface, in advance.

Choose **L3 Features > Gratuitous ARP** to display the following window.

Figure 6-4 Gratuitous ARP

In the section of **Gratuitous ARP Global Settings**, you can configure the following parameters.

Parameter	Overview
IP Gratuitous ARP State	This parameter enables or disables to transmit gratuitous ARP request packets.
Gratuitous ARP Trap State	This parameter enables or disables the trap state of a gratuitous ARP function.
IP Gratuitous ARP Dad-Reply State	This parameter enables or disables the IP gratuitous ARP Dad-Reply state.
Gratuitous ARP Learning State	This parameter enables or disables the gratuitous ARP learning state. Normally, this system learns the ARP entries, only, from the normal ARP-request packets, which require a MAC address and an IP address of the ARP entry from ARP request packets or a switch. Use this option to enable or disable to learn the ARP entries based on the gratuitous ARP packets received. A source IP address transmits gratuitous ARP packets to become the same with the IP address where packets are (on) the queried state.

Click **Apply** to reflect the change.

In the section of **Gratuitous ARP Transmission Interval**, you can configure the following parameter.

Parameter	Overview
Interval Time	After you click Edit , enter the time for gratuitous ARP transmission-interval (seconds).

Click **Edit** to edit the entry-settings.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

6.3 IPv6 Neighbor

Use the following window to implement the settings on IPv6 neighbor and display its settings.

Choose **L3 Features > IPv6 Neighbor** to display the following window.

IPv6 Address	Link-Layer Address	Interface	Type	State	
--------------	--------------------	-----------	------	-------	--

Figure 6-5 IPv6 Neighbor

In the section of **IPv6 Neighbor Settings**, you can configure the following parameters.

Parameter	Overview
Interface VLAN	Enter a VLAN interface ID.
IPv6 Address	Enter an IPv6 address.
MAC Address	Enter a MAC address.

Click **Apply** to add a new entry.

Click **Find** to search and display the entries based on the search condition specified.

Click **Clear** to clear the information based on the condition specified.

Click **Clear All** to clear all the dynamic entries.

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

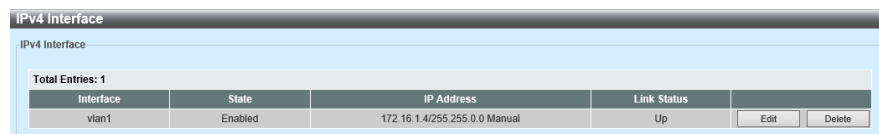
If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

6.4 Interface

6.4.1 IPv4 Interface

Use the following window to implement the settings on IPv4 interface and display its settings.

Choose **L3 Features > Interface > IPv4 Interface** to display the following window.



The screenshot shows a window titled 'IPv4 Interface'. Inside, there's a sub-header 'IPv4 Interface' and a table with the following data:

Interface	State	IP Address	Link Status	
vlan1	Enabled	172.16.1.4/255.255.0.0 Manual	Up	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Figure 6-6 IPv4 Interface

In the section of **IPv4 Interface**, you can configure the following parameter.

Parameter	Overview
Interface VLAN	Enter an Interface VLAN ID. The range is from 1 to 4,094.

Click **Apply** to add the new entry.

Click **Find** to search and display the entries based on the search condition specified.

Click **Edit** to edit the configuration of the entry specified.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Edit** to display the following window.

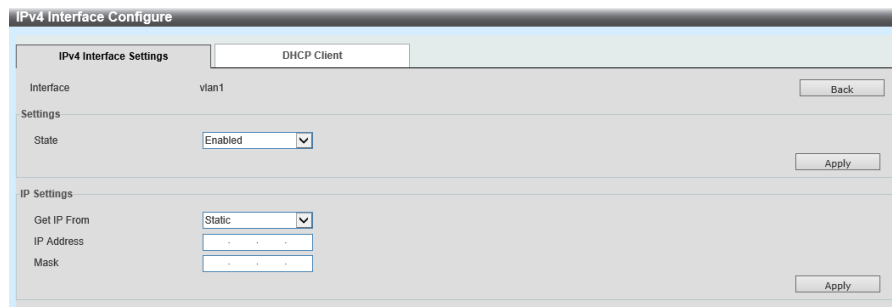


Figure 6-7 IPv4 Interface (Edit and IPv4 Interface Settings)

In the section of **Settings**, you can configure the following parameters.

Parameter	Overview
State	This parameter enables or disables the global state of an IPv4 interface.
IP MTU	Enter the value of Maximum Transmission Unit (MTU). The range is from 512 to 16,383 (bytes). By default, the value is set to 1,500 (bytes).
IP Directed Broadcast	This parameter enables or disables the function of an IP directed broadcast. Use this parameter to enable or disable the conversion to a physical broadcast of the IP directed broadcast, which is received on an interface when the destination network is directly connected to a switch.

Click **Back** to return to the previous window.

Click **Apply** to reflect the change.

In the section of **IP Settings**, you can configure the following parameters.

Parameter	Overview
Method of Obtaining IP	Choose a method of obtaining an IP address. The options available are as follows. <ul style="list-style-type: none"> • Static - Enter an IPv4 address configuration of this interface in the entry field provided, manually. • DHCP - This interface automatically obtains the IPv4 settings from DHCP servers existing in a local network.
IP Address	Enter an IPv4 address of this interface.
Mask	Enter an IPv4 subnet mask of this interface.
Secondary	If you set this option to on, use an IPv4 address and mask secondary as the interface settings.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click the **DHCP Client** tab to display the following window.

The screenshot shows the 'IPv4 Interface Configure' window. The 'DHCP Client' tab is selected. It contains the following fields and controls:

- Class ID String**: A text input field with a placeholder '32 chars'.
- Host Name**: A text input field with a placeholder '64 chars'.
- Lease**: A section with a text input field, a dropdown menu for 'Days (0-10000)' set to '00', and dropdown menus for 'Hours' and 'Minutes' both set to '00'.
- Hex**: A checkbox.
- Apply**: A button in the bottom right corner.

Figure 6-8 IPv4 Interface (Edit and DHCP Clients)

In the section of **DHCP Client**, you can configure the following parameters.

Parameter	Overview
DHCP Client Client ID	Enter an ID of a DHCP client. The range is from 1 to 4,094. Use this parameter to specify the VLAN interface, which uses the hex notation of the MAC address as a client ID for sending discover messages.

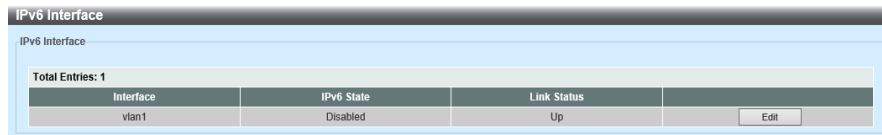
Parameter	Overview
Class ID Character Strings	Enter the character strings of a class ID. The number of character strings can be up to 32. If you choose the hex notation, enter the character strings of the class ID as the hex notation. The number of character strings can be up to 64. Use this parameter to specify the vendor class ID to use as the value of Option 60 of DHCP discovery messages.
Host Name	Enter a host-name. The number of character strings can be up to 64. Use this parameter to specify the value of the host-name option, which transmits with DHCP discovery messages.
Lease	Enter the lease period for a DHCP client. You can choose that, if necessary. Enter the number of days for the lease period in a text-box. The range is from 0 to 10,000 (days). If necessary, you can choose Time and Minute .

Click **Apply** to reflect the change.

6.4.2 IPv6 Interface

Use the following window to implement the settings on IPv6 interface and display its settings.

Choose **L3 Features > Interface > IPv6 Interface** to display the following window.



IPv6 Interface			
IPv6 Interface			
Total Entries: 1			
Interface	IPv6 State	Link Status	
vlan1	Disabled	Up	Edit

Figure 6-9 IPv6 Interface

In the section of **IPv6 Interface**, you can configure the following parameter.

Parameter	Overview
Interface VLAN	Enter an VLAN interface ID to be associated with the IPv6 entry.

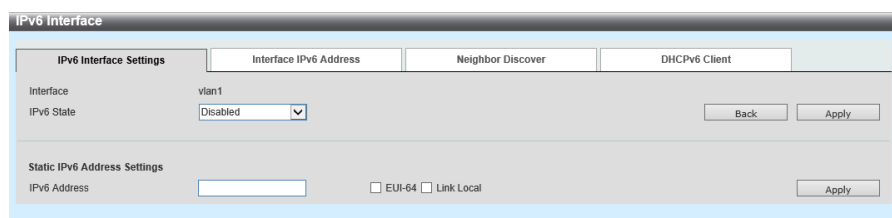
Click **Apply** to add a new entry.

Click **Find** to search and display the entries based on the search condition specified.

Click **Show Detail** to display details on the entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Show Detail** to display the following window.



IPv6 Interface	
<div> <div>IPv6 Interface Settings</div> <div>Interface IPv6 Address</div> <div>Neighbor Discover</div> <div>DHICPv6 Client</div> </div>	
Interface	vlan1
IPv6 State	Disabled <input type="button" value="Back"/> <input type="button" value="Apply"/>
Static IPv6 Address Settings	
IPv6 Address	<input type="text"/> <input type="checkbox"/> EUI-64 <input type="checkbox"/> Link Local <input type="button" value="Apply"/>

Figure 6-10 IPv6 Interface (Show Detail and IPv6 Interface Settings)

In the section of **IPv6 Interface Settings**, you can configure the following parameters.

Parameter	Overview
IPv6 MTU	Enter the value of IPv6 MTU. The range is from 1,280 to 65,534 (bytes). By default, the value is set to 1,500 (bytes). Use this parameter to configure MTU, which can be advertised by a router advertise (RA) message.
IPv6 State	This parameter enables or disables the global state for IPv6 Interface.

Click **Back** to return to the previous window.

Click **Apply** to reflect the change.

In the section of the **Static IPv6 Address Settings**, you can configure the following parameter.

Parameter	Overview
IPv6 Address	Enter an IPv6 address of this IPv6 Interface. <ul style="list-style-type: none"> If you choose Extended Unique Identifier 64-bit (EUI-64), you can configure the IPv6 address on an interface that uses EUI-64 Interface ID. If you choose Link Local, you can configure its link local address of the IPv6 interface.

Click **Apply** to reflect the change.

Click the **Interface IPv6 Address** tab to display the following window.



Figure 6-11 IPv6 Interface (Show Detail and Interface IPv6 Address)

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Choose the **Neighbor Discover** tab to display the following window.



Figure 6-12 IPv6 Interface (Show Detail and Neighbor Discover)

In the section of **ND Settings**, you can configure the following parameters.

Parameter	Overview
Management Configuration Flag	Set the management configuration flag option to ON or OFF . If a neighbor host receives RA with the flag, which is set to on, the host needs to obtain an IPv6 address with the stateful configuration protocol.
Other Config Flag	Set Other Config flag-option to ON or OFF . If you set other configuration flags to on, use the stateful configuration protocol to command the host connected to obtain the auto-configuration information except an IPv6 address.
RA Minimum-Interval	Enter the minimum value of the RA interval-time. The range is from 3 to 1,350 (seconds). The value must be smaller than the value, equivalent to 75% of the maximum value.
RA Maximum-Interval	Enter the maximum value of the RA interval-time whose range is from 4 to 1,800 (seconds).
RA Lifetime	Enter the value of an RA lifetime. The range is from 0 to 9,000 (seconds). The lifetime value of RA conveys the value, which regards a router as a default router on the host where RA is received.
RA Control	This parameter enables or disables the function of the RA control.
Reachable Time	Enter the reachable time. The range is from 0 to 3,600,000 (milli-seconds). If the time specified is 0, a router spends 1,200 (seconds) on an interface to advertise 1,200 (unspecified) for RA messages. The reachable time is used to determine the possibility of reaching a neighbor node due to an IPv6 node.
NS Interval	Enter the value of the Neighbor Solicitation (NS) interval. The range is from 0 to 3,600,000 milli-seconds (the factor of 1,000). If the time specified is 0, a router spends for one second.
Hop Limit	Enter the value of the hop limit. The range is from 0 to 255. IPv6 packets created by a system uses the value as the initial hop limit.

Click **Apply** to add a new entry.

Click **Edit** to edit the configuration of the entry specified.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Choose the **DHCPv6 Client** tab to display the following window.

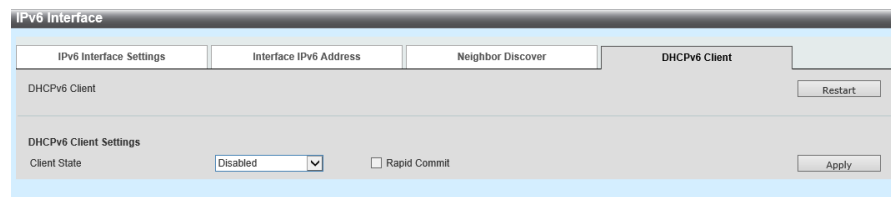


Figure 6-13 IPv6 Interface (Show Detail, DHCPv6 Client)

Click **Restart** to restart the function of DHCPv6 Client.

In the section of **DHCPv6 Client Settings**, you can configure the following parameter.

Parameter	Overview
Client State	This parameter enables or disables DHCPv6 client services. If you choose Rapid Commit , exchanging two messages for address delegation continues. The high-speed commit option is included in solicit messages, and two-message handshake is required.

In the section of **DHCPv6 Client PD Settings**, you can configure the following parameters.

Parameter	Overview
Client PD State	This parameter enables or disables the DHCPv6 client process that requires PD (Prefix Delegation) through the interface specified. If you choose the Rapid Commit option, exchanging two messages for the prefix delegation continues. The rapid commit option is included in solicit message, and two-messages handshake is required.
General Prefix Name	Enter the name of IPv6 general-prefix. The number of characters for the name can be up to 12.
IPv6 DHCP Client PD Hint	Enter an IPv6 prefix to transmit it as a hint with messages.

Click **Apply** to reflect the change.

6.5 IPv4 Default Route

Use the following window to implement the settings on an IPv4 default route and display its settings.

Choose **L3 Features > IPv4 Default Route** to display the following window.

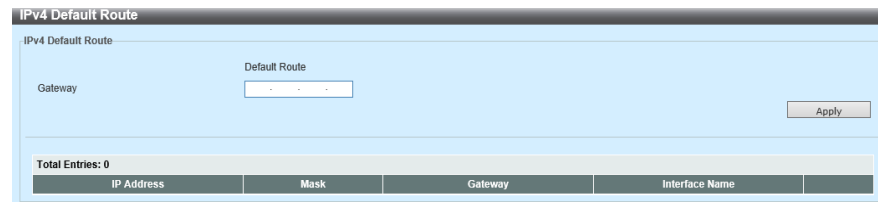


Figure 6-14 IPv4 Default Route

In these section of **IPv4 Default Route**, you can configure the following parameter.

Parameter	Overview
Gateway	Enter a gateway address of this route.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

6.6 IPv6 Default Route

Use the following window to implement the settings on an IPv6 default route and display its settings.

Choose **L3 Features > IPv6 Default Route** to display the following window.

Figure 6-15 IPv6 Default Route

In the section of **IPv6 Default Route**, you can configure the following parameters.

Parameter	Overview
IPv6 Address/Prefix Length	Enter an IPv6 address and prefix-length for this route. If you set Default Route to on, use this route for a default route.
Interface Name	Enter an interface name to be associated with this route.
Next Hop IPv6 Address	Enter an IPv6 address of the next hop.
Distance	Enter the distance for the static route management. The range is from 1 to 254. The lower the value, the better route will be. If not specified, the distance becomes 1 for managing a static-route (by default).

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

6.7 IPv6 General Prefix

Use the following window to implement the settings on the IPv6 general prefix and display its settings.

Choose **L3 Features > IPv6 General Prefix** to display the following window.

Figure 6-16 IPv6 General Prefix

In the section of the **IPv6 General Prefix**, you can configure the following parameters.

Parameter	Overview
Interface VLAN	Enter a VLAN interface ID to use. The range is from 1 to 4,094.
Prefix Name	Enter the name of an IPv6 general prefix-entry. The number of characters for the name can be up to 12.
IPv6 Address	Enter an IPv6 address and a prefix-length. The prefix-length of the IPv6 address can also be the local subnet of a VLAN interface.

Click **Apply** to add a new entry.

Click **Find** to search and display the entries based on the search condition specified.

Click **See All** to search and display all the entries available.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

7 QoS (Quality of Service)

7.1 Basic Settings

7.1.1 Port Default CoS

Use the following window to implement the settings on the default class of service (CoS) per port-interface and display its settings.

Choose **QoS > Basic Settings > Port Default CoS** to display the following window.

Port	Default CoS	Override
Fi1/0/1	0	No
Fi1/0/2	0	No
Fi1/0/3	0	No
Fi1/0/4	0	No
Te1/0/5	0	No
Te1/0/6	0	No

Figure 7-1 Port Default CoS

In the section of the **Port Default CoS**, you can configure the following parameter.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Default CoS	<p>Choose the default CoS option of the port to be specified. The range of values to choose is from 0 to 7.</p> <ul style="list-style-type: none"> If you choose Override, the CoS of packets is ignored. The default CoS is applied to all the incoming packets (tagged/untagged), which are received by ports. If you select None and packets are tagged, Cos of the packets becomes the Cos of packets, or if packets are not tagged, the default Cos of a ports becomes the CoS of the packets.

Click **Apply** to check the content changed.

7.1.2 Port Scheduler Method

Use the following window to implement the settings on the method for a scheduler function and display its settings.

Choose **QoS > Basic Settings > Port Scheduler Method** to display the following window.

Port	Scheduler Method
Fi1/0/1	WRR
Fi1/0/2	WRR
Fi1/0/3	WRR
Fi1/0/4	WRR
Te1/0/5	WRR
Te1/0/6	WRR

Figure 7-2 Port Scheduler Method

In the section of the **Port Scheduler Method**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.

Parameter	Overview
Scheduler Method	<p>Choose the scheduler method, which is applied to the port specified. The options available are as follows.</p> <ul style="list-style-type: none"> • Strict-Priority (SP) - This uses the strict-priority scheduling on all the queues. This is a strict-priority access that executes queues; the range is from the highest CoS queue to the lowest queue. • Round Robin (RR) - All the queues use and need a round robin scheduling. This is the fair access, which allows you to move to the next queue after providing one packet with services on each queue. • Weighted Round Robin (WRR) - This operates by transmitting permitted packets to the transmission queue in a sequential order of the round robin. At the beginning, each queue sets the weight to a configurable weighting. Every time packets coming from CoS queues with a higher priority are transmitted, the corresponding weights is subtracted by one. Then, the packets in the lower CoS queues receive services. If the weight of CoS queues reaches zero (0), the queue services stop until the queue is replenished. If the weight of all the CoS queues reaches 0, it becomes replenished at the time. This is the default option. • Weight Deficit Round Robin (WDRR) - Service are provided to the unprocessed credit, which is accumulated on the transmission-queue, in a sequential order of the round robin. At the beginning, each queue sets a credit counter to the value of configurable quantum. • Every time packets are transmitted from the CoS queue, the service right is provided to the next lower CoS queue. • If the value of a credit counter is less than 0, queue services stop before the credit is replenished. If the credit counter of all the CoS queues reaches 0, then it is replenished. The credit counter becomes 0 or minus, and then services are provided to all the packets before transmitting the last packet completely. If this occurs, the credit is replenished. • After that, the credit quantum is added to a credit counter of each CoS queue. The quantum of each CoS queue may differ depending on a user configuration. To set the specific CoS queue to the SP mode, all the CoS queues whose priorities are higher than it must be the strict-priority mode.

Click **Apply** to check the content changed.

7.1.3 Queue Settings

Use the following window to implement the settings on a QoS queue and display the settings.

Choose **QoS > Basic Settings > Queue Settings** to display the following window.

Port	Queue ID	WRR Weight	WDRR Quantum
F11/0/1	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1
F11/0/2	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1
F11/0/3	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1

Figure 7-3 Queue Settings

In the section of **Queue Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Queue ID	Enter the value of queue ID. The range is from 0 to 7.
WRR Weight	Enter the value of WRR weight. The range is from 0 to 127. To satisfy the operating requirements of Expedited Forwarding (EF), always choose the highest queue with Per-hop Behavior (PHB) EF. In addition, you need to designate the schedule mode of this queue as a strict priority scheduling. As long as a differentiate service is available to get supports, the weight of last queue must be 0.
WDRR Quantum	Enter the value of WDRR quantum. The range is from 0 to 127.

Click **Apply** to check the content changed.

7.1.4 CoS to Queue Mapping

Use the following window to implement the settings on CoS (transmission) to queue mapping and display its settings.

Choose **QoS > Basic Settings > CoS to Queue Mapping** to display the following window.

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

Apply

Figure 7-4 CoS to Queue Mapping

You can configure the following parameter.

Parameter	Overview
Queue ID	Choose a Queue ID to map the corresponding CoS-value. The range of the values is from 0 to 7.

Click **Apply** to check the content changed.

7.1.5 Port Rate Limiting

Use the following window to implement the settings on limiting port band frequency and display its settings.

Choose **QoS > Basic Settings > Port Rate Limiting** to display the following window.

Port	Input		Output	
	Rate	Burst	Rate	Burst
Fi1/0/1	No Limit	No Limit	No Limit	No Limit
Fi1/0/2	No Limit	No Limit	No Limit	No Limit
Fi1/0/3	No Limit	No Limit	No Limit	No Limit
Fi1/0/4	No Limit	No Limit	No Limit	No Limit
Te1/0/5	No Limit	No Limit	No Limit	No Limit
Te1/0/6	No Limit	No Limit	No Limit	No Limit

Figure 7-5 Port Rate Limiting

In the section of **Port Rate Limiting**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Direction	Choose a direction option. The options available are as follows. <ul style="list-style-type: none"> • Input - This configures to limit the bandwidth regarding the entry packets. • Output - This configures to limit the bandwidth regarding exit packets.

Parameter	Overview
Limiting a Band Frequency	<p>Choose and enter the value of limiting a bandwidth.</p> <ul style="list-style-type: none">• If you choose Bandwidth, enter the input/output bandwidth to use in the entry field displayed.• The range is from 8 to 40,000,000 (Kbps). Enter the Burst-size value in the entry field displayed. The range is from 0 to 128,000 (kilo-bytes).• If you select Percent, enter the input/output bandwidth using the unit as a percentage. The range is from 1 to 100 (percent). Enter the Burst-size value in the entry field displayed. The range is from 0 to 128,000 (kilo-bytes).• If you select None, limiting a band frequency on the specified port is removed. The specified limitation cannot exceed the maximum speed of the interface specified. In the case of the ingress bandwidth limitation, the ingress sends pause frames or flow control frames when the received traffics exceed the limitation.

Click **Apply** to check the content changed.

7.1.6 Queue Rate Limiting

Use the following window to implement the settings on limiting queue bandwidth and display its settings.

Choose **QoS > Basic Settings > Queue Rate Limiting** to display the following window.

Queue Rate Limiting

From Port: F1/0/1 To Port: F1/0/1 Queue ID: 0 Rate Limit: ☒ Min Bandwidth (64-100000000) Kbps Kbps

☐ Min Percent (1-100) % % %

☐ None

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
F1/0/1	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...
F1/0/2	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...
F1/0/3	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...
F1/0/4	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...
Te1/0/5	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...
Te1/0/6	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...

Figure 7-6 Queue Rate Limiting

In the section of **Limiting Queue Bandwidth**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Queue ID	Choose a queue ID to be configured. The range of values to choose is from 0 to 7.
Rate Limit (or Bandwidth Limitation)	<p>Choose and enter the configuration of limiting queue band. If you choose Minimum Bandwidth, enter it in the entry field where the minimum bandwidth for bandwidth-limitation is displayed.</p> <ul style="list-style-type: none"> • The range is from 8 to 40,000,000 (Kbps). • Enter the number in the entry field where the maximum bandwidth for bandwidth limitation is displayed. The range is from 8 to 40,000,000 (Kbps). If you configure the minimum bandwidth, packets transmitted from the queue are guaranteed (or assured). If you configure the maximum bandwidth, packets transmitted from the queues do not exceed the maximum bandwidth. If you configure the minimum bandwidth, the aggregation of the minimum bandwidth to be configured must be less than 75% of the interface bandwidth. Doing so ensures the minimum bandwidth (to be configured). You do not need to configure the minimally guaranteed bandwidth for the strict priority queue. The reason is this; if the minimum bandwidth of all the queues is satisfied, services are provided with this queue traffic first. The configuration of this command is attached to the physical port only, but is not attached to a port channel. This is the minimally guaranteed bandwidth of one CoS, so it cannot be used across the whole physical port(s). • If you choose the Minimum Percent option, enter the percent-value of the minimum bandwidth in the entry field provided. The range is from 1 to 100%. Enter the value of the Maximum Percent in the entry field provided. • If you choose None, the bandwidth limitation is not assigned to the port specified.

Click **Apply** to check the content changed.

7.2 Advanced Settings

7.2.1 DSCP Mutation Map

Use the following window to implement the settings on DSCP (Differentiated Services Code Point) mutation map and display its settings.

Choose **QoS > Advanced Settings > DSCP Mutation Map** to display the following window.

Figure 7-7 DSCP Mutation Map

In the section of a **DSCP Mutation Map**, you can configure the following parameters.

Parameter	Overview
Mutation Name	Enter the name of the DSCP mutation map. The number of characters for the name can be up to 32.
Input DSCP List	Enter the value of input DSCP list. The range is from 0 to 63.
Output DSCP List	Enter the value of output DSCP. The range is from 0 to 63.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

7.2.2 Port Trust State and Mutation Binding

Use the following window to implement the settings on **Port Trust State and Mutation Binding** and display its settings.

Choose **QoS > Advanced Settings > Port Trust State and Port Trust State Mutation Binding** to display the following window.

Port	Trust State	DSCP Mutation Map
Fi1/0/1	Trust CoS	
Fi1/0/2	Trust CoS	
Fi1/0/3	Trust CoS	
Fi1/0/4	Trust CoS	
Te1/0/5	Trust CoS	
Te1/0/6	Trust CoS	

Figure 7-8 Port Trust State and Mutation Binding

In the section of **Port Trust State and Mutation Binding**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Trust State	Choose the port trust state. The options available are CoS and DSCP . The options available are CoS and DSCP .
DSCP Conversion Map	Choose and enter the name of a DSCP conversion map to use. The number of characters for the name can be up to 32. If you choose None , a DSCP conversion map is not assigned to a port.

Click **Apply** to check the content changed.

7.2.3 DSCP CoS Mapping

Use the following window to implement the settings on a DSCP CoS mapping and display its settings.

Choose **QoS > Advanced Settings > DSCP CoS Mapping** to display the following window.

Port	CoS	DSCP List
F1/0/1	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63
F1/0/2	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63
F1/0/3	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63

Figure 7-9 DSCP CoS Mapping

In the section of the **DSCP CoS Mapping**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
CoS	Enter the CoS value for mapping the DSCP list. The range of the value to choose is from 0 to 7.
DSCP List	Enter the DSCP list value to map the CoS value. The range is from 0 to 63.

Click **Apply** to check the content changed.

7.2.4 CoS Color Mapping

Use the following window to implement the settings on a CoS color mapping and display its settings.

Choose **QoS > Advanced Settings > CoS Color Mapping** to display the following window.

Port	Color	CoS List
F1/0/1	Green	0-7
F1/0/1	Yellow	0-7
F1/0/1	Red	0-7
F1/0/2	Green	0-7
F1/0/2	Yellow	0-7
F1/0/2	Red	0-7
F1/0/3	Green	0-7
F1/0/3	Yellow	0-7
F1/0/3	Red	0-7
F1/0/4	Green	0-7
F1/0/4	Yellow	0-7
F1/0/4	Red	0-7
Ts1/0/5	Green	0-7
Ts1/0/5	Yellow	0-7
Ts1/0/5	Red	0-7
Ts1/0/5	Green	0-7
Ts1/0/5	Yellow	0-7
Ts1/0/5	Red	0-7

Figure 7-10 CoS Color Mapping

In the section of **CoS Color Mapping**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
CoS List	Enter the CoS value to map colors. The range is from 0 to 7.
Color	Choose the color option to map the CoS value. The options available are Green , Yellow and Red .

Click **Apply** to check the content changed.

7.2.5 DSCP Color Mapping

Use the following window to implement the settings on DSCP color mapping and display its settings.

Choose **QoS > Advanced Settings > DSCP Color Mapping** to display the following window.

Port	Color	DSCP List
F10/01	Green	0-63
	Yellow	
	Red	
F10/02	Green	0-63
	Yellow	
	Red	
F10/03	Green	0-63
	Yellow	
	Red	
F10/04	Green	0-63
	Yellow	
	Red	
Te1/0/5	Green	0-63
	Yellow	
	Red	
Te1/0/6	Green	0-63
	Yellow	
	Red	

Figure 7-11 DSCP Color Mapping

In the section of the **DSCP Color Mapping**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
DSCP List	Enter the value of DSCP list to map colors. The range is from 0 to 63.
Color	Choose the color option to map the DSCP value. The options available are Green , Yellow and Red .

Click **Apply** to check the content changed.

7.2.6 Class Map

Use the following window to configure a class map and display its settings.

Choose **QoS > Advanced Settings > Class Map** to display the following window.

Figure 7-12 Class Map

You can configure the following parameters.

Parameter	Overview
Class Map Name	Enter the name of a class map. The number of characters for the name can be up to 32.
Multiple Match Criteria	Choose Multiple Match Criteria from options. The options available are Match All and Match Any .

Click **Apply** to add a new entry.

Click **Match** to configure the match rule of the entry specified.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Match** to display the following window.

Figure 7-13 Class Map (Match)

You can configure the following parameters.

Parameter	Overview
None	If you choose this option, nothing is matched with this class map.
Specify	If you choose this option, one of the following parameters is matched with this class map.
ACL Name	Choose and enter the name of the access list to be matched with this class map. The number of characters for the name can be up to 32.
CoS List	Choose and enter the value of CoS list to be matched with this class map. The range is from 0 to 7.
DSCP List	Choose and enter the value of DSCP list to be matched with this class map. The range is from 0 to 63. If you set IPv4 to on, only IPv4 packets are matched. If not specified, the reconciliation (or cross-check) targets for both IPv4 and IPv6 packets.
Precedence List	Choose and enter the value of a precedence list that matches with this class map. The range is from 0 to 7. If you set the IPv4 option to on, IPv4 packets are matched, only. If not specified, the reconciliation targets for both IPv4 and IPv6 packets. In the case of IPv6 packets, the top three-bits of traffic class for the IPv6 header can be the precedence. The range is from 0 to 7.
Protocol Name	Choose a protocol name to match it with this class map. The options available are ARP, BGP, DHCP, DNS, EGP, FTP, IPv4, IPv6, NetBIOS, NFS, NTP, OSPF, PPPOE, RIP, RTSP, SSH, Telnet and TFTP .
VID List	Choose and enter a VLAN ID to match it with the class map. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of the VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.

Click **Apply** to check the content changed.

Click **Back** to return to the previous window.

7.2.7 Aggregate Policer

Use the following window to implement the settings on the aggregate policer and display its settings.

Choose **QoS > Advanced Settings > Aggregate Policer** to display the following window.

The screenshot shows the 'Aggregate Policer' configuration window. It has two tabs: 'Single Rate Settings' (selected) and 'Two Rate Settings'. Under 'Single Rate Settings', there are fields for 'Aggregate Policer Name' (with an asterisk indicating it's mandatory), 'Average Rate' (0-10000000 Kbps), 'Normal Burst Size' (0-16384 Kbyte), 'Maximum Burst Size' (0-16384 Kbyte), 'Conform Action' (dropdown menu with 'Transmit' selected), 'Exceed Action' (dropdown menu with 'Transmit' selected), 'Violate Action' (dropdown menu with 'None' selected), and 'Color Aware' (dropdown menu with 'Disabled' selected). There are also 'Apply' and 'Cancel' buttons. At the bottom, there is a table with 8 columns: Name, Average Rate, Normal Burst Size, Max. Burst Size, Conform Action, Exceed Action, Violate Action, and Color Aware. The table currently shows 'Total Entries: 0'.

Figure 7-14 Aggregate Policer (Single Rate Settings)

In the section of the **Single Rate Settings**, you can configure the following parameters.

Parameter	Overview
Aggregate Policer Name	Enter the name of the aggregate policer.
Average Rate	Enter the value of the average rate. The range is from 0 to 10,000,000 (Kbps).
Normal Burst Size	Enter the value of a normal burst size. The range is from 0 to 16,384 (Kbyte).
Maximum Burst Size	Enter the value of the maximum burst size. The range is from 0 to 16,384 (Kbyte).

Parameter	Overview
Confirm Action	<p>Choose a confirm action. The action specifies the action to execute for green colored packets. If the action is not specified, the default action is to Transmit. The options available are as follows.</p> <ul style="list-style-type: none"> • Drop - This option allows you to drop the packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the DSCP value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the entry field displayed. • Transmission - If you choose this option, packets are transmitted without switching them. • DSCP-1P Configuration - This option allows you to configure and transmit the value of new DSCP and IEEE 802.1p to packets. Enter the values in the entry field displayed.
Exceed Action	<p>Choose the exceed action. The action specifies the action needed on the packets, which exceed the bandwidth-limitation. Regarding a two-rate policer, if the exceed action is not specified, the default action is Drop. The options available are as follows.</p> <ul style="list-style-type: none"> • Drop - This option allows you to drop packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of IEEE 802.1p to packets. Enter the value in the entry field displayed. • Transmission - This option allows you to transmit packets without switching them. • DSCP-1P Configuration - This option allows you to configure and transmit the value of new DSCP and IEEE 802.1p to packets. Enter the values in the entry field displayed.

Parameter	Overview
Violate Action	<p>Choose the violate-action. The action specifies the action to be taken on the packets, which violate the normal and maximum burst sizes for single-rate policing. Specify the action you take on the packets which conform to neither CIR nor PIR.</p> <ul style="list-style-type: none"> Regarding a single-rate policer, if the violate action is not specified, a single-rate two-color policer is created. Regarding a two-rate policer, if the violation action is not specified, the default action becomes the exceed action. <p>The options available are as follows.</p> <ul style="list-style-type: none"> Nothing - No action is taken. Drop - This option allows you to drop the packets. Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the DSCP value in the entry field displayed. Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the entry field displayed. Transmission - This option allows you to transmit packets without switching them. DSCP-1P Configuration - This option allows you to configure and transmit the values of new DSCP and IEEE 802.1p to packets. Enter the values in the entry field displayed.
Color Aware	<p>This parameter enables or disables the function of the color aware.</p> <ul style="list-style-type: none"> If the color aware is Enabled, the policer operates as the color aware mode. If the color aware is Disabled, the policer operates as the color blind mode.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click the **2 Rate Settings** tab to display the following window.

The screenshot shows the 'Aggregate Policer' configuration window with the 'Two Rate Settings' tab selected. The window contains several input fields and dropdown menus for configuring the policer's behavior. At the bottom, there is a table showing the total entries and a list of configured entries.

Aggregate Policer								
Single Rate Settings			Two Rate Settings					
Aggregate Policer Name *	<input type="text"/>							
CIR * (0-10000000)	<input type="text"/>	Kbps	Confirm Burst (0-16384)	<input type="text"/>	Kbyte			
PIR * (0-10000000)	<input type="text"/>	Kbps	Peak Burst (0-16384)	<input type="text"/>	Kbyte			
Conform Action	<input type="button" value="Transmit"/>	<input type="button" value="Drop"/>	Exceed Action	<input type="button" value="Drop"/>	<input type="button" value="Transmit"/>			
Violate Action	<input type="button" value="Drop"/>	<input type="button" value="Transmit"/>	Color Aware	<input type="button" value="Disabled"/>	<input type="button" value="Enabled"/>			
* Mandatory Field								
<input type="button" value="Apply"/>								
Total Entries: 0								
Name	CIR	Confirm Burst	PIR	Peak Burst	Conform Action	Exceed Action	Violate Action	Color Aware

Figure 7-15 Aggregate Policer (2 Rate Settings)

In the section of **2 Rate Settings**, you can configure the following parameters.

Parameter	Overview
Name of Aggregate Policer	Enter the name of an aggregate policer.
CIR	Enter the value of CIR (Committed Information Rate). The range is from 0 to 10,000,000 (Kbps). The certified packet rate is the first token bucket for the two-rate metering.
Burst Confirmation	Enter the value of a burst confirmation. The range is from 0 to 16,384 (Kbyte). The value of the confirmation specifies the burst size for the first token bucket in kbps.
PIR	Enter the value of PIR (Peak Information Rate). The range is from 0 to 10,000,000 (Kbps). The rate is the second token bucket for the 2 rate metering.
Peak Burst	Enter the value of the peak burst. The range is from 0 to 16,384 (Kbyte). This is the burst size of the second token bucket (kilo-bytes).

Parameter	Overview
Confirm Action	<p>Choose the confirm action. The action specifies the action to be taken for green colored packets. If the action is not specified, the default action is Transmit.</p> <p>The options available are as follows.</p> <ul style="list-style-type: none"> • Drop - This option allows you to drop the packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the space provided. • Transmission - This option allows you to transmit packets without switching them. • DSCP-1P Configuration - This option allows you to configure and transmit the value of new DSCP and IEEE 802.1p to packets. Enter the values of DSCP and IEEE 802.1p in the space provided.
Exceed Action	<p>Choose the exceed action. The exceed action specifies an action to be taken on the packets, which exceed the rate limit. For a two-rate policer, if the exceed action is not specified, the default action is Drop.</p> <p>The options available are as follows.</p> <ul style="list-style-type: none"> • Drop - This option allows you to drop the packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the value in the entry field displayed. • Transmission - This option allows you to transmit packets without switching them. • DSCP-1P Configuration - This option allows you to configure and transmit the value of new DSCP and IEEE 802.1p to packets. • Enter the values of DSCP and IEEE 802.1p in the entry field provided.

Parameter	Overview
Violate Action	<p>Choose the violate action. The action specifies the action you take on the packets, which violate the normal and maximum burst size for a single rate policing. It specifies the action you take on the packets, which conform to neither CIR nor PIR.</p> <ul style="list-style-type: none"> Regarding a single rate policer, if the violate action is not specified, a single-rate two-color policer is created. Regarding a two-rate policer, if the violation action is not specified, the default action becomes the exceed action. <p>The options available are as follows.</p> <ul style="list-style-type: none"> Drop - This option allows you to drop the packets. Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the DSCP value in the entry field displayed. Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the entry field displayed. Transmission - This option allows you to transmit packets without switching them. DSCP-1P Configuration - This option allows you to configure the values of DSCP and IEEE 802.1p in packets to transmit them. Enter the values of DSCP and IEEE 802.1p in the entry field displayed.
Color Aware	<p>This parameter enables or disables the function of the color aware.</p> <ul style="list-style-type: none"> If the color aware is Enabled, a policer operates with the color aware mode. If the color aware is Disabled, the policer operates with the color blind mode.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

7.2.8 Policy Map

Use the following window to implement the settings on a policy map and display its settings.

Choose **QoS > Advanced Settings > Policy Map** to display the following window.

Figure 7-16 Policy Map

In the section of **Create/Delete Policy Map**, you can configure the following parameter.

Parameter	Overview
Name of a Policy Map	Enter the name of a policy map to create or delete. The number of characters for the name can be up to 32.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

In the section of **Traffic Policy**, you can configure the following parameters.

Parameter	Overview
Name of a Policy Map	Enter the name of a policy map. The number of characters for the name can be up to 32.
Name of a Class Map	Enter the name of a class map. The number of characters for the name can be up to 32.

Click **Apply** to add a new entry.

Click **Set Action** to configure the action of the entries specified.

Click **Policer** to configure the police action for the entry specified.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Set Action** to display the following window.

Figure 7-17 Policy Map (Action Settings)

In the section of **Set Action**, you can configure the following parameters.

Parameter	Overview
None	If you choose this option, no action is taken.
Specify	If you choose this option, an action needs to be taken based on a configuration.
New Precedence	Choose the value of the new precedence for packets. The range is from 0 to 7. If you choose the IPv4 Only option, the IPv4 precedence is marked. If you do not choose it, the precedence for both IPv4 and IPv6 is marked. In the case of IPv6 packets, the top (three-bits) traffic class for the IPv6 header can be the precedence.
New DSCP	Choose the value of new DSCP for packets. The range is from 0 to 63. If you choose IPv4 Only , the IPv4 DSCP is marked. If you do not choose it, DSCP for both IPv4 and IPv6 is marked.
New CoS	Choose the value of new CoS for packets. The range is from 0 to 7.
New CoS Queue	Choose the value of a new CoS queue for packets. Doing so overwrites the original CoS queue selection. If the policy map is applied to the exit-flow of an interface, the settings on the CoS queue does not become enabled.

Click **Apply** to check the content changed.

Click **Back** to return to the previous window.

Click **Policer** and then specify **Police** as a police action to display the following window.

Figure 7-18 Policy Map (Policer and Police)

In the section of **Police Action**, you can configure the following parameters.

Parameter	Overview
None	If you choose this option, a policer is not configured on this entry.
Specify	If you choose this option, the following policer configuration is applied on this entry.
Average Rate	Enter a value of the average rate. The range is from 0 to 10,000,000 (Kbps).
Normal Burst Size	Enter the value of a normal burst size. The range is from 0 to 16,384 (Kbps).
Maximum Burst Size	Enter the value of the maximum burst size. The range is from 0 to 16,384 (Kbps).

Parameter	Overview
Conform Traffic Action	<p>Choose the conform-traffic action to be taken. Perform the action on green colored packets. The options available are as follows.</p> <ul style="list-style-type: none"> • Drop - This option allows you to drop the packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the DSCP value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the entry field displayed. • Transmission - This option allows you to transmit packets without changing them. • DSCP-1P Configuration - This option allows you to configure and transmit the values of a new DSCP and IEEE 802.1p to packets. Enter the values in the entry field displayed.
Exceed Action	<p>Choose the exceed-action to be taken. This action is taken on the yellow colored packets, which exceed the bandwidth limitation. The options available are as follows.</p> <ul style="list-style-type: none"> • Drop - This option allows you to drop the packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the DSCP value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the entry field displayed. • Transmission - This option allows you to transmit packets without changing them. • DSCP-1P Configuration - This option allows you to configure and transmit the values of a new DSCP and IEEE 802.1p to packets. Enter the values in the entry field displayed.

Parameter	Overview
Violate Action	<p>Choose the violate action to perform it. This action is performed on red colored packets. The options available are as follows.</p> <ul style="list-style-type: none"> • None - No violate action is taken. • Drop - This option allows you to drop the packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the DSCP value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the entry field displayed. • Transmission - This option allows you to transmit packets without changing them. • DSCP-1P Configuration - This option allows you to configure and transmit the values of a new DSCP and IEEE 802.1p to packets. Enter the values in the entry field displayed.
Color Aware	<p>This parameter enables or disables the function of the color aware.</p> <ul style="list-style-type: none"> • If enabled, the policer operates as the color aware mode. • If disabled, the policer operates as the color blind mode.

Click **Apply** to check the content changed.

Click **Back** to return to the previous window.

Click the **Policer** button, and then specify the **Police CIR** as a police action to display the following window.

Figure 7-19 Policy Map (Policer, Police CIR)

In the section of **Police Action**, you can configure the following parameters.

Parameter	Overview
None	If you choose this option, a policer is not configured in this entry.
Specify	If you choose this option, the following policer configuration is applied in this entry.
CIR	Enter the value of CIR (Committed Information Rate). This is the first token bucket for two-rate metering. The range is from 0 to 10,000,000 (Kbps).
Confirm Burst	Enter the value of a burst confirmation. This is the size of the first token bucket. The range is from 0 to 16,384 (kilo-bytes).
PIR	Enter the value of PIR (Peak Information Rate). This is the second token bucket for two-rate metering. The range is from 0 to 10,000,000.
Peak Burst	Enter the value of the peak burst. This is the size of the second token bucket. The range is from 0 to 16,384 (kilo-bytes).
Conform Traffic Action	<p>Choose the conform traffic action to execute. This action is performed on green colored packets. The options available are as follows.</p> <ul style="list-style-type: none"> • Drop - This option allows you to drop the packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the DSCP value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the entry field displayed. • Transmission - This option allows you to transmit packets without changing them. • DSCP-1P Configuration - This option allows you to configure and transmit the values of a new DSCP and IEEE 802.1p to packets. Enter the values in the entry field displayed.

Parameter	Overview
Exceed Action	<p>Choose the exceed-action to be taken. This action is taken on the yellow colored packets, which exceed the bandwidth limitation. The options available are as follows.</p> <ul style="list-style-type: none"> • Drop - This option allows you to drop the packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the DSCP value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the entry field displayed. • Transmission - This option allows you to transmit packets without changing them. • DSCP-1P Configuration - This option allows you to configure and transmit the values of a new DSCP and IEEE 802.1p to packets. Enter the values in the entry field displayed.
Violate Action	<p>Choose a violate action to be taken. This action is executed for the red colored packets. The options available are as follows.</p> <ul style="list-style-type: none"> • None - No violate action is taken. • Drop - This option allows you to drop the packets. • Set-DSCP-Transmit - This option allows you to configure and transmit the value of new DSCP to packets. Enter the DSCP value in the entry field displayed. • Set-1P-Transmit - This option allows you to configure and transmit the value of new IEEE 802.1p to packets. Enter the IEEE 802.1p value in the entry field displayed. • Transmission - This option allows you to transmit packets without changing them. • DSCP-1P Configuration - This option allows you to configure and transmit the values of a new DSCP and IEEE 802.1p to packets. Enter the values in the entry field displayed.
Color Aware	<p>This parameter enables or disables the function of the color aware.</p> <ul style="list-style-type: none"> • If enabled, the policer operates as the Color Aware mode. • If disabled, the policer operates as the color blind mode.

Click **Apply** to check the content changed.

Click **Back** to return to the previous window.

Click the **Policer** button, and then specify the **Police Aggregate** as **Police Action** to display the following window.

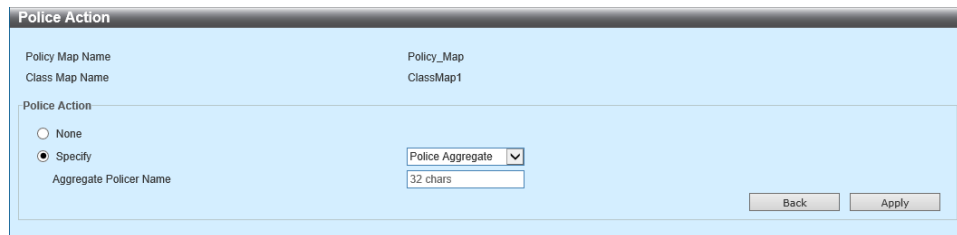


Figure 7-20 Policy Map (Policer and Police Aggregate)

In the section of **Police Action**, you can configure the following parameters.

Parameter	Overview
None	If you choose this option, a policer is not configured on this entry.
Specify	If you choose this option, the following policer configuration is applied on this entry.
Aggregate Policer Name	Enter the name of an aggregate policing rule. The number of characters for the name can be up to 32.

Click **Apply** to check the content changed.

Click **Back** to return to the previous window.

7.2.9 Policy Binding

Use the following window to implement the settings on a policy binding and display its settings.

Choose **QoS > Advanced Settings > Policy Binding** to display the following window.

Port	Direction	Policy Map Name
Fi1/0/1		
Fi1/0/2		
Fi1/0/3		
Fi1/0/4		
Te1/0/5		
Te1/0/6		

Figure 7-21 Policy Binding

In the section of the settings on a **Policy Binding**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Direction	Choose a direction option. The options available are Input and Output . Specify the entry traffic for Input and exit traffic for Output , respectively.
Name of a Policy Map	Enter the name of a policy map. The number of characters for the name can be up to 32. <ul style="list-style-type: none"> If you choose None, a policy map is not associated with this entry.

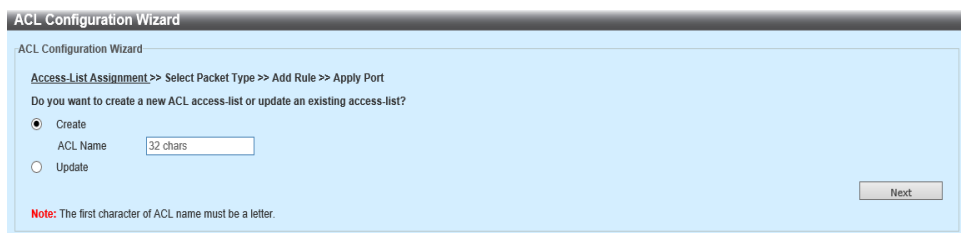
Click **Apply** to check the content changed.

8 ACL (Access Control List)

8.1 ACL Configuration Wizard

Use the following window to configure new and existing ACLs on the ALC configuration wizard.

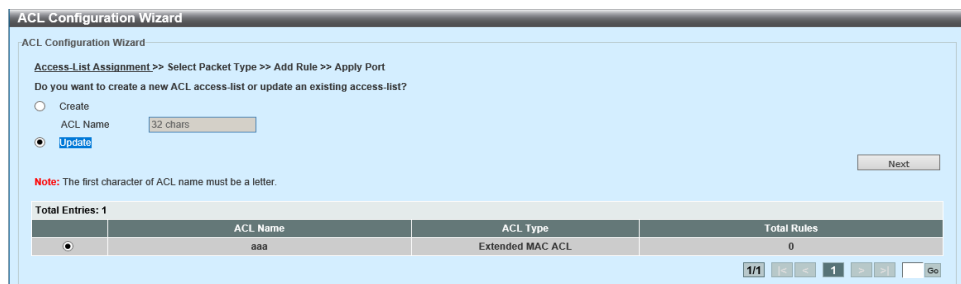
Choose **ACL > ACL Configuration Wizard** to display the following window.



The screenshot shows the 'ACL Configuration Wizard' window. The title bar says 'ACL Configuration Wizard'. Inside, the breadcrumb is 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port'. The main text asks 'Do you want to create a new ACL access-list or update an existing access-list?'. There are two radio buttons: 'Create' (selected) and 'Update'. Below 'Create' is a text field for 'ACL Name' with a '32 chars' limit. A 'Next' button is on the right. A red note at the bottom says 'Note: The first character of ACL name must be a letter.'

Figure 8-1 ACL Configuration Wizard (Create)

Click **Update** to display the following window.



The screenshot shows the 'ACL Configuration Wizard' window with the 'Update' radio button selected. The 'ACL Name' field now contains 'aaa'. Below the form is a table showing the current configuration.

Total Entries: 1			
	ACL Name	ACL Type	Total Rules
<input checked="" type="radio"/>	aaa	Extended MAC ACL	0

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

Figure 8-2 ACL Configuration Wizard (Update)

You can configure the following parameters.

Parameter	Overview
Create	Choose this option to create a new ALC access list using the configuration wizard.
ACL Name	Enter a new ACL name. The number of characters for the name can be up to 32.
Update	Choose this option to update an existing ACL access list. Choose the existing ACL in a table to be updated.

Click **Next** to proceed to the next step in the wizard.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

If you click **Create ACL** and **Next** from the **Create** option, the following window is displayed.

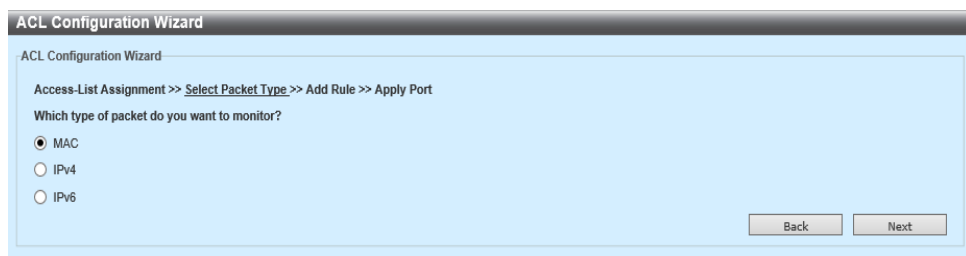


Figure 8-3 ACL Configuration Wizard (Choose ACL Type)

You can configure the following parameters.

Parameter	Overview
MAC	If you choose this option, MAC ACL is created.
IPv4	If you choose this option, IPv4 ACL is created.
IPv6	If you choose this option, IPv6 ACL is created.

Click **Next** to proceed to the next step in the wizard.

Click **Back** to return to the previous step in the wizard.

8.1.1 MAC ACL

After you choose **Create/Update** from **MAC ACL**, the following window is displayed.

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

☒ Sequence No. (1-65535) ☐ Auto Assign

Assign Rule Criteria

MAC Address **Ethernet Type** **802.1Q VLAN**

MAC Address

Source ☒ Any ☐ Host ☐ MAC ☐ Wildcard 11-DF-36-4B-A7-CC

Destination ☒ Any ☐ Host ☐ MAC ☐ Wildcard 11-DF-36-4B-A7-CC

Ethernet Type

Specify Ethernet Type Please Select

Ethernet Type (0x0-0xFFFF)

Ethernet Type Mask (0x0-0xFFFF)

802.1Q VLAN

CoS Please Select

VID (1-4094)

Mask (0x0-0x7)

Mask (0x0-0xFF)

Time Range 32 chars

Action ☒ Permit ☐ Deny

Back Next

Figure 8-4 ACL Configuration Wizard (Configuration of MAC ACL)

You can configure the following parameters.

Parameter	Overview
Sequence Number	Enter the ACL rule number. The range is from 1 to 65,535. Choose Auto Assign to automatically generate the ACL rule number for this entry.
Source	Choose and enter the source MAC address information. The options available are as follows. <ul style="list-style-type: none"> • Optional - Evaluates the optional source traffic according to this rule condition. • Host - Enter a source-host MAC address. • MAC - Enter a source MAC address and the Wildcard value in the entry field displayed.
Destination	Choose and enter the destination MAC address information. The options available are as follows. <ul style="list-style-type: none"> • Optional - Evaluates an optional destination traffic according to this rule condition. • Host - Enter a destination-host MAC address. • MAC - Enter a destination MAC address and the Wildcard value in the entry field displayed.
Specify Ethernet Type	Choose the Ethernet-type option. The options available are aarp , appletalk , decent-iv , etype-6000 , etype-8042 , lat , lavc-sca , mop-console , mop-dump , vines-echo , vines-ip , xns-idp and arp .

Parameter	Overview
Ethernet Type	Enter the Ethernet-type with hexadecimal-value. The range is from 0x600 to 0xFFFF. If you choose an optional Ethernet-type profile from the Specify Ethernet Type drop-down list, the appropriate hexadecimal-value is automatically displayed.
Ethernet Type Mask	Enter the Ethernet-type mask with hexadecimal-value. The range is from 0x0 to 0xFFFF. If you choose an optional Ethernet-type profile from the Specify Ethernet Type drop-down list, the appropriate hexadecimal-value is automatically displayed.
CoS	Choose the CoS-value you use. The range is from 0 to 7. <ul style="list-style-type: none"> Mask - Enter the CoS mask value. The range is from 0x0 to 0x7.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094. <ul style="list-style-type: none"> Mask - Enter the value of VLAN ID mask. The range is from 0x0 to 0xFFFF.
Time Range	Enter the name of the time-range profile, which is used in this ACL rule. The number of characters for the name can be up to 32.
Action	Choose an action to execute with this rule. The options available are Permit , Reject , and Reject CPU .

Click **Next** to proceed to the next step in the wizard.

Click **Back** to return to the previous step in the wizard.

After you click **Next** (in the previous step), the following window is displayed.

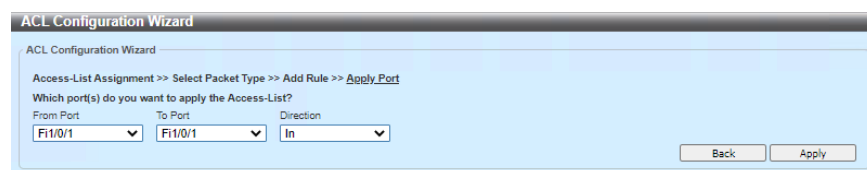


Figure 8-5 ACL Configuration Wizard (Choosing a port and direction)

You can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Direction	Choose a direction. The options available are In and Out .

Click **Apply** to check the changes made and return to the **ACL Configuration Wizard** window.

Click **Back** to return to the previous step in the wizard.

8.1.2 IPv4

If you choose **Update** from the standard IP ACL, the following window is displayed.

The screenshot shows the 'ACL Configuration Wizard' window for configuring a standard IP ACL. The progress bar indicates the steps: Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port. The current step is 'Add Rule', where the user is prompted to 'Please assign a sequence number to create a new rule.' The 'Sequence No. (1-65535)' field is empty, and the 'Auto Assign' radio button is selected. The 'Protocol Type' is set to 'TCP'. Below this, the 'Assign Rule Criteria' section has tabs for 'IPv4 Address', 'Port', 'IPv4 DSCP', and 'TCP Flag'. The 'IPv4 Address' tab is active, showing 'Source' and 'Destination' sections. Both have radio buttons for 'Any', 'Host', 'IP', and 'Wildcard'. The 'Any' radio button is selected for both. The 'Time Range' field is set to '32 chars'. The 'Action' section has radio buttons for 'Permit' (selected) and 'Deny'. 'Back' and 'Next' buttons are at the bottom right.

Figure 8-6 ACL Configuration Wizard (Configuration of a Standard IP ACL)

If you choose **Update an Extended IP ACL** or **Create an IPv4 ACL**, the following window is displayed.

The screenshot shows the 'ACL Configuration Wizard' window for configuring an extended IP ACL. The progress bar indicates the steps: Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port. The current step is 'Add Rule', where the user is prompted to 'Please assign a sequence number to create a new rule.' The 'Sequence No. (1-65535)' field is empty, and the 'Auto Assign' radio button is selected. The 'Protocol Type' is set to 'TCP'. Below this, the 'Assign Rule Criteria' section has tabs for 'IPv4 Address', 'Port', 'IPv4 DSCP', and 'TCP Flag'. The 'IPv4 Address' tab is active, showing 'Source' and 'Destination' sections. Both have radio buttons for 'Any', 'Host', 'IP', and 'Wildcard'. The 'Any' radio button is selected for both. The 'Port' section has 'Source Port' and 'Destination Port' dropdowns, all set to 'Please Select'. The 'IPv4 DSCP' section has 'IP Precedence' and 'ToS' dropdowns, all set to 'Please Select'. The 'TCP Flag' section has checkboxes for 'ack', 'fin', 'psh', 'rst', 'syn', and 'urg'. The 'Time Range' field is set to '32 chars'. The 'Action' section has radio buttons for 'Permit' (selected) and 'Deny'. 'Back' and 'Next' buttons are at the bottom right.

Figure 8-7 ACL Configuration Wizard (Configuration of an Extended IP ACL)

You can configure the following parameters.

Parameter	Overview
Sequence Number	Enter the ACL rule number. The range is from 1 to 65,535. If you choose Auto Allocation , the ACL rule number regarding this entry is automatically generated.
Protocol Type	<p>Choose the protocol type option. The options available are TCP, UDP, ICMP, EIGRP (88), ESP (50), GRE (47), IGMP (2), OSPF (89), PIM (103), VRRP (112), IP-in-IP (94), PCP (108), Protocol ID and None.</p> <ul style="list-style-type: none"> • Value - You can enter the protocol ID, manually. The range is from 0 to 255. • Mask - After choosing the Protocol ID option, enter the value of the protocol mask, manually. The range is from 0x0 to 0xFF. • Fragment - If you choose this option, the packet fragment filtering is included.
Source	<p>Choose and enter the source information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates optional source traffics according to this rule condition. • Host - Uses and enters an IP address of source host. • IP - Use the bit-map of Wildcard, and then use and enter a group of the source IP address. The bit corresponding to the bit-value of 1 is ignored, but the bit corresponding to the bit-value of 0 is checked.
Destination	<p>Choose and enter the destination information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates the optional destination traffic according to this rule condition. • Host - Uses and enters an IP address of a destination host. • IP - Use the bit-map of Wildcard, and then use and enter a group of the destination IP address. The bit corresponding to the bit value of 1 is ignored, but the bit corresponding to the bit value of 0 is checked.

Parameter	Overview
Source Port	<p>Choose and enter the value of the source port. The options available are as follows.</p> <ul style="list-style-type: none"> • = - ACL uses the port-number specified, only. • > - ACL uses all the ports, which are greater than the port-number specified. • < - ACL uses all the ports, which are smaller than the port-number specified. • ≠ - ACL uses all the ports except the port-number specified. • Range - ACL uses the port, which is specified within the range. • Mask - ACL uses the port within the range of the mask specified. Enter the value of a port-mask in the entry field displayed. The range is from 0x0 to 0xFFFF. <p>This parameter is available when you select TCP or UDP as the protocol type.</p>
Destination Port	<p>Choose and enter the value of the destination port. The options available are as follows.</p> <ul style="list-style-type: none"> • = - ACL uses the port-number specified, only. • > - ACL uses all the ports, which are greater than the port-number specified. • < - ACL uses all the ports, which are smaller than the port-number specified. • ≠ - ACL uses all the ports except the port-number specified. • Range - ACL uses the port, which is specified within the range. • Mask - ACL uses the port within the range of the mask specified. Enter the value of a port-mask in the entry field displayed. The range is from 0x0 to 0xFFFF. <p>This parameter is available when you select TCP or UDP as the protocol type.</p>
Specify ICMP Message Type	<p>Choose the ICMP Message Type you use. This parameter is available when you select ICMP as the protocol type.</p>
ICMP Message Type	<p>If you do not choose the Specify ICMP Message type, enter the numerical value of the ICMP Message Type you use. The range is from 0 to 255. If you choose the ICMP Message Type, the numerical value of the message type is automatically entered. This parameter is available when you select ICMP as the protocol type.</p>

Parameter	Overview
Message Code	If you do not choose the Specify ICMP Message type, enter the numerical value of a message code you use. The range is from 0 to 255. If you choose the ICMP Message Type , the numerical value of the message type is automatically entered. This parameter is available when you select ICMP as the protocol type.
IP Precedence	Choose the value of IP precedence you use. The options available are routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), Internet (6) and network (7). <ul style="list-style-type: none"> • Value - You can enter the value of the IP precedence, manually. The range is from 0 to 7. • Mask - Enter the value of an IP precedence mask. The range is from 0x0 to 0x7.
ToS	Choose the value of Type-of-Service (ToS). The options available are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4) and min-delay (8). <ul style="list-style-type: none"> • Value - You can enter the ToS value, manually. The range is from 0 to 15. • Mask - Enter the ToS mask value. The range is from 0x0 to 0xF.
DSCP	Choose the DSCP value. The options available are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56) and ef (46). <ul style="list-style-type: none"> • Value - You can manually enter the DSCP value. The range is from 0 to 63. • Mask - Enter the value of DSCP mask. The range is from 0x0 to 0x3F.
TCP Flag	Choose the TCP flag to evaluate for this ACL. The options available are ack , fin , psh , rst , syn and urg . This parameter is available only if you choose TCP from the Protocol Type .
Time-Range	Enter the name of the time-range profile used in this ACL rule. The number of characters for the name can be up to 32.
Action	Choose an action to execute with this rule. The options available are Permit and Reject .

Click **Next** to proceed to the next step in the wizard.

Click **Back** to return to the previous step in the wizard.

After you click **Next** (in the previous step), the following window is displayed.

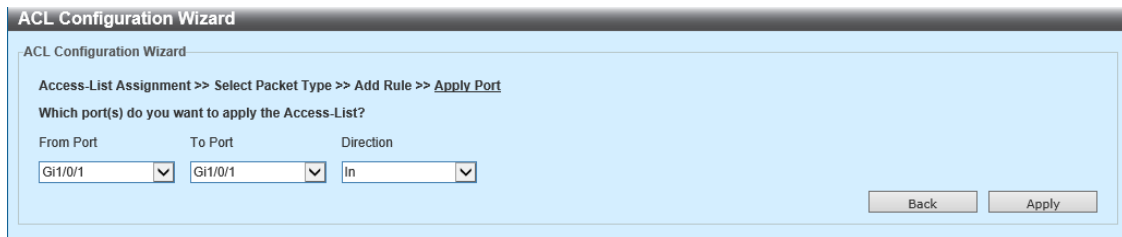


Figure 8-8 ACL Configuration Wizard (IPv4, Step 3)

You can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Direction	Choose a direction. The options available are In and Out .

Click **Apply** to check the content changed and return to the **ACL Configuration Wizard** window.

Click **Back** to return to the previous step in the wizard.

8.1.3 IPv6

If you choose to update the **Standard IPv6 ACL**, the following window is displayed.

The screenshot shows the 'ACL Configuration Wizard' window. The title bar reads 'ACL Configuration Wizard'. Below the title bar, the progress bar shows 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port'. The main area is titled 'Please assign a sequence number to create a new rule.' and has two radio buttons: 'Sequence No. (1-65535)' (selected) and 'Auto Assign'. Below this is the 'Assign Rule Criteria' section. It has a tab labeled 'IPv6 Address'. Under this tab, there are two columns for 'Source' and 'Destination'. Each column has radio buttons for 'Any' (selected), 'Host', and 'IPv6'. There are text input fields for 'Prefix Length' and 'Time Range' (set to '32 chars'). At the bottom, there are radio buttons for 'Action': 'Permit' (selected) and 'Deny'. 'Back' and 'Next' buttons are at the bottom right.

Figure 8-9 ACL Configuration Wizard (Configuration of Standard IPv6 ACL)

If you choose **Update an Extended IPv6 ACL** or **Create an IPv6 ACL**, the following window is displayed.

The screenshot shows the 'ACL Configuration Wizard' window. The title bar reads 'ACL Configuration Wizard'. Below the title bar, the progress bar shows 'Access-List Assignment >> Select Packet Type >> Apply Port'. The main area is titled 'Please assign a sequence number to create a new rule.' and has two radio buttons: 'Sequence No. (1-65535)' (selected) and 'Auto Assign'. Below this is the 'Assign Rule Criteria' section. It has five tabs: 'IPv6 Address', 'Port', 'IPv6 DSCP', 'TCP Flag', and 'Flow Label'. The 'IPv6 Address' tab is selected. Under this tab, there are two columns for 'Source' and 'Destination'. Each column has radio buttons for 'Any' (selected), 'Host', and 'IPv6'. There are text input fields for 'Prefix Length' and 'Time Range' (set to '32 chars'). Below this, there are sections for 'Port', 'IPv6 DSCP', 'TCP Flag', and 'Flow Label'. Each section has radio buttons and text input fields. At the bottom, there are radio buttons for 'Action': 'Permit' (selected) and 'Deny'. 'Back' and 'Next' buttons are at the bottom right.

Figure 8-10 ACL Configuration Wizard (Configuration of an Extended IPv6 ACL)

You can configure the following parameters.

Parameter	Overview
Sequence Number	Enter the ACL rule number. The range is from 1 to 65,535. If you choose Auto Allocation , the ACL rule-number regarding this entry is automatically generated.

Parameter	Overview
Protocol Type	<p>Choose the protocol type option. The options available are TCP, UDP, ICMP, Protocol ID, ESP (50), PCP (108), SCTP (132) and None.</p> <ul style="list-style-type: none"> • Value - You can enter the protocol ID, manually. The range is from 0 to 255. • Mask - After choosing the Protocol ID option, enter the value of the protocol mask, manually. The range is from 0x0 to 0xFF. • Fragment - If you choose this option, the packet fragment filtering is included.
Source	<p>Choose and enter the source information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates the optional source traffic according to this rule condition. • Host - Uses and enters a source host IPv6 address. • IPv6 - Enter the source IPv6 address and the value of Prefix-length in the entry field displayed.
Destination	<p>Choose and enter the destination information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates the optional destination traffic according to this rule condition. • Host - Uses and enters an IPv6 address of a destination host. • IPv6 - Enter the destination IPv6 address and the value of Prefix-length in the entry field displayed.
Source Port	<p>Choose and enter the value of the source port. The options available are as follows.</p> <ul style="list-style-type: none"> • = - ACL uses the port-number specified, only. • > - ACL uses all the ports, which are greater than the port-number specified. • < - ACL uses all the ports, which are smaller than the port-number specified. • ≠ - ACL uses all the ports except the port-number specified. • Range - ACL uses the specified port within the range. • Mask - ACL uses the port within the range of the mask specified. Enter the value of a port-mask in the entry field displayed. The range is from 0x0 to 0xFFFF. <p>This parameter is available when you select TCP or UDP as the protocol type.</p>

Parameter	Overview
Destination	<p>Choose and enter the value of the destination port. The options available are as follows.</p> <ul style="list-style-type: none"> • = - ACL uses the port-number specified, only. • > - ACL uses all the ports, which are greater than the port-number specified. • < - ACL uses all the ports, which are smaller than the port-number specified. • ≠ - ACL uses all the ports except the port-number specified. • Range - ACL uses the port, which is specified within the range. • Mask - ACL uses the port within the range of the mask specified. Enter the value of a port-mask in the entry field displayed. The range is from 0x0 to 0xFFFF. This parameter is available when you select TCP or UDP as the protocol type.
Specify ICMP Message Type	Choose the ICMP Message Type you use. This parameter is available when you select ICMP as the protocol type.
ICMP Message Type	If you do not choose the Specify ICMP Message type, enter the numerical value of an ICMP Message Type . The range is from 0 to 255. If you choose the ICMP Message Type , the numerical value of the message type is automatically entered. This parameter is available when you select ICMP as the protocol type.
Message Code	If you do not choose the Specify ICMP Message type, enter the numerical value of a message code to use. The range is from 0 to 255. If you choose the ICMP Message Type , the numerical value of the message type is automatically entered. This parameter is available when you select ICMP as the protocol type.
DSCP	<p>Choose the DSCP value you use. The options available are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46).</p> <ul style="list-style-type: none"> • Value - You can enter the DSCP value, manually. The range is from 0 to 63. • Mask - Enter the value of DSCP mask. The range is from 0x0 to 0x3F.
Traffic Class	<p>Choose and enter the value of a traffic class. The range is from 0 to 255.</p> <ul style="list-style-type: none"> • Mask - Enters the value of a traffic-class mask. The range is from 0x0 to 0xFF.

Parameter	Overview
TCP Flag	Choose the TCP flag to evaluate for this ACL. The options available are ack , fin , psh , rst , syn and urg . This parameter is available only if you choose TCP from the Protocol Type .
Flow Label	Enter the value of a flow label. The range is from 0 to 1,048,575. <ul style="list-style-type: none">• Mask - Enter the flow label mask. The range is from 0x0 to 0xFFFFF.
Time Range	Enter the name of the time range profile used in this ACL rule. The number of characters for the name can be up to 32.
Action	Choose an action to execute with this rule. The options available are Permit and Deny .

Click **Next** to proceed to the next step in the wizard.

Click **Back** to return to the previous step in the wizard.

After you click **Next** (in the previous step), the following window is displayed.

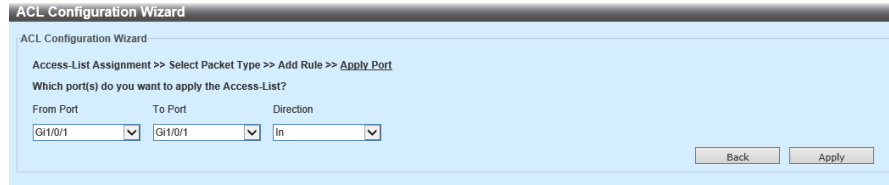


Figure 8-11 ACL Configuration Wizard (IPv6, Step 3)

You can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Direction	Choose a direction. The options available are In and Out .

Click **Apply** to check the content changed and return to the **ACL Configuration Wizard** window.

Click **Next** to return to the previous step in the wizard.

8.2 ACL Access List

Use the following window to implement the settings on ACL and ACL rules and to display their settings.

Choose **ACL > ACL Access List** to display the following window.

Figure 8-12 ACL Access List

In the section of **ACL Access List**, you can configure the following parameters.

Parameter	Overview
ACL Type	Choose an ACL type to search. The options available are All , IP ACL , IPv6 ACL , MAC ACL and Expert ACL .
ID	Choose and enter an access list ID whose range is from 1 to 14,999.
ACL Name	Choose and enter the name of an access list. The number of characters for the name can be up to 32.

Click **Find** to search and display the entries based on the search condition specified.

Click **Add ACL** to add a new ACL profile entry.

Click **Edit** to edit the configuration of the entry specified.

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

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

Click **Clear a Counter** to clear the counter information, which is related to an ACL profile selected.

Click **Add Rules** to add a new ACL rule entry on the ACL profile selected.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Edit** to display the following window.

ACL Access List

ACL Type: All (dropdown) | ID(1-14999) (radio button) | ACL Name (radio button) | 32 chars (text box) | Find (button)

Total Entries: 1 | Add ACL (button)

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark
1999	std_ip_acl	Standard IP ACL	10	10	Disabled (dropdown)	

1/1 | 1 | Go (button)

Clear All Counter (button) | Clear Counter (button) | Add Rule (button)

Sequence No.	Action	Rule	Time Range	Counter
--------------	--------	------	------------	---------

Figure 8-13 ACL Access List (Edit)

In the section of **ACL Access List**, you can configure the following parameters.

Parameter	Overview
Starting Sequence Number	Enter the starting sequence number.
Step	Enter the step of sequence numbers. The range of step is from 1 to 32. This specifies the number of steps for the sequence number. The default value is 10. For example, if the increment (step) value is 5 and the starting sequence number is 20, the following sequence numbers become 25, 30, 35 and 40.
Counter State	This parameter enables or disables the counter state option.
Annotation	Enter (or insert) an annotation for the option to associate with this ACL.

Click **Apply** to check the content changed.

8.2.1 Standard IP ACL

Click **Add ACL** (the **ACL Access List** window) to display the following window.

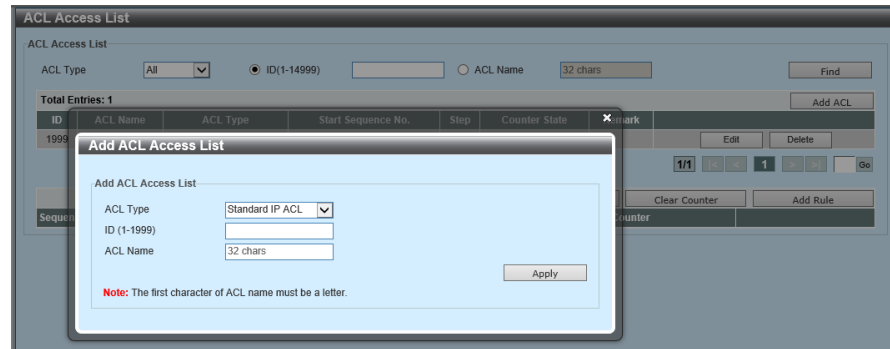


Figure 8-14 ACL Access List (Add ACL, standard IP ACL)

In the section of **Add an ACL Access-list**, you can configure the following parameters.

Parameter	Overview
ACL Type	Choose an ACL type to create. The options available are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL and Extended Expert ACL . This section describes how to configure the standard IP ACL.
ID	Enter an ID of the standard IP ACL. The range is from 1 to 1,999.
ACL Name	Enter the name of ACL. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL profile.

Choose the **Standard IP ACL** profile and then click the **Add Rules (ACL Access-list)** window to display the following window.

The screenshot shows the 'Add ACL Rule' configuration window. The fields are as follows:

- ID:** 1
- ACL Name:** std
- ACL Type:** Standard IP ACL
- Sequence No. (1-65535):** (If it isn't specified, the system automatically assigns.)
- Action:** ☒ Permit ☐ Deny
- Match IP Address:**
 - Source:** ☒ Any, ☐ Host, ☐ IP, ☐ Wildcard
 - Destination:** ☒ Any, ☐ Host, ☐ IP, ☐ Wildcard
- Time Range:** 32 chars
- Buttons:** Back, Apply

Figure 8-15 ACL Access List (Add Rules, a standard IP ACL)

In the section of **Adding ACL Rules**, you can configure the following parameters.

Parameter	Overview
Sequence Number	Enter the ACL rule number. The range is from 1 to 65,535. If you do not specify the number, it is automatically generated.
Action	Choose an action to execute with this rule. The options available are Permit and Deny .
Source	Choose and enter the source information. The options available are as follows. <ul style="list-style-type: none"> • Optional - Evaluates the optional source traffic according to this rule condition. • Host - Uses and enters a source host IP address. • IP - Uses and enters a group of source IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value of 1 is ignored, but the bit corresponding to the bit value of 0 is checked.
Destination	Choose and enter the destination information. The options available are as follows. <ul style="list-style-type: none"> • Optional - Evaluates the optional destination traffic according to this rule condition. • Host - Uses and enters an IP address of the destination host. • IP - Uses and enters a group of a destination IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value of 1 is ignored. The bit corresponding to the bit value of 0 is checked.
Time Range	Enter the name of the time-range profile to be used in this ACL rule. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL rule.

Click **Back** to return to the ACL access list window.

8.2.2 Extended IP ACL

Click **Add ACL** (in the **ACL Access List** window) to display the following window.

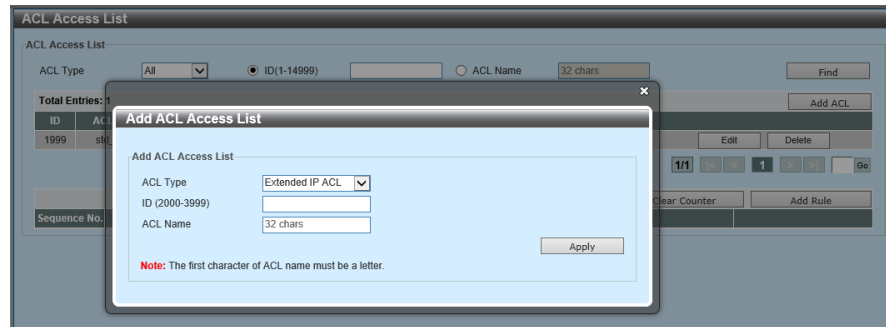


Figure 8-16 ACL Access List (Add ACL, Extended IP ACL)

In the section of **Add ACL Access List**, you can configure the following parameters.

Parameter	Overview
ACL Type	Choose the ACL type to create. The options available are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL and Extended Expert ACL . This section describes how to configure Extended IP ACL .
ID	Enter an ID of the extended IP ACL. The range is from 2,000 to 3,999.
ACL Name	Enter the name of ACL. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL profile.

Choose the **Extended IP ACL** profile, and then click **Add Rules (ACL Access List window)** to display the following window.

Figure 8-17 ACL Access List (Add Rules, Extended IP ACL)

In the section of **Adding ACL Rules**, you can configure the following parameters.

Parameter	Overview
Sequence Number	Enter the ACL rule number. The range is from 1 to 65,535. The number is automatically generated if you do not specify it.
Action	Choose an action to execute with this rule. The options available are Permit and Reject .
Protocol Type	<p>Choose a protocol type option. The options available are TCP, UDP, ICMP, EIGRP (88), ESP (50), GRE (47), IGMP (2), OSPF (89), PIM (103), VRRP (112), IP-in-IP (94), PCP (108), Protocol ID and None.</p> <ul style="list-style-type: none"> Value - Enter the protocol ID, manually. The range is from 0 to 255. Mask - If you choose the Protocol IDs option, enter the protocol-mask value, manually. The range is from 0x0 to 0xFF. Fragment - If you choose this option, the packet fragment filtering is included.

Parameter	Overview
Source	<p>Choose and enter the source information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates the optional source traffic according to this rule condition. • Host - Uses and enters a source host IP address. • IP - Uses and enters a group of source IP addresses using the Wildcard bitmap. The bit corresponding to the bit value 1 is ignored, but the bit corresponding to 0 as the bit value is checked.
Destination	<p>Choose and enter the destination information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates the optional destination traffic according to this rule condition. • Host - Uses and enters a destination host IP address. • IP - Uses and enters a group of destination IP addresses using the Wildcard bitmap. • The bit corresponding to 1 as the bit value is ignored, • but the bit corresponding to 0 as the bit value is checked.
Source Port	<p>Choose and enter the value of source port. The options available are as follows.</p> <ul style="list-style-type: none"> • = - ACL uses the port-number specified, only. • > - ACL uses all the ports, which are greater than the port-number specified. • < - ACL uses all the ports, which are smaller than the port-number specified. • ≠ - ACL uses all the ports except the port-number specified. • Range - ACL uses the port, which is specified within the range. • Mask - ACL uses the port within the range of the mask specified. Enter the value of a port-mask in the entry field displayed. The range is from 0x0 to 0xFFFF. <p>This parameter is available when you select TCP or UDP from the Protocol Type.</p>

Parameter	Overview
Destination Ports	<p>Choose and enter the value of a destination port. The options available are as follows.</p> <ul style="list-style-type: none"> • = - ACL uses the port-number specified, only. • > - ACL uses all the ports, which are greater than the port-number specified. • < - ACL uses all the ports, which are smaller than the port-number specified. • ≠ - ACL uses all the ports except for the port-number specified. • Range - ACL uses the port, which is specified within the range. • Mask - ACL uses the port within the range of the mask specified. Enter the value of a port-mask in the entry field displayed. The range is from 0x0 to 0xFFFF. • This parameter is available when you select TCP or UDP from the Protocol Type.
TCP Flag	<p>Choose a TCP flag, which is evaluated in this ACL. The options available are ack, fin, psh, rst, syn and urg. This parameter is available when you select TCP from the Protocol Type.</p>
Specify ICMP Message Type	<p>Choose an ICMP Message Type to use. This parameter is available when you select ICMP from the Protocol Type.</p>
ICMP Message Type	<p>If you do not choose Specify ICMP Message Type, enter the numerical value of an ICMP Message Type to use. The range is from 0 to 255. If you choose the ICMP Message Type, the numerical value of the message type is automatically entered. This parameter is available when you select ICMP from the Protocol Type.</p>
Message Code	<p>If you do not choose Specify ICMP Message Type, enter the numerical value of a message code to use. The range is from 0 to 255. If you choose the ICMP Message Type, the numerical value of the message type is automatically entered. This parameter is available when you select ICMP from the Protocol Type.</p>
IP Precedence	<p>Choose the value of IP precedence to use. The options available are routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6) and network (7).</p> <ul style="list-style-type: none"> • Value - You can enter the value of IP precedence, manually. The range is from 0 to 7. • Mask - Enter the value of IP precedence mask. The range is from 0x0 to 0x7.

Parameter	Overview
ToS	<p>Choose the value of Type-of-Service (ToS) to use. The options available are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4) and min-delay (8).</p> <ul style="list-style-type: none"> • Value - You can enter the ToS value, manually. The range is from 0 to 15. • Mask - Enter the value of ToS mask. The range is from 0x0 to 0xF.
DSCP	<p>Choose the DSCP value to use. The options available are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56) and ef (46).</p> <ul style="list-style-type: none"> • Value - You can enter the DSCP value, manually. The range is from 0 to 63. • Mask - Enter the value of DSCP mask. The range is from 0x0 to 0x3F.
Time Range	<p>Enter the name of the time-range profile to use in this ACL rule. The number of characters for the name can be up to 32.</p>

Click **Apply** to add a new ACL rule.

Click **Back** to return to the ACL access list window.

8.2.3 Standard IPv6 ACL

Click **Add ACL** (ACL Access window) to display the following window.

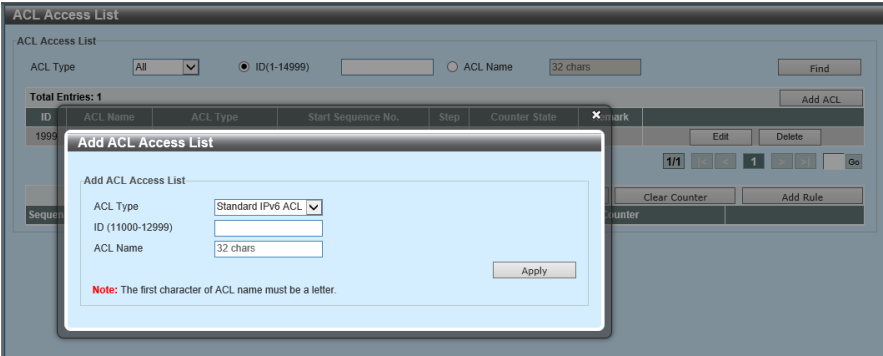


Figure 8-18 ACL Access List (Adding ACL/Standard IPv6 ACL)

In the section of **Add ACL Access List**, you can configure the following parameters.

Parameter	Overview
ACL Type	Choose the ACL type to create. The options available are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL and Extended Expert ACL . This section describes how to implement the settings on the standard IPv6 ACL
ID	Enter one ID of the standard IPv6 ACL. The range is from 11,000 to 12,999.
ACL Name	Enter the name of ACL. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL profile.

Choose the **standard IPv6 ACL** profile, and then click **Add Rules (ACL Access List Window)** to display the following window.

Add ACL Rule

Add ACL Rule

ID11000

ACL Namestdv6

ACL TypeStandard IPv6 ACL

Sequence No. (1-65535)(If it isn't specified, the system automatically assigns.)

Action

☒ Permit

☐ Deny

Match IPv6 Address

☒ Any

☐ Host

Source

2012:1

2012:1

Prefix Length

☒ Any

☐ Host

Destination

2012:1

2012:1

Prefix Length

Time Range

32 chars

Back

Apply

Figure 8-19 ACL Access List (Adding Rules, Standard IPv6 ACL)v

In the section of **Add ACL Rule**, you can configure the following parameters.

Parameter	Overview
Sequence Number	Enter an ACL rule-number. The range is from 1 to 65,535. If you do not specify the number, it is automatically generated.
Action	Choose an action to execute with this rule. The options available are Permit and Reject .
Source	Choose and enter the source information. The options available are as follows. <ul style="list-style-type: none">• Optional - Evaluates the optional source traffic according to this rule condition.• Host - Uses and enters a source host IPv6 address.• IPv6 - Enter the value of a source IPv6 address and prefix-length in the entry field displayed.
Destination	Choose and enter the destination information. The options available are as follows. <ul style="list-style-type: none">• Optional - Evaluates the optional destination traffic according to this rule condition.• Host - Uses and enters an IPv6 address of the destination host.• IPv6 - Enter the value of a destination IPv6 address and prefix-length in the entry field displayed.
Time Range	Enter the name of the time-range profile to use in this ACL rule. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL rule.

Click **Back** to return to the **ACL Access List** window.

8.2.4 Extended IPv6 ACL

Click **Add ACL** (**ACL Access List** window) to display the following window.

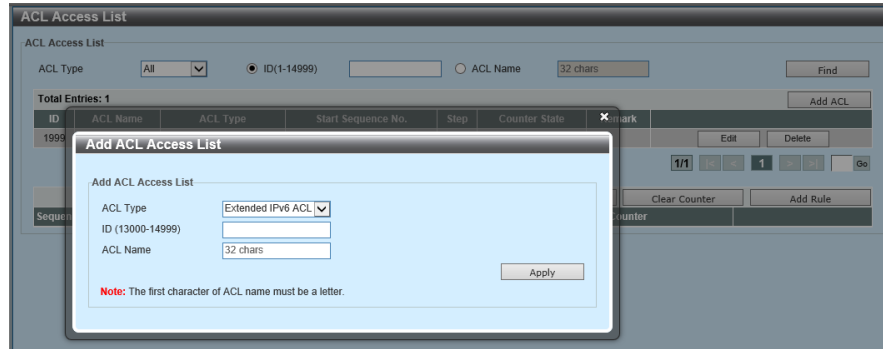


Figure 8-20 ACL Access List (Add ACL, Extended IPv6 ACL)

In the section of **Add an ACL Access List**, you can configure the following parameters.

Parameter	Overview
ACL Type	Choose the ACL type to create. The options available are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL and extended Expert ACL . This section describes how to configure Extended IPv6 ACL .
ID	Enter the ID of the extended IPv6 ACL. The range is from 13,000 to 14,999.
ACL Name	Enter the name of ACL. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL profile.

Choose the **Extended IPv6 ACL** profile and then click **Add Rule** (in the **ACL Access List** window) to display the following window.

The screenshot shows the 'Add ACL Rule' configuration window. The 'ID' is 14999, 'ACL Name' is 'ext_ipv6_acl', and 'ACL Type' is 'Extended IPv6 ACL'. The 'Sequence No.' is 1-65535. The 'Action' is 'Permit'. The 'Protocol Type' is 'TCP'. The 'Match IPv6 Address' section has 'Source' and 'Destination' both set to 'Any'. The 'Match Port' section has 'Source' and 'Destination' both set to 'Please Select'. The 'TCP Flag' section has 'ack', 'fin', 'psh', 'rst', 'syn', and 'urg' all unchecked. The 'DSCP/Traffic Class' section has 'DSCP (0-63)' selected. The 'Flow Label' section has 'Flow Label (0-1048575)' selected. The 'Time Range' section has '32 chars' selected. The 'Back' and 'Apply' buttons are at the bottom right.

Figure 8-21 ACL Access List (Add Rule, Extended IPv6 ACL)

In the section of **Add ACL Rule**, you can configure the following parameters.

Parameter	Overview
Sequence Number	Enter the ACL rule number. The range is from 1 to 65,535. This number is automatically generated if not specified.
Action	Choose an action to execute with this rule. The options available are Permit and Reject .
Protocol Type	<p>Choose the protocol type option. The options available are TCP, UDP, ICMP, Protocol ID, ESP (50), PCP (108), SCTP (132) and None.</p> <ul style="list-style-type: none"> Value - The protocol ID can also manually be entered. The range is from 0 to 255. Mask - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. Fragments - Select this option and then the packet fragment filtering is included.

Parameter	Overview
Source	<p>Choose and enter the source information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates an optional source traffics based on this rule condition. • Host - Use and enter an IPv6 address of the source host. • IPv6 - Specifies and enter the source IPv6 address and Prefix Length value in the spaces provided.
Destination	<p>Choose and enter the destination information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Specifies that any destination traffic is evaluated according to the conditions of this rule. • Host - Specifies and enters the destination host IPv6 address. • IPv6 - Specifies and enter the destination IPv6 address and prefix-length value in the spaces provided.
Source Port	<p>Choose and enter the source-port value. The options available are as follows.</p> <ul style="list-style-type: none"> • = - The ACL uses the port-number specified. • > - The ACL uses all the ports, which are greater than the port number specified. • < - The ACL uses all the ports, which are smaller than the port number specified. • ≠ - The ACL uses all the ports except for the port-number. • Range - The ACL uses the ports specified, within the range. • Mask - The ACL uses the ports, within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. • This parameter is available when you select TCP or UDP as the protocol type.

Parameter	Overview
Destination Port	<p>Choose and enter the destination-port value. The options available are as follows.</p> <ul style="list-style-type: none"> • = - The ACL uses the port-number specified. • > - The ACL uses all the ports, which are greater than the port number specified. • < - The ACL uses all the ports, which are smaller than the port number specified. • ≠ - The ACL uses all the ports except for the port-number. • Range - The ACL uses the ports specified, within the range. • Mask - The ACL uses the ports, within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. • This parameter is available when you select TCP or UDP as the protocol type.
TCP Flag	<p>Select the TCP flag, which is evaluated in this ACL. The options available are ack, fin, psh, rst, syn and urg. This parameter is available when you select TCP as the protocol type.</p>
Specify ICMP Message Type	<p>Choose the ICMP Message Type to use. This parameter is available when you select ICMP as the protocol type.</p>
ICMP Message Type	<p>When the ICMP Message Type is not specified, enter the ICMP message type numerical-value used here. The range is from 0 to 255. When you select the ICMP Message Type, this numerical value is automatically entered. This parameter is available when you select ICMP as the protocol type.</p>
Message Code	<p>When the ICMP Message Type is not selected, enter the message code numerical-value (to use). The range is from 0 to 255. When you select the ICMP Message Type, the value is automatically entered. This parameter is available when you select ICMP as the protocol type.</p>

Parameter	Overview
DSCP	<p>Choose the DSCP value. The options available are: default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56) and ef (46).</p> <ul style="list-style-type: none"> • Value - The DSCP value can be manually entered. The range is from 0 to 63. • Mask - Enter the DSCP mask value. The range is from 0x0 to 0x3F.
Traffic Class	<p>Choose and enter the traffic class value. The range is from 0 to 255.</p> <ul style="list-style-type: none"> • Mask - Enter the value of traffic class mask. The range is from 0x0 to 0xFF.
Flow Label	<p>Enter the flow label value. The range is from 0 to 1,048,575.</p> <ul style="list-style-type: none"> • Mask - Enter the flow label mask. The range is from 0x0 to 0xFFFFF.
Time Range	<p>Enter the name of the time range profile to use in this ACL rule. The number of characters for the name can be up to 32.</p>

Click **Apply** to add a new ACL rule.

Click **Back** to return to the **ACL Access List** window.

8.2.5 Extended MAC ACL

Click **Add ACL** (the **ACL Access List** window) to display the following window.

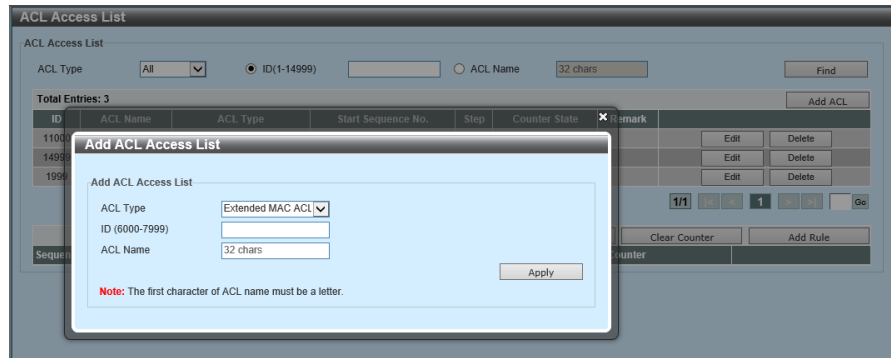


Figure 8-22 ACL Access List (Adding ACL, Extended MAC ACL)

In the section of **Add ACL Access List**, you can configure the following parameters.

Parameter	Overview
ACL Type	Choose the ACL type to create. The options available are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL and Extended Expert ACL . This section describes how to configure Extended MAC ACL .
ID	Enter an ID of extended MAC ACL. The range is from 6 to 7,999.
ACL Name	Enter the name of ACL. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL profile.

Click **Extended MAC ACL** profile and **Add Rules** (in the **ACL Access List** window) to display the following window.

Figure 8-23 ACL Access List (Adding Rules, Extended MAC ACL)

In the section of **Add ACL Rules**, you can configure the following parameters.

Parameter	Overview
Sequence Number	Enter the ACL rule number. The range is from 1 to 65,535. If not specified, this number is automatically generated.
Action	Choose an action to execute with this rule. The options available are Permit and Reject .
Source	Choose and enter the information on a source MAC address. The options available are as follows. <ul style="list-style-type: none"> Optional - Evaluates the optional source traffic according to this rule condition. Host - Enter a source-host MAC address. MAC - Enter the source MAC address and the Wildcard value in the entry fields provided
Destination	Choose and enter the destination MAC address information. The options available are as follows. <ul style="list-style-type: none"> Optional - Evaluates the optional destination traffic according to this rule condition. Host - Enter a destination host MAC address. MAC - Enter a destination MAC address and the Wildcard value in the entry field displayed.
Specify Ethernet Type	Choose the Ethernet type option. The options available are aarp , appletalk , decent-iv , etype-6000 , etype-8042 , lat , lavc-sca , mop-console , mop-dump , vines-echo , vines-ip , xns-idp and arp .

Parameter	Overview
Ethernet Type	Enter the Ethernet type as the hexadecimal value. The range is from 0x600 to 0xFFFF. If you choose the optional Ethernet type profile from the drop-down list of Specify Ethernet Type , the appropriate hexadecimal-value is automatically displayed.
Ethernet Type Mask	Enter the Ethernet type mask as the hexadecimal value. The range is from 0x0 to 0xFFFF. If you choose an optional Ethernet type profile from the drop-down list of Specify Ethernet Type , the appropriate hexadecimal-value is automatically displayed.
CoS	Choose the CoS-value; the range is from 0 to 7. <ul style="list-style-type: none">• Mask - Enter the value of CoS mask. The range is from 0x0 to 0x7.
VID	Enter one VLAN ID to use. The range is from 1 to 4,094. <ul style="list-style-type: none">• Mask - Enter the value of VLAN ID mask. The range is from 0x0 to 0xFFF.
Time Range	Enter the name of the time range profile to use in this ACL rule. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL rule.

Click **Back** to return to the ACL access list window.

8.2.6 Extended Expert ACL

Click **Add ACL** (in the **ACL Access List** window) to display the following window.

The screenshot shows the 'Add ACL Rule' window with the following fields and options:

- ID:** 6000
- ACL Name:** exmac
- ACL Type:** Extended MAC ACL
- Sequence No. (1-65535):** (If it isn't specified, the system automatically assigns.)
- Action:** ☒ Permit ☐ Deny
- 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)
- Match Ethernet Type:**
 - Specify Ethernet Type:** Please Select
 - Ethernet Type (0x0-0xFFFF):**
 - Ethernet Type Mask (0x0-0xFFFF):**
- VID (1-4094):**
- Mask (0x0-0xFFF):**
- CoS:** Please Select
- Mask (0x0-0x7):**
- Time Range:** 32 chars
- Buttons:** Back, Apply

Figure 8-24 ACL Access List (Add ACL, Extended Expert ACL)

In the section of **Add ACL Access List**, you can configure the following parameters.

Parameter	Overview
ACL Type	Choose the ACL type to create. The options available are Standard IP ACL , ExtendedIP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL and Extended Expert ACL . This section describes how to configure Extended Expert ACL .
ID	Enter an ID of the Extended Expert ACL. The range is from 8,000 to 9,999.
ACL Name	Enter the name of ACL. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL profile.

Choose the **Extended Expert ACL** profile and click **Add Rules (ACL Access List window)** to display the following window.

The screenshot shows the 'Add ACL Rule' window for Extended Expert ACL. The fields are as follows:

- ID:** 8000
- ACL Name:** extex
- ACL Type:** Extended Expert ACL
- Sequence No. (1-65535):** (If it isn't specified, the system automatically assigns.)
- Action:** ☒ Permit ☐ Deny
- Protocol Type:** TCP (0-255) Mask (0x0-0xFF) 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
- Match Port:**
 - Source:** Please Select (0-65535)
 - Destination:** Please Select (0-65535)
- TCP Flag:** ☐ ack ☐ fin ☐ psh ☐ rst ☐ syn ☐ urg
- IP Precedence:** ☒ IP Precedence ☐ ToS ☐ DSCP (0-63)
- Value (0-7):** Please Select (0-7) Mask (0x0-0x7)
- Value (0-15):** Please Select (0-15) Mask (0x0-0xF)
- Value (0-63):** Please Select (0-63) Mask (0x0-0x3F)
- VID (1-4094):** Please Select Mask (0x0-0xFFF)
- CoS:** Please Select Mask (0x0-0x7)
- Time Range:** 32 chars

Figure 8-25 ACL Access List (Add Rules, Extended Expert ACL)

In the section of **Add ACL Rules**, you can configure the following parameters.

Parameter	Overview
Sequence Number	Enter the ACL rule number. The range is from 1 to 65,535. If not specified, the number is automatically generated.
Action	Choose an action to execute with this rule. The options available are Permit and Reject .

Parameter	Overview
Protocol Type	<p>Choose the protocol type option. The options available are TCP, UDP, ICMP, EIGRP (88), ESP (50), GRE (47), IGMP (2), OSPF (89), PIM (103), VRRP (112), IP-in-IP (94), PCP (108), Protocol ID and None.</p> <ul style="list-style-type: none"> • Value - You can manually enter the protocol ID whose range is from 0 to 255. • Mask - After you choose the protocol ID option, enter the value of protocol mask, manually. • The range is from 0x0 to 0xFF. • Fragment - If you choose this, a packet fragment filtering is included.
Source (IP Address)	<p>Choose and enter the source information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates the optional source traffic according to this rule condition. • Host - Uses and enters a source host IP Address. • IP - Use the bit map of Wildcard and enter a group of the source IP address. The bit corresponding with 1 of the bit value is ignored, but the bit corresponding to 0 as the bit value is checked.
Destination (IP Address)	<p>Choose and enter the destination information. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates the optional destination traffic according to this rule condition. • Host - Uses and enters a destination host IP Address. • IP - Use the bit map of Wildcard and enter the group of the destination IP address. The bit corresponding with 1 of the bit value is ignored, but the bit corresponding to 0 as the bit value is checked.
Source (MAC Address)	<p>Choose and enter the information on a source MAC address. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates the optional source traffic according to this rule condition. • Host - Enter a source-host MAC address. • MAC - Enter a source MAC address and the Wildcard value in the entry field displayed.
Destination (MAC Address)	<p>Choose and enter the information on a destination MAC address. The options available are as follows.</p> <ul style="list-style-type: none"> • Optional - Evaluates the optional destination traffic according to this rule condition. • Host - Enter a destination-host MAC address. • MAC - Enter a destination MAC address and the Wildcard value in the entry field displayed.

Parameter	Overview
Source Port	<p>Choose and enter the source-port value. The options available are as follows.</p> <ul style="list-style-type: none"> • = - ACL uses the port-number specified, only. • > - ACL uses all the ports, which are greater than the port-number specified. • < - ACL uses all the ports, which are smaller than the port-number specified. • ≠ - ACL uses all the ports except for the port-number specified. • Range - ACL uses the port, which is specified within the range. • Mask - ACL uses the port within the range of the mask specified. Enter the value of a port-mask in the entry field displayed. The range is from 0x0 to 0xFFFF. <p>This parameter is available when you select TCP or UDP from the Protocol Type.</p>
Destination Port	<p>Choose and enter the value of a destination port. The options available are as follows.</p> <ul style="list-style-type: none"> • = - ACL uses the port number specified, only. • > - ACL uses all the ports, which are greater than the port-number specified. • < - ACL uses all the ports, which are smaller than the port-number specified. • ≠ - ACL uses all the ports except for the port-number specified. • Range - ACL uses the port, which is specified within the range. • Mask - ACL uses the port within the range of the mask specified. Enter the value of a port-mask in the entry field displayed. The range is from 0x0 to 0xFFFF. <p>This parameter is available when you select TCP or UDP from the Protocol Type.</p>
Specify ICMP Message Type	<p>Choose the ICMP Message Type to use. This parameter is available when you select ICMP from the Protocol Type.</p>
ICMP Message Type	<p>If you do not choose the Specify ICMP Message Type, enter the numerical value of the ICMP message type to use. The range is from 0 to 255. If you choose the ICMP Message Type, the numerical value of message type is automatically entered. This parameter is available when you select ICMP from the Protocol Type.</p>

Parameter	Overview
Message Code	If you do not choose the Specify ICMP Message Type , enter the numerical value of message code to use. The range is from 0 to 255. If you choose the ICMP Message Type , the numerical value of a message type is automatically entered. This parameter is available when you select ICMP from the Protocol Type .
IP Precedence	Choose the value of IP Precedence to use. The options available are routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6) and network (7). <ul style="list-style-type: none"> • Value - You can enter the value of IP Precedence, manually. The range is from 0 to 7. • Mask - Enter the value of IP Precedence mask. The range is from 0x0 to 0x7.
ToS	Choose the value of Type-of-Service (ToS) to use. The options available are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4) and min-delay (8). <ul style="list-style-type: none"> • Value - You can enter the ToS value, manually. The range is from 0 to 15. • Mask - Enter the ToS mask value. The range is from 0x0 to 0xF.
DSCP	Choose the DSCP value to use. The options available are: default (0) af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56) and ef (46). <ul style="list-style-type: none"> • Value - You can enter the DSCP value, manually. The range is from 0 to 63. • Mask - Enter the DSCP mask value. The range is from 0x0 to 0x3F.
TCP Flag	Choose the TCP flag to evaluate for this ACL. The options available are ack , fin , psh , rst , syn , and urg . This parameter is available when you select TCP from the Protocol Type .
VID	Enter the VLAN ID you use. The range is from 1 to 4,094. <ul style="list-style-type: none"> • Mask - Enter the value of VLAN ID mask. The range is from 0x0 to 0xFFFF.
CoS Apply	Choose the CoS-value to use. The range is from 0 to 7. <ul style="list-style-type: none"> • Mask - Enter the CoS-mask value. The range is from 0x0 to 0x7.

Parameter	Overview
Time Range	Enter the name of the time range profile to use in this ACL rule. The number of characters for the name can be up to 32.

Click **Apply** to add a new ACL rule.

Click **Back** to return to the ACL access list window.

8.3 ACL Interface Access Group

Use the following window to implement the settings on an ACL access group of the port specified and display its settings.

Choose **ACL > ACL Interface Access Group** to display the following window.

Figure 8-26 ACL Interface Access Group

In the section of **ACL Interface Access Group**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Direction	Choose a direction. The options available are In and Out .
Action	Choose the action you perform. The options available are Add and Delete .
Type	Choose an ACL type. The options available are IP ACL , IPv6 ACL , MAC ACL and Expert ACL .
ACL Name	Enter the name of ACL. The number of characters for the name can be up to 32. Then click ACL Name to choose an existing ACL from a list.

Click **Apply** to check the content changed.

Click **Please Select** to display the access control list configured already and use it in this window.

Click **Please Select** to display the following window.

Port	In				Out			
	IP ACL	IPv6 ACL	MAC ACL	Expert ACL	IP ACL	IPv6 ACL	MAC ACL	Expert ACL
F11/0/1								
F11/0/2								
F11/0/3								
F11/0/4								
Te11/0/5								
Te11/0/6								

Figure 8-27 ACL Interface Access Group (Please select.)

Click **OK** to use the access-control list selected.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

8.4 ACL VLAN Access Map

Use the following window to implement the settings on an ACL VLAN access map and display its settings.

Choose **ACL > ACL VLAN Access Map** to display the following window.

ACL VLAN Access Map

ACL VLAN Access Map

Access Map Name 32 chars

Sub Map Number (1-65535)

Action Forward

Apply

Access Map Name 32 chars Counter State Disabled

Apply

Access Map Name 32 chars

Clear All Counter Clear Counter Find

Total Entries: 0

Access Map Name	Sub Map Number	Action	Match Access-List	Counter State
-----------------	----------------	--------	-------------------	---------------

Figure 8-28 ACL VLAN Access Map

In the section of **ACL VLAN Access Map**, you can configure the following parameters.

Parameter	Overview
Access Map Name	Enter the name of an access-map. The number of characters for the name can be up to 32.
Sub Map Number	Enter the sub map number. The range is from 1 to 65,535.
Action	Choose the action you perform. The options available are Forward , Drop and Redirect . If you choose the Redirect option, choose the redirect-destination interface from the drop-down list.
Counter State	This parameter enables or disables the counter state.

Click **Apply** to add a new entry.

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

Click **Clear Counters** to clear the counter information about the specified access map.

Click **Find** to search and display the entries based on the search condition specified.

Click the **Binding** button to configure the binding for the specified entry.

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

If two or more pages exist, enter the page-numbers. Then click **Go** to move to a specific page.

Click the **Binding** button to display the following window.

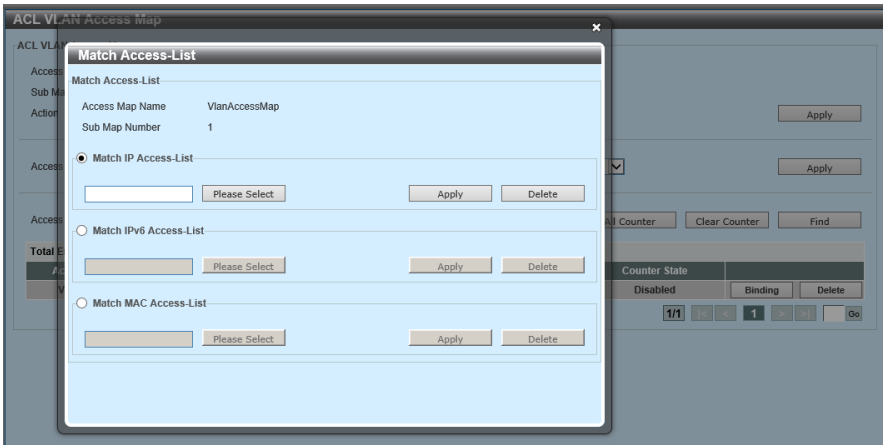


Figure 8-29 ACL VLAN Access Map (Binding)

In the section of **Match Access List**, you can configure the following parameters.

Parameter	Overview
Match IP Access-List	The IP access list (to be matched) is displayed.
Match IPv6 Access-List	The IPv6 access list (to be matched) is displayed.
Match MAC Access-List	The MAC access list (to be matched) is displayed.

Click **Please Select** to display the configured access-control list, which can be used in this window.

Click **Apply** to check the content changed.

Click **Delete** to delete the binding specified.

Click **Please Select** to display the following window.

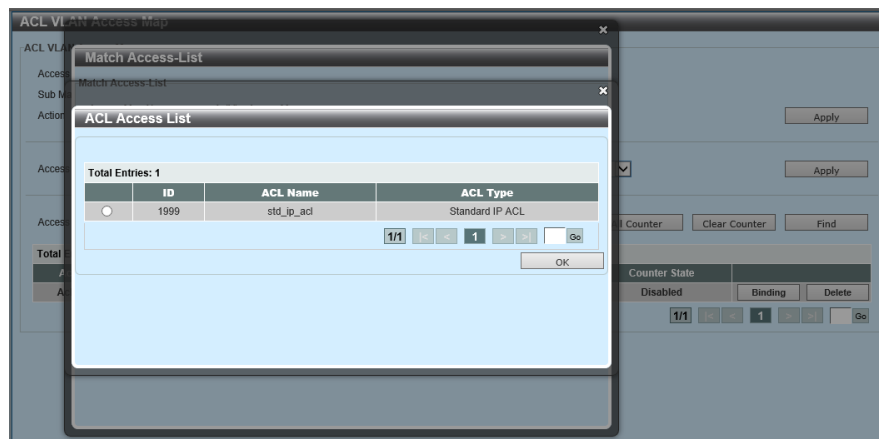


Figure 8-30 ACL VLAN Access Map (Please choose a binding.)

Click **OK** to use the access control list selected.

Click **Go** to move a specific page.

If two or more pages exist, enter the page-numbers. Then click **Go** to move to a specific page.

8.5 ACL VLAN Filter

Use the following window to implement the settings on the ACL VLAN filtering and display its settings.

Choose **ACL > ACL VLAN Filter** to display the following window.

Figure 8-31 ACL VLAN Filter

In the section of **ACL VLAN Filter**, you can configure the following parameters.

Parameter	Overview
Access Map Name	Enter the name of an access-map. The number of characters for the name can be up to 32.
Action	Choose the action you perform. The options available are Add and Delete .
VID List	Enter the VLAN ID you use. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094. If you choose All VLANs , this configuration is applied to all the VLANs, which are configured on this switch.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page-numbers. Then click **Go** to move to a specific page.

9 Security

9.1 Port Security

9.1.1 Port Security Global Settings

Use the following window to implement the settings on a global port security and display its settings.

Choose **Security > Port Security > Port Security Global Settings** to display the following window.

VID	Max Learning Address	Current No.
1	No Limit	0

Figure 9-1 Port Security Global Settings

In the section of **Port Security System Settings**, you can configure the following parameter.

Parameter	Overview
Maximum Address of a System	Enter the maximum number of secure MAC addresses to be allowed (or permitted). If not specified, the default value is No Restriction. The valid range is from 1 to 3,328. If you choose No Restriction , the maximum number of secure MAC addresses is permitted.

Click **Apply** to check the content changed.

In the section of **Port Security VLAN Settings**, you can configure the following parameters.

Parameter	Overview
VID list	Enter the VLAN ID you use. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.
VLAN Maximum Learning Address	Enter the maximum number of MAC addresses to be allowed (or permitted), which can be learned with the VLAN specified. The range is from 1 to 3,328. If you choose No Restriction , the maximum number of secure MAC addresses is allowed.

Click **Apply** to add new entries based on the information specified.

In the section of **Searching VLAN**, you can configure the following parameter.

Parameter	Overview
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Find** to search and display entries based on the search condition specified.

9.1.2 Port Security Port Settings

Use the following window to implement the port-security settings on the port specified and display its settings.

Choose **Security > Port Security > Port Security Port Settings** to display the following window.

Port	Maximum	Current No.	Violation Action	Violation Count	Security Mode	Admin State	Current State	Aging Time	Aging Type
Fi1/0/1	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Fi1/0/2	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Fi1/0/3	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Fi1/0/4	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Te1/0/5	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Te1/0/6	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute

Figure 9-2 Port Security Port Settings

In the section of **Port Security Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
State	This parameter enables or disables a port-security function on the port specified.
Maximum	Enter the maximum number of secure MAC addresses to permit on the port (s) specified. The range is from 0 to 3,328. By default, the value is set to 32.
Violation Action	Choose the violation action to conduct. The options available are as follows. <ul style="list-style-type: none"> • Protect - Although all the packets are deleted from the host, which is insecure as the port security process level, the security-violation count is not increased. • Restrict - All the packets coming from the host, which is insecure as the port-security-process level, are deleted. The security-violation count is increased to be recorded on the system log. • Shutdown - If a security-violation occurs, the port becomes shut down to be recorded on the system-log.

Parameter	Overview
Security Mode	Choose the security mode option. The options available are as follows. <ul style="list-style-type: none">• Permanent - All the MAC addresses learned are not cleared except for the cases which users manually deleted entries.• Delete-On-Timeout - All the learned MAC addresses become cleared if an entry ages out, or if the users manually delete these entries.
Aging Time	Enter the aging-time value to use it for the secure dynamic address, which automatically learned on the port specified. The range is from 0 to 1,440 (minutes).
Aging Type	Choose the aging type. The options available are as follows. <ul style="list-style-type: none">• Absolute - All the secure addresses on this port become age-out immediately if the specified time passes, and they are deleted from a list of the addresses. This is the default type.• Inactivity - The secure address on this port becomes age-out only if there are no data-traffics coming from the secure-source address, during the period specified.

Click **Apply** to check the content changed.

9.1.3 Port Security Address Entries

Use the following window to implement the settings on the MAC address entry of the port security and display its settings.

Choose **Security > Port Security > Port Security Address Entries** to display the following window.

Figure 9-3 Port Security Address Entries

In the section of **Port Security Address Entries**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
MAC Address	Enter a MAC address. If you choose the Permanent option, all the MAC addresses learned are not cleared except for the case that users delete an entry, manually.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.

Click **Add** to add new entries.

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

Click the **Clear by Port** button to delete all the secure MAC addresses for the port specified.

Click the **Clear by Mac** button to delete the address specified among the secure MAC addresses on the optional port.

Click **Clear All** to clear and delete all the secure MAC addresses for a port.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.2 802.1X

9.2.1 802.1X Global Settings

Use the following window to implement the settings on the global IEEE 802.1X and display its settings.

Choose **Security > 802.1X > 802.1X Global Settings** to display the following window.

Figure 9-4 802.1X Global Settings

In the section of **802.1X Global Settings**, you can configure the following parameters.

Parameter	Overview
System Authentication Control	This parameter enables or disables the system authentication control. This function controls the network access coming from unauthorized hosts.
NAS ID	Enter an ID regarding Network Access Server (NAS).
EAP Request Interval	Enter the request interval of the Extensible Authentication Protocol (EAP). The range is from 1 to 3,600 (seconds).

Click **Apply** to check the content changed.

In the section of **802.1X Authentication Port Settings**, you can configure the following parameters.

Parameter	Overview
Authentication Port Mode	Choose the authentication mode to use (it) on the port specified. The options available are Port Based and Mac-Based .
From Port/ To Port	Choose the port you use.

Click **Apply** to check the content changed.

9.2.2 802.1X Forced Authorized MAC Settings

Use the following window to implement the settings on IEEE 802.1X forced authorized MAC and display its settings.

Choose **Security > 802.1X > 802.1X Forced Authorized MAC Settings** to display the following window.

Figure 9-5 802.1X Forced Authorized MAC Settings

In the section of **Forced Authorized MAC Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
MAC Address	Enter a MAC address of supplicant.
Mask Length	Enter the MAC mask bit-length. The range is from 0 to 48.
Authentication Status	Choose the authentication status. The options available are as follows. <ul style="list-style-type: none"> • Authorized - Choose this option to force the authorized status. • Unauthorized - Choose this to force the unauthorized status.

Click **Apply** to add a new entry.

Click **Find** to search and display the entries based on the search condition specified.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.2.3 802.1X Unauthorized MAC Settings

Use the following window to implement the settings on IEEE 802.1X unauthorized MAC and display its settings.

Choose **Security > 802.1X > 802.1X Unauthorized MAC Settings** to display the following window.

Figure 9-6 802.1X Unauthorized MAC Settings

In the section of **Unauthorized MAC Address Settings**, you can configure the following parameters.

Parameter	Overview
Age-Out Time	Enter the value of age-out time. The time is used for aging out a static unauthorized host. The range is from 0 to 65,535 (seconds).
From Port/ To Port	Choose the port you use.
MAC Address	Enter a MAC address of an unauthorized host.
Find By MAC	Choose this option to find the configured dynamic host, which is unauthorized, and display in a sequential order of MAC addresses.
Find By Port	Choose this to find and display the configured dynamic host, which is unauthorized, on the port specified. • From Port / To Port - Choose the port you use.

Click **Apply** to check the content changed.

Click **Find** to search and display the entries based on the search condition specified.

9.2.4 802.1X Ports Settings

Use the following window to implement the settings on IEEE 802.1X port-based/MAC based access-control on the port specified and display its settings.

Choose **Security > 802.1X > 802.1X Ports Settings** to display the following window.

The screenshot shows the '802.1X Ports Settings' window with the 'Port-Based Access Control' tab selected. The 'Port-Based Authentication Ports' are listed as 'Fi1/0/1-1/0/4, Te1/0/5-1/0/6'. The configuration parameters are as follows:

Parameter	Value	Unit
From Port	Fi1/0/1	
To Port	Fi1/0/1	
Port Control	Force Authorized	
AdminControlDirection	Both	
Quiet Period (1-65535)	60	sec
Transmission Period (1-65535)	30	sec
Supplicant Timeout (1-65535)	30	sec
Server Timeout (1-65535)	30	sec
Re-authentication Period (1-65535)	3600	sec
Maximum Request (1-10)	2	
Per-Port Re-authentication	Disabled	
Re-authentication Time Local	Disabled	

Buttons at the bottom include 'Apply', 'Show', 'Init', and 'Re-authenticate'.

Figure 9-7 802.1X Ports Settings (Port-Based Access Control)

In the section of **Port Based Access Control**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Port Control	Choose an authentication state of a port. The options available are as follows. <ul style="list-style-type: none"> • Auto - Enables the IEEE 802.1X authentication. • Force Authorized - Sets a port to an authorized state, forcefully. • Force Unauthorized - Sets a port to the unauthorized state, forcefully.
Admin Control Direction	Choose the control direction of traffics on the port(s). The options available are as follows. <ul style="list-style-type: none"> • Both - Controls traffics in both directions. • In - Controls traffics in an inbound direction, only.
Quiet Period	Enter the quiet (or silent) period. This is the number of seconds needed, for a switch, to maintain the quiet state after failing an authentication process. The range is from 1 to 65,535 (seconds).
Transmission Period	Enter a transmission period. This is the number of seconds needed, for a switch, to wait for the EAP requests/identity-frames coming from supplicants. When passing the period, a request is retransmitted. The range is from 1 to 65,535 (seconds).

Parameter	Overview
Supplicant Time-out	Enter the value of a supplicant time-out. This is the number of seconds needed to wait for the response coming from the supplicant. If this period passes, the supplicant message becomes time-out. This is not applied to the EAP request ID. The range is from 1 to 65,535 (seconds).
Server Time-out	Enter the value of a server time-out. This is the number of seconds needed to wait for the response coming from an authentication server. When passing this period, the connection becomes time-out. The range is from 1 to 65,535 (seconds).
Re-authentication Period	Enter the re-authentication period. This is the number of seconds needed for an interval of re-authentication trials. The range is from 1 to 65,535 (seconds).
Maximum Request	Enter the maximum number of EAP requests that are allowed from a back-end authentication machine. When exceeding this, an authentication process restarts. The range is from 1 to 10.
Per-Port Re-authentication	This parameter enables or disables the regular re-authentication for the port specified.
Re-authentication Time Local	This parameter enables or disables usage for the local settings on the session re-authentication, which is done by a timer.

Click **Apply** to check the content changed.

Click **Show** to display the settings on the port-based access control, which is associated with the specified port(s).

Click **Init** to initiate the settings on the port-based access control on the specified port(s).

Click **Re-authenticate** to re-authenticate all the connections to the specified port(s).

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click the **MAC-Based Access Control** tab to display the following window.

The screenshot shows the '802.1X Ports Settings' window with the 'MAC-Based Access Control' tab selected. The 'MAC-Based Authentication Ports' section contains the following fields and values:

- From Port: F11/0/1
- To Port: F11/0/1
- Number of Supplicant (1-1024): 512
- AdminControlDirection: Both
- Quiet Period (1-65535): 60 sec
- Transmission Period (1-65535): 30 sec
- Supplicant Timeout (1-65535): 30 sec
- Server Timeout (1-65535): 30 sec
- Re-authentication Period (1-65535): 3600 sec
- Maximum Request (1-10): 2
- Re-authentication Time Local: Disabled
- Per-Port Re-authentication: Disabled
- Force Authentication Timeout (0-65535): 3600 sec

Buttons at the bottom include 'Apply', 'Show', 'Init', and 'Re-authenticate'.

Figure 9-8 802.1X Ports Settings (MAC-Based Access Control)

In the section of **MAC-Based Access Control**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Number of Supplicants	Enter the maximum number of authenticated users who are allowed on the port(s). The range is from 1 to 512.
Admin Control Direction	Choose the control direction of traffics on the port(s). The options available are as follows. <ul style="list-style-type: none"> • Both - controls traffics in both directions • In - controls traffics in Inbound direction, only.
Quiet Period	Enter the quiet period. This is the number of seconds, for a switch, to maintain the quiet state after failing an authentication process. The range is from 1 to 65,535 (seconds).
Transmission Period	Enter the transmission period. This is the number of seconds needed, for a switch, to wait for the EAP requests/identity-frames, which come from supplicants. When passing the period, requests are re-transmitted. The range is from 1 to 65,535 (seconds).
Supplicant Timeout	Enter the value of the supplicant timeout. This is the number of seconds needed to wait for the response coming from the supplicant. If this period passes, the supplicant message becomes time-out. This is not applied to EAP request ID. The range is from 1 to 65,535 (seconds).

Parameter	Overview
Server Time-out	Enter the value of the server time-out. This is the number of seconds needed to wait for the response coming from an authentication server. If this period passes, the connection becomes time-out. The range is from 1 to 65,535 (seconds).
Re-authentication Period	Enter the re-authentication period. This is the number of seconds for the interval of re-authentication attempts. The range is from 1 to 65,535 (seconds).
Maximum Request	Enter the maximum number of EAP requests, which are allowed from a back-end authentication machine. When exceeding this, an authentication process restarts. The range is from 1 to 10.
Re-authentication Time Local	This parameter enables or disables the use of the local settings for the session re-authentication done by a timer.
Per-Port Re-authentication	This parameter enables or disables the regular re-authentication on the port(s) specified.
Forced Authentication Timeout	Enter the value of the forced authentication timeout. This is the number of seconds for a switch to wait for the migration to forced authentication/un-authorization. If this period passes, the migration becomes time-out. The range is from 0 to 65,535 (seconds). To avoid that the migration becomes time-out, enter 0 for it.

Click **Apply** to check the content changed.

Click **Show** to display the settings on MAC-based access control, which is associated with the specified port(s).

Click **Init** to initiate the settings on Mac-based access control on the specified port(s).

Click **Re-authenticate** to re-authenticate all the connections to the specified port(s).

Click **Show Detail** to display details on the entry.

Click **Show Detail** to display the following window.

MAC-Based Port Information

NAS ID	nas1	Port Number	F11/0/2
Number of Supplicant	512	OperControlDirection	Both
AdminControlDirection	Both	Transmission Period	30
Maximum Request	2	Supplicant Timeout	30
Quiet Period	60	Server Timeout	30
Re-authentication Period	3600	Force Authentication Timeout	3600
Per-Port Re-authentication	Disabled	Re-authentication Timer Mode	RADIUS

Total Entries: 0

Supplicant MAC Address	Type	MAC Control	Authentication Status	Re-Authentication
------------------------	------	-------------	-----------------------	-------------------

Back

Figure 9-9 802.1X Ports Settings (MAC Based Access Control, Show Detail)

Click **Edit** to enable or disable the re-authentication function.

Click **Initiate** to initiate the settings on the MAC-based access control on the port specified.

Click **Re-authenticate** to re-authenticate the MAC address connections of the supplicant specified.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Back** to return to the previous window.

9.2.5 EAP Port Config

Use the following window to implement the EAP settings on the port specified and display its settings.

Choose **Security > 802.1X > EAP Port Config** to display the following window.

Figure 9-10 EAP Port Config

You can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
EAP Request	This parameter enables or disables the function of EAP requests on the port specified.
EAP Forward	This parameter enables or disables the function of EAP forward on the port specified. You can use it to enable or disable the forwarding of IEEE 802.1X Protocol Data Units (PDU).

Click **Apply** to check the content changed.

9.2.6 802.1X Authenticator Statistics Information

Use the following command to display and clear the statistics information about the IEEE 802.1X authentication of the port specified.

Choose **Security > 802.1X > 802.1X Authenticator Statistics Information** to display the following window.

Port	F11/0/1	Elapsed Time Since Reset	011:22:03:37
TxReqId	0		
TxReq	0		
TxTotal	0		
RxStart	0		
RxLogoff	0		
RxRespId	0		
RxResp	0		
RxInvalid	0		
RxLenError	0		
RxTotal	0		
RxVersion	0		
LastRxSrcMac	00-00-00-00-00-00		

Figure 9-11 802.1X Authentication Statistics Information

In the section of **Statistics**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
Since	Choose the time range. The options available are as follows. <ul style="list-style-type: none"> • Since-Reset - displays the statistics, which has been recorded since the last switch reset. • Since-Up - displays the statistics, which has been recorded since the last switch boot-up.

Click **Find** to display the information based on the search condition specified.

Click **Reset All** to reset all the statistics information.

9.2.7 802.1X Supplicant Global Settings

In the following screen, you can configure a user-name and a password to operate a switching hub as a supplicant. With the supplicant function of 802.1X, you can connect this device to the port, which configures the IEEE802.1X function (port-based authentication) on a upper switching-hub. Doing so enhances the security or countermeasure against unauthorized-accesses.

Choose **Security > 802.1X > 802.1X Supplicant Global Settings** to display the following window.

Figure 9-12 802.1X Supplicant Global Settings

In the section of **802.1X Supplicant Global Settings**, you can configure the following parameters.

Parameter	Overview
User-name	Configure a user-name of the supplicant.
Password	Configure a supplicant-password.
Encrypting Password	Use the encrypted password when configuring it.
Authentication Method	Choose an authentication method. The options available are as follows. <ul style="list-style-type: none"> md5- Set an authentication method to md5. peap-mschapv2 - Set an authentication method to peap-mschapv2.

Click **Apply** to reflect the change.

9.2.8 802.1X Supplicant Port Settings

The following window displays the configuration and state regarding the function of IEEE 802.1X supplicant of the port specified.

Choose **Security > 802.1X > 802.1X Supplicant Port Settings** to display the following window.

802.1X Supplicant Port Settings

802.1X Supplicant Port Settings

Port:

Held Period (0-65535): ☐ Default

Authentication Period (1-65535): ☐ Default

Start Period (1-65535): ☐ Default

Max Start (1-65535): ☐ Default

State:

802.1X Supplicant Port Table

Port	Held Period	Authentication Period	Start Period	Max Start	State
F1/0/1	60	30	30	3	Disabled
F1/0/2	60	30	30	3	Disabled
F1/0/3	60	30	30	3	Disabled
F1/0/4	60	30	30	3	Disabled
Te1/0/5	60	30	30	3	Disabled
Te1/0/6	60	30	30	3	Disabled

Figure 9-13 802.1X Supplicant Port Settings

In the section of **802.1X Supplicant Port Settings**, you can configure the following parameters.

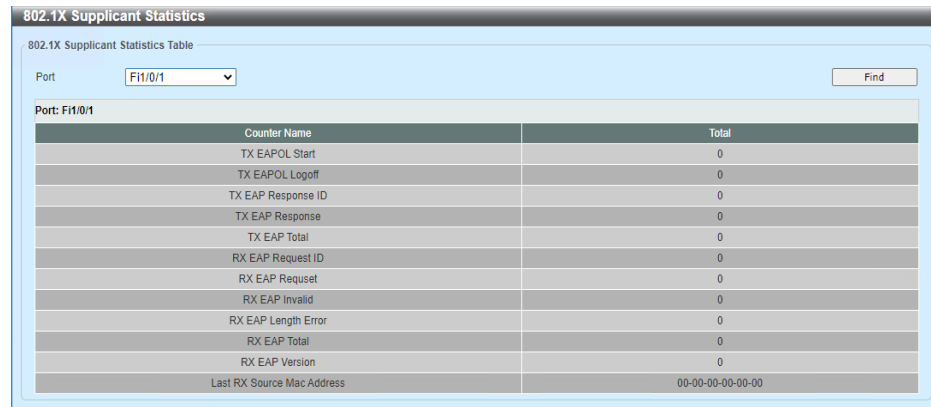
Parameter	Overview
Port	Choose a port to be configured.
Held Period	This parameter configures the necessary time for waiting the next authentication when the supplicant fails to authenticate. The range is from 0 to 65,535. The default is 60 (seconds).
Authentication Period	This parameter configures the necessary time for waiting the request from an authenticator. The range is from 1 to 65,535. The default is 30 (seconds).
Start Period	This parameter configures the transmission interval of EAPOL when starting an authentication. The range is from 1 to 65,535. The default is 30 (seconds).
Max Start	This parameter configures the maximum number of EAPOL-Start packets transmissions. The range is from 1 to 65,535. The default is three times.
State	This parameter configures to enable or disable the function of a port supplicant. <ul style="list-style-type: none"> Disabled - Displays the statics since the reset of the last switch (default value). Enabled - Displays the statistics since the boot-up of the last switch.

Click **Apply** to reflect the change.

9.2.9 802.1X Supplicant Statistics Information

The following window displays the IEEE 802.1X supplicant statistics information on the port specified.

Choose **Security > 802.1X > 802.1X Supplicant Statistics** to display the following window.



Counter Name	Total
TX EAPOL Start	0
TX EAPOL Logoff	0
TX EAP Response ID	0
TX EAP Response	0
TX EAP Total	0
RX EAP Request ID	0
RX EAP Request	0
RX EAP Invalid	0
RX EAP Length Error	0
RX EAP Total	0
RX EAP Version	0
Last RX Source Mac Address	00-00-00-00-00-00

Figure 9-14 802.1X Supplicant Statistics Information

In the section of **802.1X Supplicant Statistics**, you can configure the following parameter.

Parameter	Overview
Port	Choose a port to be configured.

Click **Retrieve** to display information on the port specified.

9.3 AAA (Authentication, Authorization, and Accounting)

9.3.1 AAA Global Settings

Use the following window to enable or disable to set the AAA function to global.

Choose **Security > AAA > AAA Global Settings** to display the following window.



Figure 9-15 AAA Global Settings

In the section of **AAA Condition Settings**, you can configure the following parameter.

Parameter	Overview
AAA Condition	Enables or disables to set an AAA function to global.

Click **Apply** to check the content changed.

9.3.2 AAA Authentication Settings

Use the following window to implement the settings on the AAA authentication and display its settings.

Choose **Security > AAA > AAA Authentication Settings** to display the following window.

Figure 9-16 AAA Authentication Settings

In the section of **AAA Web Authentication Settings**, you can configure the following parameters.

Parameter	Overview
Primary Database	Choose a primary database to use for Web authentication. The options available are as follows. <ul style="list-style-type: none"> • RADIUS - Uses the database on a RADIUS server as the primary database. • Local - Uses the local database on a switch as the primary database.
Secondary Database	Choose a secondary database to use for Web authentication. The options available are as follows. <ul style="list-style-type: none"> • None - Authentication on the secondary database is treated as approved. • RADIUS - Uses the database on a RADIUS server as the secondary database. • Local - Uses the local database on a switch as the secondary database.
Authentication Fail Action	<ul style="list-style-type: none"> • Stop - Specifies to stop authentication when Web authentication failed using the primary database. However the secondary database applies if it cannot communicate with the RADIUS server which is the primary database. • Secondary DB - Specifies to initiate authentication using the secondary database when Web authentication failed using the primary database.

Parameter	Overview
Authentication Fail Block Time	Enter the number of seconds (needed) to block a host in case of the Web authentication failure. The range is from 1 to 65,535 (seconds).

Click **Apply** to check the content changed.

In the section of **AAA MAC Authentication Settings**, you can configure the following parameters.

Parameter	Overview
Primary Database	Choose a primary database to use for a MAC authentication. The options available are as follows. <ul style="list-style-type: none"> • RADIUS - Uses the database on a RADIUS server as the primary database. • Local - Uses the local database on a switch as the primary database.
Secondary Database	Choose a secondary database to use for a MAC authentication. The options available are as follows. <ul style="list-style-type: none"> • None - Authentication on the secondary database is treated as approved. • RADIUS - Uses the database on a RADIUS server as the secondary database. • Local - Uses the local database on a switch as the secondary database.
Authentication Fail Action	<ul style="list-style-type: none"> • Stop - Specifies to stop authentication when MAC authentication failed using the primary database. However the secondary database applies if it cannot communicate with the RADIUS server which is the primary database. • Secondary DB - Specifies to initiate authentication using the secondary database when MAC authentication failed using the primary database.
Authentication Failure Block-time	Enter the number of seconds to block a host in case of the MAC authentication failure. The range is from 1 to 65,535 (seconds).

Click **Apply** to check the content changed.

In the section of **AAA 802.1X Authentication Settings**, you can configure the following parameters.

Parameter	Overview
Primary Database	Choose a primary database to use for IEEE 802.1X authentication. The options available are as follows. <ul style="list-style-type: none">• RADIUS - Uses the database on a RADIUS server as the primary database.• Local - Uses the local database on a switch as the primary database.
Secondary Database	Choose a secondary database to use for IEEE 802.1X authentication. The options available are as follows. <ul style="list-style-type: none">• None - Does not use the secondary database.• Local - Uses the local database on a switch as the secondary database.

Click **Apply** to check the content changed.

9.3.3 AAA Authentication User Settings

This window is used to configure and display the AAA authentication user settings.

Click **Security > AAA > AAA Authentication User Settings** to view the following window:

AAA Authentication User Settings

AAA Authentication User Settings

User Name: 32 chars

Filter-ID (1-14999):

2-Step Authentication: Disabled

Encrypt: ☐ Encrypt

Encrypt Password: ☐ Encrypt Password

Authentication Type: Both

2nd Authentication: ☐

Apply

Total Entries: 1

User Name	Password	VLAN	Filter-ID	Authentication Type	2-Step Authentication	2nd Authentication	
user	password	1	1	Both	No	Yes	Delete

1/1 1 Go

Figure 9-17 AAA Authentication User Settings

The following parameters can be configured in the **AAA Authentication User Settings** section:

Parameter	Description
User Name	Enter the username for the local authentication account here. This can be up to 32 characters long.
VLAN ID	Enter the target VLAN ID for the local authentication account here. The range is from 1 to 4094.
Password	Select and enter the clear-text password for the local authentication account here. Select the Encrypt option to enable password encryption for this account. The clear-text password will be saved in the encrypted form on the switch.
Encrypt Password	Select and enter the encrypted password for the local authentication account here.
Authentication Type	Select the authentication type here. Options to choose from are: <ul style="list-style-type: none"> Both - Specifies that the local authentication account will be used for IEEE 802.1X and web authentication. Web - Specifies that the local authentication account will be used for web authentication only. Dot1X - Specifies that the local authentication account will be used for IEEE 802.1X authentication only.
2-Step Authentication	Select to enable or disable two-step authentication here.

Parameter	Description
2nd Authentication	Select to enable the second authentication step account for two-step authentication.

Click the **Apply** button to add a new entry.

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

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

9.3.4 AAA Authentication MAC Settings

Use the following window to implement the settings on AAA authentication MAC and display its settings.

Choose **Security > AAA > AAA Authentication MAC Settings** to display the following window.

Figure 9-18 AAA Authentication MAC Settings

In the section of the **AAA Authentication MAC Settings**, you can configure the following parameters.

Parameter	Overview
MAC Address	Enter a MAC address of a local authentication account. This is used for a MAC authentication.
VLAN ID	Enter the target VLAN ID of a local authentication account. The range is from 1 to 4,094.
2 Steps Authentication	<p>This parameter enables or disables the 2 steps authentication. The options available are as follows.</p> <ul style="list-style-type: none"> • No - Disables the 2 step authentication of a local authentication account. • Web - Enables the 2 step authentication to use the Web authentication as the second authentication method. • 802.1X - Enables the 2 step authentication to use the IEEE 802.1X authentication as the second authentication method. • Optional - Enables the 2 step authentication to use the IEEE 802.1X authentication and Web authentication as the second authentication method.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.3.5 Application Authentication Settings

Use the following window to implement the settings on the application authentication and display its settings.

Choose **Security > AAA > Application Authentication Settings** to display the following window.

Application	Login Method List	
Console	default	Edit
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 9-19 Application Authentication Settings

Click **Edit** to display the following window.

Application	Login Method List	
Console	<input type="text" value="default"/>	Apply
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 9-20 Application Authentication Settings (Edition)

In the section of **Application Authentication Settings**, you can configure the following parameters.

Parameter	Overview
Login Method List	Enter the name of the login method list.

Click **Edit** to edit the configuration of the entry specified.

Click **Apply** to check the content changed.

9.3.6 Application Accounting Settings

Use the following window to implement the settings on an application accounting and display its settings.

Choose **Security > AAA > Application Accounting Settings** to display the following window.

Figure 9-21 Application Accounting Settings

Click **Edit** to display the following window.

Figure 9-22 Application Accounting Settings (Edition)

In the section of **Application Accounting Exec Method List**, you can configure the following parameter.

Parameter	Overview
Exec Method List	Enter the name of the exec method list.

Click **Apply** to check the content changed.

In the section of the **Application Accounting Command Method List**, you can configure the following parameters.

Parameter	Overview
Application	Choose the application you use. The options available are Console , Telnet and SSH .
Level	Choose the privilege level you use. The range of values to choose is from 1 to 15.
Command Method List	Enter the name of the command method list you use.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.3.7 Authentication EXEC Settings

Use the following window to implement the settings on the authentication EXEC and display its settings.

Choose **Security > AAA > Authentication EXEC Settings** to display the following window.

Figure 9-23 Authentication EXEC Settings

In the section of **AAA Authentication Enable**, you can configure the following parameters.

Parameter	Overview
Status	This parameter enables or disables the enabled state regarding the AAA authentication.
Method 1 - Method 4	<p>Choose the method list to use for this configuration. The options available are as follows.</p> <ul style="list-style-type: none"> • None - This method specifies as the last method of a list. Users are authenticated if (the step for) the authentication of the previous method is not denied. Usually, the method specifies as the last method of a list. • Enable - Uses the local enable password for an authentication. • Group - Uses the server groups, which are defined by using the AAA group server command. Enter the name of the AAA group server in the entry field displayed. The number of characters for this string can be up to 32. • RADIUS - Uses the server, which is defined by using the RADIUS server host command. • TACACS+ - Uses the server, which is defined by using the tacacs+ server host command.

Click **Apply** to check the content changed.

In the section of **AAA Authentication Login**, you can configure the following parameters.

Parameter	Overview
List Name	Enter the method-list name, which is used in the AAA Authentication Login option.
Method 1 - Method 4	<p>Choose the method lists, which are used for this configuration. The options available are as follows.</p> <ul style="list-style-type: none">• None - Users are authenticated if (the step for) the authentication of the previous method is not denied. Usually, the method specifies as the last method of a list.• Local - Uses the local database for authentication.• Group - Uses the server group, which is defined by using the AAA group server command.• Enter the name of the AAA group server in the entry field displayed. The number of characters for this character strings can be up to 32.• RADIUS - Uses the server, which is defined by using the RADIUS server host command.• TACACS+ - Uses the server, which is defined by using the TACACS+ server host command.

Click **Apply** to add a new entry.

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

9.3.8 Accounting Settings

Use the following window to implement the settings on AAA account and display its settings.

Choose **Security > AAA > Accounting Settings** to display the following window.

Figure 9-24 Accounting Settings (AAA Accounting Network)

In the section of **AAA Accounting Network**, you can configure the following parameters.

Parameter	Overview
Default	This parameter enables or disables the default method list.
Method 1 - Method 4	Choose the method list to use for this configuration. The options available are None , Group , RADIUS and TACACS+ . The None option is available for the method 1.

Click **Apply** to check the content changed.

Click the **AAA Accounting System** tab to display the following window.

Figure 9-25 Accounting Settings (AAA Accounting System)

In the section of **AAA Accounting System**, you can configure the following parameters.

Parameter	Overview
Default	This parameter enables or disables the default method list.

Parameter	Overview
Method 1 - Method 4	Choose the method list to use for this configuration. The options available are None , Group , RADIUS and TACACS+ . The None option is available for the method 1.

Click **Apply** to check the content changed.

Click **AAA Accounting Exec** tab to display the following window.

Figure 9-26 Accounting Settings (AAA Accounting Exec)

In the section of **AAA Accounting Exec**, you can configure the following parameters.

Parameter	Overview
List Name	Enter a method-list name to use in the AAA Accounting Exec option.
Method 1 - Method 4	Choose a method list to use for this configuration. The options available are None , Group , RADIUS and TACACS+ . The None option is available for the method 1, only.

Click **Apply** to add a new entry.

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

Click the **AAA Accounting Command** tab to display the following window.

The screenshot shows the 'Accounting Settings' window with the 'AAA Accounting Commands' tab selected. The configuration fields are as follows:

- Level: 1
- List Name: 32 chars
- Method 1: None
- Method 2: Please Select
- Method 3: Please Select
- Method 4: Please Select

Below the fields is a table with the following structure:

Level	Name	Method 1	Method 2	Method 3	Method 4
Total Entries: 0					

Figure 9-27 Accounting Settings (AAA Accounting Command)

In the section of **AAA Accounting Command**, you can configure the following parameters.

Parameter	Overview
Level	Choose the privilege level you use. The range of values to choose is from 1 to 15 (level).
List Name	Enter the method list name to use in the AAA Accounting Command option.
Method 1 - Method 4	Choose the method list to use for this configuration. The options available are None , Group and TACACS+ . The None option is available for the method 1, only.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.4 Authentication

9.4.1 Authentication Dynamic VLAN Settings

Use the following window to implement the dynamic VLAN settings, which is used for an authentication, and display its settings.

Choose **Security > Authentication > Authentication Dynamic VLAN Settings** to display the following window.

Port	Current PVID	Authentication Status	Guest VLAN	Default VLAN
F11/0/1	1	Authorized	----	----
F11/0/2	1	Authorized	----	----
F11/0/3	1	Authorized	----	----
F11/0/4	1	Authorized	----	----
Te11/0/5	1	Authorized	----	----
Te11/0/6	1	Authorized	----	----

Figure 9-28 Authentication Dynamic VLAN Settings

In the section of **Authentication Dynamic VLAN Settings**, you can configure the following parameters.

Parameter	Overview
Accept RADIUS Attribute	This parameter enables or disables the acceptance of the RADIUS attribute.
From Port/ To Port	Choose the port you use.
Guest VLAN	This parameter enables or disables a Guest VLAN. If this is enabled, hosts are allowed to access to the guest VLAN without any authentication.
Guest VLAN ID	Enter the guest VLAN ID whose range is from 1 to 4,094.
Default VLAN	This parameter enables or disables the default VLAN. The hosts, which are accurately authenticated, are allocated to the default VLAN if the dynamic VLAN function is disabled or a host target VLAN is disabled (or invalid).
Default VLAN ID	Enter a default VLAN ID. The range is from 1 to 4,094.

Click **Apply** to check the content changed.

9.4.2 Authentication Status Table

Use the following window to display an authentication state table and its information. In addition, the authentication aging time can be configured in this window.

Choose **Security > Authentication > Authentication Status Table** to display the following window.

Figure 9-29 Authentication Status Table

In the section of **Authentication Status Table**, you can configure the following parameters.

Parameter	Overview
Authentication Aging Time	Enter the value of time-out of the MAC/Web authentication session. The range is from 0 to 65,535 (minutes).
Sort By - MAC	If you choose this option, an authentication session is displayed in a sequential order of MAC addresses.
Sort By - Port	If you choose this option, an authentication session of the port specified is displayed. <ul style="list-style-type: none"> • From Port/ To Port - Choose the port you use.

Click **Apply** to check the content changed.

Click **Find** to search and display the entries based on the search condition specified.

9.4.3 2-Step Authentication Settings

Use the following window to implement the settings on the 2 step authentication of the port specified and display its settings.

Choose **Security > Authentication > 2-Step Authentication Settings** to display the following window.

Figure 9-30 2-Step Authentication Settings

In the section of **2-Step Authentication Settings**, you can configure the following parameters.

Parameter	Overview
2 Step Authentication Timeout	Enter the time-out value. If this time passes, the second step of an authentication is tried (or attempted). The range is from 0 to 65,535 (minutes).
From Port/ To Port	Choose the port you use.
2 Step Authentication Mode	Choose the 2 step authentication mode. The options available are as follows. <ul style="list-style-type: none"> • MAC-Web - Both MAC and WEB authentication are used in the first step of the two-step authentication method. • MAC-Dot1X - Both MAC and IEEE802.11X authentication are used in the first step of the two-step authentication method. • Dot1X-Web - Both IEEE 802.1X and WEB authentication are used in the first step of the two-step authentication method.

Click **Apply** to check the content changed.

Click **Clear** to clear the information based on the condition specified.

9.5 RADIUS (Remote Authentication Dial-In User Service)

9.5.1 RADIUS Global Settings

Use the following window to implement the global settings, which is associated with the RADIUS function, and display its settings.

Choose **Security > RADIUS > RADIUS Global Settings** to display the following window.

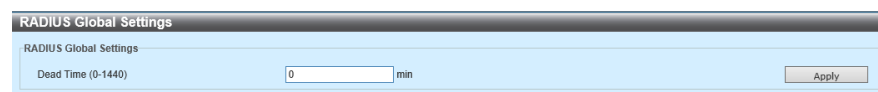


Figure 9-31 RADIUS Global Settings

In the section of **RADIUS Global Settings**, you can configure the following parameter.

Parameter	Overview
Dead Time	Enter the dead-time value. If the system implements an authentication by using an authentication server, it attempts a server one by one. If the server does not respond, the system attempts the next server. If the system finds a server that does not respond, it marks the server as a down server to start the dead time timer. The server on this state is skipped until the dead time passes in the following request authentication. The range is from 1 to 1440 (minutes). By default, this value is set to 0 (minute). If this option is 0, the unresponsive server is not marked as dead. Use this settings to shorten the time needed for an authentication processing by configuring the dead time to skip the unresponsive server host-entry.

Click **Apply** to reflect the change.

In the section of **RADIUS Global IPv4 Source Interface**, you can configure the following parameter.

Parameter	Overview
IPv4 RADIUS Source Interface Name	Enter the name of the IPv4 RADIUS source interface.

Click **Apply** to reflect the change.

In the section of **RADIUS Global IPv6 Source Interface**, you can configure the following parameter.

Parameter	Overview
IPv6 RADIUS Source Interface Name	Enter the name of the IPv6 RADIUS source interface.

Click **Apply** to reflect the change.

9.5.2 RADIUS Server Settings

Use the following window to implement the settings on a RADIUS server and display its settings.

Choose **Security > RADIUS > RADIUS Server Settings** to display the following window.

Figure 9-32 RADIUS Server Settings

In the section of the **RADIUS Server Settings**, you can configure the following parameters.

Parameter	Overview
IP Address	Enter an IPv4 address of a RADIUS server.
IPv6 Address	Enter an IPv6 address of a RADIUS server.
Authentication Port	Enter the authentication port-number (value) you use. The range is from 0 to 65,535. By default, the value is set to 1,812. If no authentication is used, use the value of 0.
Accounting Port	Enter the accounting port-number (value) you use. The range is from 0 to 65,535. By default, the value is set to 1,813. If no accounting is used, use the value of 0.
Retransmission	Enter the value regarding the number of retransmissions. The range is from 0 to 20. By default, the value is set to 3. To disable this option, enter the value of 0.
Timeout	Enter the timeout value you use. The range is from 1 to 255 seconds. By default, the value is set to 5 seconds.
Key Type	Choose the key type you use. The options available are Plain Text and Encrypted .
Key	Enter the key, which is used to communicate with a RADIUS server. The number of characters for the key can be up to 32.

Click **Apply** to add a new entry.

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

9.5.3 RADIUS Group Server Settings

Use the following window to implement the settings on and display its settings.

Choose **Security > RADIUS > RADIUS Group Server Settings** to display the following window.

Figure 9-33 RADIUS Group Server Settings

In the section of **RADIUS Group Server Settings**, you can configure the following parameters.

Parameter	Overview
Group Server Name	Enter the name of a RADIUS group server. The number of characters for the name can be up to 32.
IP Address	Enter an IPv4 address of a RADIUS group server.
IPv6 Address	Enter an IPv6 address of a RADIUS group server.

Click **Add** to add new entries.

Click **Show Detail** to display details on the entry.

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

Click **Show Detail** to display the following window.

Figure 9-34 RADIUS Group Server Settings (Show Detail.)

You can configure the following parameters.

Parameter	Overview
IPv4 RADIUS Source Interface Name	Enter the name of the IPv4 RADIUS source-interface.
IPv6 RADIUS Source Interface Name	Enter the name of the IPv6 RADIUS source-interface.

Click **Apply** to add a new entry.

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

Click **Back** to return to the previous window.

9.5.4 RADIUS Statistic

Use the following window to display and clear the RADIUS statistics information.

Choose **Security > RADIUS > RADIUS Statistic** to display the following window.

The screenshot shows the 'RADIUS Statistic' window. At the top, there is a 'Group Server Name' dropdown menu with 'Please Select' and buttons for 'Clear' and 'Clear All'. Below this, a summary table shows 'Total Entries: 1' for the RADIUS Server Address '172.16.230.10', with Authentication Port '1812' and Accounting Port '1813'. The state is 'Up'. A pagination bar shows '1/1' and a 'Go' button. Below the summary, there is a 'Clear' button and a detailed table of statistics for the RADIUS Server Address '172.16.230.10'.

Parameter	Authentication Port	Accounting Port
Round Trip Time	0	0
Access Requests	0	NA
Access Accepts	0	NA
Access Rejects	0	NA
Access Challenges	0	NA
Acct Request	NA	0
Acct Response	NA	0
Retransmissions	0	0
Malformed Responses	0	0
Bad Authenticators	0	0
Pending Requests	0	0
Timeouts	0	0
Unknown Types	0	0
Packets Dropped	0	0

Figure 9-35 RADIUS Statistic

In the section of **RADIUS Statistics**, you can configure the following parameter.

Parameter	Overview
Group Server Name	Choose the name of a RADIUS group server from this list.

Click **Clear**, the first one, to clear the statistics information based on the condition specified.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **Clear** (the second one) to clear the statistics information on a table.

9.6 TACACS+ (Terminal Access Controller Access-Control System Plus)

9.6.1 TACACS+ Global Settings

This window is used to configure and display the global settings associated with the TACACS+ function.

Choose **Security > TACACS+ > TACACS+ Global Settings** to display the following window.

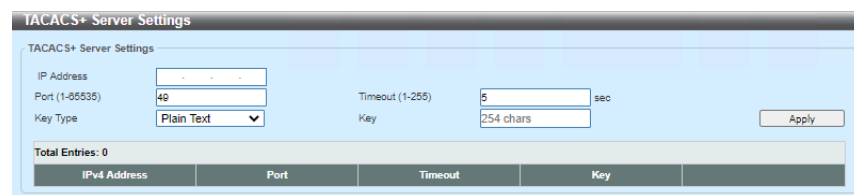


Figure 9-36 TACACS+ Global Settings

You can configure the following parameters in the **TACACS+ Global IPv4 Source Interface** section.

Parameter	Description
IPv4 TACACS+ Source Interface Name	Enter the name of the IPv4 TACACS+ source interface.

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

9.6.2 TACACS+ Group Server Settings

This window is used to configure and display the TACACS+ group server settings.

Choose **Security > TACACS+ > TACACS+ Group Server Settings** to display the following window.

[illegible]

Figure 9-37 TACACS+ Group Server Settings

You can configure the following parameters in the **TACACS+ Group Server Settings** section.

Parameter	Description
Group Server Name	Enter the TACACS+ group server name here. This name can be up to 32 characters long.
IPv4 IP Address	Enter the IPv4 address of the TACACS+ group server here.

Click the **Add** button to add a new entry.

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to display the following window.

[illegible]

Figure 9-38 TACACS+ Group Server Settings (Show Detail)

You can configure the following parameters in the **TACACS+ Group Server Settings** section.

Parameter	Description
IPv4 TACACS+ Source Interface Name	Enter the name of the source IPv4 TACACS+ interface here.

Click the **Apply** button to add a new entry.

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

Click the **Back** button to return to the previous window.

9.6.3 TACACS+ Statistic

This window is used to display and clear the TACACS+ statistics information.

Choose **Security > TACACS+ > TACACS+ Statistic** to display the following window.

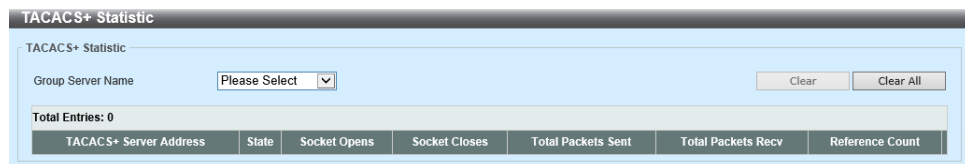


Figure 9-39 TACACS+ Statistic

You can configure the following parameters in the **TACACS+ Statistic** section.

Parameter	Description
Group Server Name	Select the TACACS+ group server name from this list here.

Click the first **Clear** button to clear the statistics information based on the criteria specified.

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

Click the second **Clear** button to clear the statistics information on the specified entry.

9.7 SAVI (Source Address Validation Improvements)

9.7.1 IPv4

9.7.1.1 DHCPv4 Snooping

9.7.1.1.1 DHCP Snooping Global Settings

Use the following window to implement the global settings, which is associated with the DHCP Snooping function, and display its settings.

Choose **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings** to display the following window.

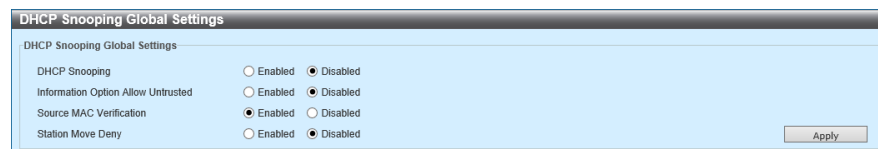


Figure 9-40 DHCP Snooping Global Settings

In the section of **DHCP Snooping Global Settings**, you can configure the following parameters.

Parameter	Overview
DHCP Snooping	This parameter enables or disables to set DHCP Snooping to global.
Information Option Allow Untrusted	This parameter enables or disables the option globally to allow DHCP packets where the relay option 82 is configured on the untrusted interface.
Source MAC Verification	This parameter enables or disables a verification; a source MAC address of DHCP packets matches with a client hardware address.
Station Move Deny	This parameter enables or disables the state of the DHCP Snooping station move. If the DHCP Snooping station move is enabled, the dynamic DHCP Snooping binding entry, including the same VLAN ID and MAC address on the specific port, can be moved to the other port. If you detect a new DHCP process that uses the same VLAN ID and MAC address.

Click **Apply** to reflect the change.

9.7.1.1.2 DHCP Snooping Port Settings

Use the following window to implement the settings on the DHCP Snooping and display its settings.

Choose **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings** to display the following window.

Port	Trusted	Rate Limit	Entry Limit
F11/0/1	No	No Limit	No Limit
F11/0/2	No	No Limit	No Limit
F11/0/3	No	No Limit	No Limit
F11/0/4	No	No Limit	No Limit
Te1/0/5	No	No Limit	No Limit
Te1/0/6	No	No Limit	No Limit

Figure 9-41 DHCP Snooping Port Settings

In the section of **DHCP Snooping Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Entry Limit	Enter the entry limit value. The range is from 0 to 508. If you set No Limit to on, the function becomes disabled.
Bandwidth Limit (Rate Limit)	Enter the value of bandwidth limitation. The range is from 1 to 300. If you set No Limit to on, the function becomes disabled.
Trusted	Choose the trusted option. The options available are No and Yes . The port connected to a DHCP server or other switches must be configured as a trusted interface. The ports connected to a DHCP client must be configured as an untrusted interface. DHCP Snooping operates as a firewall between an untrusted interface and a DHCP server.

Click **Apply** to reflect the change.

9.7.1.1.3 DHCP Snooping VLAN Settings

Use the following window to implement the settings on DHCP Snooping of the VLAN specified and display its settings.

Choose **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings** to display the following window.

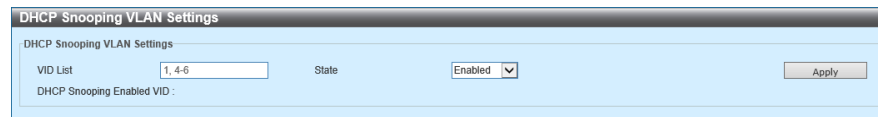


Figure 9-42 DHCP Snooping VLAN Settings

In the section of **DHCP Snooping VLAN Settings**, you can configure the following parameters.

Parameter	Overview
VID List	Enter a VLAN ID to use it. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.
State	This parameter enables or disables the settings on a DHCP Snooping VLAN.

Click **Apply** to reflect the change.

9.7.1.1.4 DHCP Snooping Database

Use the following window to implement the settings on the DHCP Snooping database and display its settings.

Choose **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Database** to display the following window.

Figure 9-43 DHCP Snooping Database

In the section of **DHCP Snooping Database**, you can configure the following parameter.

Parameter	Overview
Write Delay	Enter the write-delay time (value). The range is from 60 to 86,400 (seconds). By default, the value is set to 300 (seconds).

Click **Reset** to reset the DHCP Snooping database.

Click **Apply** to reflect the change.

In the section of **Store DHCP Snooping Database**, you can configure the following parameter.

Parameter	Overview
URL	Choose a location from the drop-down list and then enter the URL for storing the DHCP Snooping database. The locations to choose are TFTP , FTP and Local .

Click **Reset** to reset the stored DHCP Snooping database.

Click **Apply** to store (or save) the DHCP Snooping database.

In the section of **Load DHCP Snooping Database**, you can configure the following parameter.

Parameter	Overview
URL	Choose a location from the drop-down list and enter the URL for loading the DHCP Snooping database. The locations to choose are TFTP , FTP and Local .

Click **Apply** to load the DHCP Snooping database.

Click **Clear** to clear the counter information.

9.7.1.1.5 DHCP Snooping Binding Entry

Use the following window to implement the settings on the DHCP Snooping binding entry and display its settings.

Choose **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry** to display the following window.

Figure 9-44 DHCP Snooping Binding Entry

In the section of **DHCP Snooping Manual Binding**, you can configure the following parameters.

Parameter	Overview
MAC Address	Enter a MAC address of the DHCP Snooping binding entry.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
IP Address	Enter an IP address of the DHCP Snooping binding entry.
Port	Choose the port you use.
Expiry	Enter the value of the valid deadline to use. The range is from 60 to 4,294,967,295 (seconds).

Click **Add** to add new entries.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.7.1.2 Dynamic ARP Inspection

9.7.1.2.1 ARP Access List

Use the following window to implement the settings on the ARP access list and display its settings.

Choose **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Access List** to display the following window.

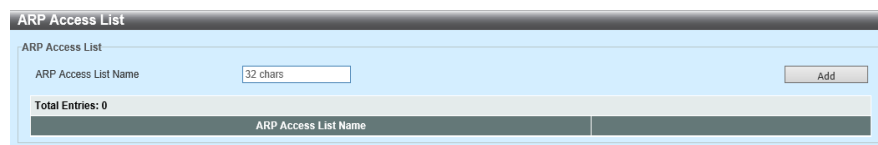


Figure 9-45 ARP Access List

In the section of the **ARP Access List**, you can configure the following parameter.

Parameter	Overview
ARP Access List Name	Enter the name of the ARP access list you use. The number of characters for the name can be up to 32.

Click **Add** to add new entries.

Click **Edit** to edit the configuration of the entry specified.

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

Click **Edit** to display the following window.

Figure 9-46 ARP Access List (Edit)

You can configure the following parameters.

Parameter	Overview
Action	Choose the action you perform. The options available are Permit and Deny .
IP	Choose the type of the sender IP address you use. The options available are Any , Host and IP and Mask
Sender IP	If you choose Host or IP and Mask as the IP type, enter a sender IP address.
Sender IP Mask	If you choose the IP and Mask option as the IP type, enter a sender IP mask.
MAC	Choose the sender MAC address type you use. The options available are Optional , Host , and MAC and Mask .
Sender MAC	If you choose Host or MAC and Mask as the MAC type, enter a sender MAC address.
Sender MAC Mask	If you choose MAC and Mask as the MAC type, enter the sender MAC mask you use.

Click **Apply** to add a new entry.

Click **Back** to return to the previous window.

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

9.7.1.2.2 ARP Inspection Settings

Use the following window to implement the settings on ARP inspections and display its settings.

Choose **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings** to display the following window.

The screenshot shows the 'ARP Inspection Settings' window. It has a light blue background and a dark blue header. The 'ARP Inspection Validation' section has three rows of radio buttons: Src-MAC, Dst-MAC, and IP, each with 'Enabled' and 'Disabled' options. The 'ARP Inspection VLAN Logging' section has a 'VID List' text box with '1, 4-6' and a 'State' dropdown menu set to 'Enabled'. The 'ARP Inspection Filter' section has three fields: 'ARP Access List Name' (32 chars), 'VID List' (1, 4-6), and 'Static ACL' (No). At the bottom, there are two tables: 'ACL Logging' and 'DHCP Logging', each with columns for 'VID', 'ACL Logging', and 'DHCP Logging'.

Figure 9-47 ARP Inspection Settings

In the section of **ARP Inspection Items**, you can configure the following parameters.

Parameter	Overview
Src-MAC	This parameter enables or disables the source MAC option. The option checks ARP requests, response packets and the consistency between a source MAC address in the Ethernet header and a sender MAC address of the ARP payload.
Dst-MAC	This parameter enables or disables the destination MAC option. The option checks ARP response packets and the consistency between a destination MAC address in the Ethernet header and a target MAC address in the ARP payload.

Parameter	Overview
IP	This parameter enables or disables the IP option. The parameter checks a disabled IP address and an unexpected IP address on the ARP body. In addition, the parameter checks the validity of an IP address of the ARP payload. The sender IP in both the ARP request and response and the target IP of the ARP response are verified. Packets whose destinations are these IP addresses (e.g. 0.0.0.0 and 255.255.255.255) and all the IP multicast addresses are dropped. The sender IP addresses are checked by all the ARP requests and responses. Target IP addresses are checked by ARP responses.

Click **Apply** to reflect the change.

In the section of **ARP Inspection VLAN Logging**, you can configure the following parameters.

Parameter	Overview
VID List	Enter the VLAN ID you use. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.
State	This parameter enables or disables ARP inspection VLAN logging of the VLAN specified.

Click **Apply** to add a new entry.

Click **Edit** to edit the configuration of the entry specified.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

In the section of **ARP Inspection Filtering**, you can configure the following parameters.

Parameter	Overview
ARP Access List Name	Enter the name of the ARP access list to be used. The number of characters for the name can be up to 32.
VID List	Enter the VLAN ID you use. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.
Static ACL	Click Yes or No if you need to use a static ACL.

Click **Add** to add new entries.

Click **Delete** to delete entries based on the information specified.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.7.1.2.3 ARP Inspection Port Settings

Use the following window to implement the settings on the ARP inspection port settings and display its settings.

Choose **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings** to display the following window.

Port	Trust State	Rate Limit (pps)	Burst Interval
F1/0/1	Untrusted	15	1
F1/0/2	Untrusted	15	1
F1/0/3	Untrusted	15	1
F1/0/4	Untrusted	15	1
Te1/0/5	Untrusted	15	1
Te1/0/6	Untrusted	15	1

Figure 9-48 ARP Inspection Port Settings

You can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Rate Limit	Enter the value of rate limit. The range is from 1 to 150 (packets), per second.
Burst Interval	Enter the value of a burst-interval. The range is from 1 to 15. If you set None to on, the option becomes disabled.
Trust State	This parameter enables or disables the trust state.

Click **Apply** to reflect the change.

Click **Default Configuration** to set the trust state to the default settings.

9.7.1.2.4 ARP Inspection Statistics Information

Use the following window to display and clear the statistics information on the dynamic ARP inspection.

Choose **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics Information** to display the following window.

Figure 9-49 ARP Inspection Statistics Information

You can configure the following parameter.

Parameter	Overview
VID List	Enter the VLAN ID you use. You can enter its consecutive VLAN IDs by delimiting with a comma or enter the range of VLAN IDs by delimiting with a hyphen. The range is from 1 to 4,094.

Click **Clear by VLAN** to clear the statistics information about the VLAN specified.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.7.1.2.5 ARP Inspection Log

Use the following window to display and clear the information on dynamic ARP inspection log. In addition, you can configure the log-buffer value in the window.

Choose **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Log** to display the following window.

ARP Inspection Log

ARP Inspection Log

Log Buffer (1-1024) ☐ Default

Total Entries: 0

Port	VLAN	Sender IP	Sender MAC	Occurrence
------	------	-----------	------------	------------

Figure 9-50 ARP Inspection Log

In the section of **ARP Inspection Log**, you can configure the following parameter.

Parameter	Overview
Log Buffer	Enter the log-buffer size (value). The range is from 1 to 1,024. By default, the value is set to 32. When you choose Default, use the default value.

Click **Apply** to reflect the change.

Click **Clear Log** to clear the ARP inspection log.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.7.1.3 IP Source Guard

9.7.1.3.1 IP Source Guard Port Settings

Use the following window to implement the settings on an IP source guard of the port specified and display its settings.

Choose **Security > SAVI > IPv4 > IP Source Guard > IP Source Guard Port Settings** to display the following window.

Port	Validation Type

Figure 9-51 IP Source Guard Port Settings

You can configure the following parameters.

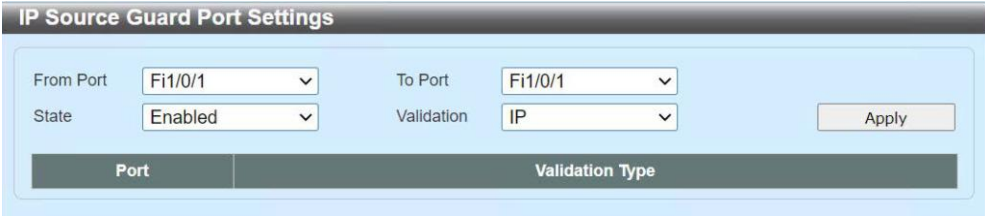
Parameter	Overview
From Port to Port: from the Beginning to the End	Choose the port you use.
State	This parameter enables or disables the state of the IP source guard for the port specified.
Verification	Choose a verification method of using. The options available are as follows. <ul style="list-style-type: none"> • IP - checks the IP address of the received packets. • IP-MAC - checks the IP address and MAC address of the received packets

Click **Apply** to add a new entry.

9.7.1.3.2 IP Source Guard Binding

Use the following window to implement the settings on an IP source guard binding and display its settings.

Choose **Security > SAVI > IPv4 > IP Source Guard > IP Source Guard Binding** to display the following window.

The image shows a web-based configuration window titled "IP Source Guard Port Settings". It has a light blue background. At the top, there are four dropdown menus: "From Port" (set to Fi1/0/1), "To Port" (set to Fi1/0/1), "State" (set to Enabled), and "Validation" (set to IP). To the right of these is an "Apply" button. Below the dropdowns is a table with two columns: "Port" and "Validation Type". The table is currently empty.

From Port	To Port	State	Validation	Apply
Fi1/0/1	Fi1/0/1	Enabled	IP	

Port	Validation Type
------	-----------------

Figure 9-52 IP Source Guard Binding

In the section of the settings on **IP Source Binding**, you can configure the following parameters.

Parameter	Overview
MAC Address	Enter a MAC address of the binding entry.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
IP Address	Enter an IP address of the binding entry.
From Port/ To Port	Choose the port you use.

Click **Apply** to reflect the change.

In the section of **IP Source Binding Entry**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
IP Address	Enter an IP address of the binding entry.
MAC Address	Enter a MAC address of the binding entry.
VID	Enter the VLAN ID you use. The range is from 1 to 4,094.
Type	<p>Choose a type of binding entries for searching. The options available are as follows.</p> <ul style="list-style-type: none"> • All - displays all the DHCP binding entries. • DHCP Snooping - displays the IP-source guard binding entry learned by DHCP binding snooping. • Static - displays the IP source guard binding entry, which is manually configured.

Click **Find** to search and display the entries based on the search condition specified.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.7.1.3.3 IP Source Guard HW Entry

Use the following window to display the IP source guard HW entry and its information.

Choose **Security > SAVI > IPv4 > IP Source Guard > IP Source Guard HW Entry** to display the following window.



Port	Filter-type	Filter-mode	IP Address	MAC Address	VLAN
------	-------------	-------------	------------	-------------	------

Figure 9-53 IP Source Guard HW Entry

You can configure the following parameter.

Parameter	Overview
From Port/ To Port	Choose the port you use.

Click **Find** to search and display the entries based on the search condition specified.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.8 DHCP Server Protection

9.8.1 Global Settings on Protecting a DHCP Server

Use the following window to implement the global settings on the function of DHCP server protection and display its settings.

Choose **Security > DHCP Server Protection > Global Settings on Protecting a DHCP Server** to display the following window

Figure 9-54 Global Settings on Protecting a DHCP Server

In the section of the **Profile Settings**, you can configure the following parameters.

Parameter	Overview
Profile Name	Enter the profile name of DHCP server protect. The number of characters for the name can be up to 32.
Client MAC	Enter a MAC address to use.

Click **Apply** to add a new entry.

Click **Delete** to delete a MAC address from the profile specified.

Click **Delete a Profile** to delete.

In the section of **Log Information**, you can configure the following parameter.

Parameter	Overview
Log Buffer Entry	Enter the number of entries to be recorded on a log. The range is from 10 to 1024. By default, the value is set to 32.

9.8.2 DHCP Server Protect Global Settings

This window is used to configure and display the global settings associated with the DHCP server protect feature.

Choose **Security > DHCP Server Protect > DHCP Server Protect Global Settings** to display the following window.

Figure 9-55 DHCP Server Protect Global Settings

The following parameters can be configured in the **Profile Settings** section.

Parameter	Description
Profile Name	Enter the DHCP Server Protect profile name here. This name can be up to 32 characters long.
Client MAC	Enter the MAC address used here.

Click the **Apply** button to add a new entry.

Click the **Delete** button to remove the MAC address from the specified profile.

Click the **Delete Profile** button to delete the profile.

The following parameters can be configured in the **Log Information** section.

Parameter	Description
Log Buffer Entries	Enter the amount of entries that will be logged here. The range is from 10 to 1,024. By default, this value is 32.

9.8.3 DHCP Server Protect Port Settings

Use the following window to configure and display the DHCP server protect settings on the specified port(s).

Choose **Security > DHCP Server Protect > DHCP Server Protect Port Settings** to display the following window.

Port	State	Server IP	Profile Name	Delete
Fi1/0/1	Disabled	-	-	Delete
Fi1/0/2	Disabled	-	-	Delete
Fi1/0/3	Disabled	-	-	Delete
Fi1/0/4	Disabled	-	-	Delete
Te1/0/5	Disabled	-	-	Delete
Te1/0/6	Disabled	-	-	Delete

Figure 9-56 DHCP Server Protect Port Settings

You can configure the following parameters in the **DHCP Server Protect Port Settings** section.

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
From Port - To Port	Select the port(s) that will be used here.
State	Select to enable or disable the DHCP Server Protect function on the port(s) specified.
Server IP	Enter the DHCP server IP address here.
Profile Name	Enter the DHCP Server Protect profile that will be used for the port(s) specified here.

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

Click the **Delete** button to remove the server IP address and profile name from the specified port.

9.9 BPDU Guard

Use the following window to implement the settings on the state of the BPDU guard function on the port specified and display its settings.

Choose **Security > BPDU Guard** to display the following window.

BPDU Guard

BPDU Guard Settings

BPDU Guard State

☐ Enabled

☒ Disabled

BPDU Guard Trap State

☐ Enabled

☒ Disabled

Apply

BPDU Guard Port Settings

From Port

To Port

State

Mode

Apply

Fi1/0/1

Fi1/0/1

Disabled

Shutdown

Port	State	Mode	Status
Fi1/0/1	Disabled	Shutdown	Normal
Fi1/0/2	Disabled	Shutdown	Normal
Fi1/0/3	Disabled	Shutdown	Normal
Fi1/0/4	Disabled	Shutdown	Normal
Te1/0/5	Disabled	Shutdown	Normal
Te1/0/6	Disabled	Shutdown	Normal

Figure 9-57 BPDU Guard

In the section of **BPDU Guard Settings**, you can configure the following parameters.

Parameter	Overview
BPDU Guard State	This parameter enables or disables to set a BPDU guard function to global.
BPDU Guard Trap State	This parameter enables or disables the BPDU guard trap state.

Click **Apply** to reflect the change.

In the section of **BPDU Guard Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
State	This parameter enables or disables the BPDU guard on the port specified.
Mode	Choose the BPDU guard mode to be applied to the port specified. The options available are as follows. <ul style="list-style-type: none"> • Drop - drops all the received BPDU packets when detecting attacks on the port. • Block - drops all the packets, including BPDU and normal packets, when detecting attacks on the port. • Shutdown - shut-downs the port when a network device detects attacks on the port.

Click **Apply** to reflect the change.

9.10 NetBIOS Filtering

Use the following window to implement the settings on the NetBIOS filtering of the port specified and display its settings.

Choose **Security > NetBIOS Filtering** to display the following window.

The screenshot shows the 'NetBIOS Filtering' configuration window. It has a title bar 'NetBIOS Filtering' and a subtitle 'NetBIOS Filtering'. Below the subtitle, there are four dropdown menus: 'From Port' (set to 'Fi1/0/1'), 'To Port' (set to 'Fi1/0/1'), 'NetBIOS Filtering State' (set to 'Disabled'), and 'Extensive NetBIOS Filtering State' (set to 'Disabled'). An 'Apply' button is located to the right of these dropdowns. Below the dropdowns is a table with three columns: 'Port', 'NetBIOS Filtering State', and 'Extensive NetBIOS Filtering State'. The table contains six rows of data, all showing 'Disabled' for both filtering states.

Port	NetBIOS Filtering State	Extensive NetBIOS Filtering State
Fi1/0/1	Disabled	Disabled
Fi1/0/2	Disabled	Disabled
Fi1/0/3	Disabled	Disabled
Fi1/0/4	Disabled	Disabled
Te1/0/5	Disabled	Disabled
Te1/0/6	Disabled	Disabled

Figure 9-58 NetBIOS Filtering

In the section of **NetBIOS Filtering**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
NetBIOS Filtering State	This parameter enables or disables the NetBios filtering state on the port specified. Use this to permit or deny NetBIOS packets on the physical port.
Extensive NetBIOS Filtering State	This parameter enables or disables the state of the extensive NetBIOS filtering on the port specified. Use this to permit or deny the NetBIOS packets through the 802.3 frame on the physical port.

Click **Apply** to reflect the change.

9.11 MAC Authentication

Use the following window to implement the settings on the MAC authentication and display its settings.

Choose **Security > MAC Authentication** to display the following window.

Figure 9-59 MAC Authentication

In the section of the **MAC Authentication Settings**, you can configure the following parameter.

Parameter	Overview
MAC Authentication State	This parameter enables or disables to set the function of MAC authentication to global.

Click **Apply** to reflect the change.

In the section of **MAC Format Settings**, you can configure the following parameters.

Parameter	Overview
Case	Choose the format of characters to use for a MAC address. The options available are as follows. <ul style="list-style-type: none"> • Capital Letters - Uses the format of capital letters for a MAC address (e.g. AA-BB-CC-DD-EE-FF). • Small Letters - Uses the format of small letters for a MAC address (e.g. aa-bb-cc-dd-ee-ff).

Parameter	Overview
Delimiter	Choose the type of a delimiter to use for a MAC address. The options available are as follows. <ul style="list-style-type: none"> • Hyphen - Uses a hyphen as a delimiter for a MAC address (e.g. AA-BB-CC-DD-EE-FF). • Colon - Uses a colon as a delimiter for a MAC address (e.g. AA:BB:CC:DD:EE:FF). • Dot - Uses a dot as a delimiter for a MAC address (e.g. AA.BB.CC.DD.EE.FF). • None - does not use a delimiter for a MAC address (e.g. AABBCCDDEEFF).
Delimiter Characters	Choose the number of delimiters to use for a MAC address. The options available are as follows. <ul style="list-style-type: none"> • 2 - uses one delimiter for a MAC address (e.g. AABBCC-DDEEFF). • 4 - uses two delimiters for a MAC address (e.g. AABB-CCDD-EEFF). • 6 - uses five delimiters for a MAC address (e.g. AA-BB-CC-DD-EE-FF).

Click **Apply** to reflect the change.

In the section of **MAC Authentication Password Settings**, you can configure the following parameters.

Parameter	Overview
RADIUS Password Type	Choose the RADIUS password type. The options available are as follows. <ul style="list-style-type: none"> • MAC Address - Enter a MAC address as a RADIUS password. • Manual - Uses the manual character-strings as a RADIUS password.
Manual	Enter a RADIUS password of a MAC authentication account.

Click **Apply** to reflect the change.

In the section of **MAC Authentication Port**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
State	This parameter enables or disables the MAC authentication on the port(s) specified.

Click **Apply** to reflect the change.

9.12 Web Authentication

9.12.1 Web Authentication Settings

Use the following window to implement the settings on Web authentication and display its settings.

Choose **Security > Web Authentication > Web Authentication Settings** to display the following window.

Figure 9-60 Web Authentication Settings

In the section of **Global Settings**, you can configure the following parameter.

Parameter	Overview
Authentication State	This parameter enables or disables to set the Web authentication function to global.

Click **Apply** to reflect the change.

In the section of **Authentication Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
State	This parameter enables or disables the function of Web authentication of the port specified.

Click **Apply** to reflect the change.

In the section of **Authentication Settings**, you can configure the following parameters.

Parameter	Overview
Virtual	Enter a virtual IPv4 address to use. All the Web authentication processes communicate with the virtual IP address, and the virtual IP does not respond to ICMP packets or ARQ requests. The IPv4 address for a virtual IPv4 address and a switch needs to use a different subnet. The virtual IPv4 address is an indispensable component for the normal operation of the Web authentication.
HTTP Port-Number	Enter the port-number (value) of HTTP TCP/UDP. The range is from 1 to 65,535. By default, the value is set to 80. HTTP stands for Hypertext Transfer Protocol.
Redirect URL	Enter the redirect URL. The number of characters for this can be up to 64.

Click **Apply** to reflect the change.

9.12.2 Web Page Contents Settings

This window is used to configure and display the Web page content settings.

Click **Security > Web Authentication > Web Page Contents Settings** to view the following window:

Figure 9-61 Web Page Contents Settings

The following parameters can be configured in the **Web Page Content Settings** section:

Parameter	Description
Logo Data File Select	Click the Browse button and navigate to the image file (JPG/GIF/PNG) that will be uploaded here.

Parameter	Description
Logo Data	This displays the uploaded image file (in use). Click the Delete Logo button to delete the existing image file.
Page Title	Enter a custom page title message here. This can be up to 64 characters long.
User Name String	Enter a custom username title here. This can be up to 32 characters long.
Password String	Enter a custom password title here. This can be up to 32 characters long.
Message	Enter a custom message here. This can be up to 256 characters long.
Description	Enter a custom description message here. This can be up to 256 characters long.

Click the **Upload** button to upload the new logo.

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

9.12.3 Temporary DHCP Server Settings

This window is used to configure the temporary DHCP server settings.

Click Security > Web Authentication > Temporary DHCP Server Settings to view the following window:

Figure 9-62 Temporary DHCP Server Settings

The following parameters can be configured in the Temporary DHCP Server Settings section:

Parameter	Description
Temporary DHCP Server State	Select to enable or disable the temporary DHCP server function here.

Parameter	Description
Number of Leased IP Address	Enter the number of IP addresses that will be leased. The range is from 1 to 64.
DHCP Lease Time	Enter the DHCP lease time here. The range is from 10 to 60 seconds.
Start of Leased IP Address	Enter the starting IP address in the temporary DHCP server pool here.
DNS Server Address	Enter the IP address of the DNS server that will be assigned to DHCP clients here.
Default Gateway	Enter the IP address of the default gateway that will be assigned to DHCP clients here.

Click the Apply button to accept the changes made.

9.13 Trusted Host

Use the following window to implement the settings on the trusted host and display its settings.

Choose **Security > Trusted Host** to display the following window.




Figure 9-63 Trusted Host

In the section of the **Trusted Host**, you can configure the following parameters.

Parameter	Overview
ACL Name	Enter the name of ACL. The number of characters for the name can be up to 32.
Type	Enter the type of the trusted host. The options available are Telnet , SSH , Ping , HTTP and HTTPS (Hyper Text Transfer Protocol Secure).

Click **Apply** to add a new entry.

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

9.14 Traffic Segmentation Settings

Use the following window to configure and display the traffic segmentation settings on the specified port(s).

Choose **Security > Traffic Segmentation Settings** to display the following window.

Port	Forwarding Domain
------	-------------------

Figure 9-64 Traffic Segmentation Settings

You can configure the following parameters in the **Traffic Segmentation Settings** section.

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack that will receive packets.
From Port - To Port	Select the port(s) that will receive packets.
Forward Unit	Select the unit ID of the switch in the physical stack that will forward packets.
From Forward Port - To Forward Port	Select the port(s) that will forward packets.

Click the **Add** button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

9.15 Storm Control

Use the following window to implement the storm-control settings and display its settings.

Choose **Security > Storm Control** to display the following window.

Storm Control

Storm Control Trap Settings
Trap State: **None** [Apply]

Storm Control Polling Settings
Polling Interval (5-600): **5** sec Shutdown Retries (0-360): **3** times [Infinite] [Apply]

Storm Control Port Settings
From Port: **F1/0/1** To Port: **F1/0/1** Type: **Broadcast** Action: **Drop** Level Type: **PPS** PPS Rise (0-1488100): [] pps PPS Low (0-1488100): [] pps [Apply]

Total Entries: 18

Port	Storm	Action	Threshold	Current	State
F1/0/1	Broadcast	Drop	—	—	Inactive
	Multicast		—	—	Inactive
	Unicast		—	—	Inactive
F1/0/2	Broadcast	Drop	—	—	Inactive
	Multicast		—	—	Inactive
	Unicast		—	—	Inactive
F1/0/3	Broadcast	Drop	—	—	Inactive
	Multicast		—	—	Inactive
	Unicast		—	—	Inactive
F1/0/4	Broadcast	Drop	—	—	Inactive
	Multicast		—	—	Inactive
	Unicast		—	—	Inactive
T1/0/5	Broadcast	Drop	—	—	Inactive
	Multicast		—	—	Inactive
	Unicast		—	—	Inactive
T1/0/6	Broadcast	Drop	—	—	Inactive
	Multicast		—	—	Inactive
	Unicast		—	—	Inactive

Figure 9-65 Storm Control (Level Type and PPS)

In the section of **Storm Control Polling Settings**, you can configure the following parameters.

Parameter	Overview
Polling Interval	Enter the value regarding a polling interval to use. The range is from 5 to 600 (seconds). By default, the value is 5 (seconds).
Shutdown Retries	Enter the value regarding the number of shutdown-retrials. The range is from 0 to 360. By default, the value is 3. If you set the Unlimited option to on, this function becomes disabled.

Click **Apply** to reflect the change.

In the section of **Storm Control Port Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Type	Choose the storm-attack type to control it. The options available are Broadcast , Multicast and Unicast . If you configure Shutdown as an action, unicast refers to (or means) both known and unknown unicast packets. If the number of known and unknown unicast packets reaches the threshold specified, the port becomes shutdown. Other than that, unicast refers to unknown unicast packets.
Action	Choose an action to do. The options available are as follows. <ul style="list-style-type: none"> • None - Does not filter storm packets. • Shutdown - Shutdowns a port when reaching the value, which is specified for the rising threshold. • Drop - Drops the packets, which exceed the high threshold.
Level Type	Choose the level-type option. The options available are PPS (Packets Per Second), Kbps and Level .
PPS Rise	Enter the value of PPS rise. This option specifies the upper rate of the packet count per second. The range is from 1 to 255,000 (packets) per second. If you do not specify the value of PPS low, the value equivalent to 80% of the rising-PPS specified becomes the default value.
PPS Low	Enter the value of PPS low. This option specifies the low rate of the packet-count per second. The range is from 1 to 255,000 (packets). If you do not specify the value of PPS low, the value equivalent to 80% of the rising-PPS specified becomes the default value.

Click **Apply** to reflect the change.

If you choose **Kbps** from **Level Type**, the following window is displayed.

Storm Control

Storm Control Trap Settings
Trap State: **None** [Apply]

Storm Control Polling Settings
Polling Interval (0-600): **5** [ms] Shutdown Polling (0-360): **5** [ms] ☐ Inhibit [Apply]

Storm Control Port Settings
From Port: **F1/0/1** To Port: **F1/0/1** Type: **Broadcast** Action: **Drop** Level Type: **PPS** PPS Rise (0-1488100): **100** PPS Low (0-1488100): **100** [Apply]

Total Entries: 18

Port	Storm	Action	Threshold	Current	State
F1/0/1	Broadcast	Drop	100	0	Inactive
	Multicast		100	0	Inactive
	Unicast		100	0	Inactive
F1/0/2	Broadcast	Drop	100	0	Inactive
	Multicast		100	0	Inactive
	Unicast		100	0	Inactive
F1/0/3	Broadcast	Drop	100	0	Inactive
	Multicast		100	0	Inactive
	Unicast		100	0	Inactive
F1/0/4	Broadcast	Drop	100	0	Inactive
	Multicast		100	0	Inactive
	Unicast		100	0	Inactive
T1/0/5	Broadcast	Drop	100	0	Inactive
	Multicast		100	0	Inactive
	Unicast		100	0	Inactive
T1/0/6	Broadcast	Drop	100	0	Inactive
	Multicast		100	0	Inactive
	Unicast		100	0	Inactive

Figure 9-66 Storm Control (Level Type, Kbps)

You can configure the following additional parameters.

Parameter	Overview
KBPS Rise	Enter the value of Kbps rise. This option specifies the rising-threshold with the rate (the number of kilo-bits per second). The rate receives traffics on the port. The range is from 1 to 2,147,483,647 (Kbps).
KBPS Low	Enter the value of Kbps low. This option specifies the low threshold on the rate (the number of kilo-bits per second). The rate receives traffics on the port. The range is from 1 to 2,147,483,647 (Kbps). If you do not specify the value of Kbps low, the value equivalent to 80% of the rising Kbps specified becomes the default value.

Click **Apply** to reflect the change.

If you choose **Level** from **Level Type**, the following window is displayed.

Storm Control

Storm Control Trap Settings

Trap State: None Apply

Storm Control Polling Settings

Polling Interval (5-600): 5 sec Shutdown Retries (0-300): 0 times ☐ Infinite Apply

Storm Control Port Settings

From Port: F1/0/1 To Port: F1/0/1 Type: Broadcas Action: Drop Level Type: PPS PPS Rise (5-1488100): PPS Low (0-1488100): Apply

Total Entries: 10

Port	storm	Action	Threshold	Current	State
F1/0/1	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
F1/0/2	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
F1/0/3	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
F1/0/4	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
Te1/0/5	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
Te1/0/6	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive

Figure 9-67 Storm Control (Level Type, Level)

You can configure the following additional parameters.

Parameter	Overview
Level Rise	Enter the value of level rise. This option specifies the rising threshold (with a percent) to all the bandwidth per port, which receives traffics. The range is from 1 to 100 (%).
Level Low	Enter the value of level low. This option specifies the low threshold (with a percent) to all the bandwidth per port, which receives traffics. The range is from 1 to 100 (%). If you do not specify the value of level low, the value equivalent to 80% of the specified rising-level becomes the default value.

Click **Apply** to reflect the change.

9.16 SSH (Secure Shell)

9.16.1 SSH Global Settings

Use the following window to implement the global settings, which is associated with the SSH function, and display its settings.

Choose **Security > SSH > SSH Global Settings** to display the following window.

Figure 9-68 SSH Global Settings

In the section of **SSH Global Settings**, you can configure the following parameters.

Parameter	Overview
IP SSH Server State	This parameter enables or disables to set an SSH server to global.
IP SSH Service Port	Enter the SSH service port-number (value) to use. The range is from 1 to 65,535. By default, the value is set to 22.
Authentication Timeout	Enter the value of an authentication time-out. The range is from 30 to 600 (seconds). By default, the value is set to 120 (seconds).
Number of Authentication Retries	Enter the value regarding the number of authentication-retries. The range is from 1 to 32. By default, the value is set to 3.

Click **Apply** to reflect the change.

9.16.2 Host Key

Use the following window to implement the settings on SSH host key and display its settings.

Choose **Security > SSH > Host Key** to display the following window.

Figure 9-69 Host Key

In the section of **Host Key Management**, you can configure the following parameters.

Parameter	Overview
Encryption Type	Choose the encryption-key type to use. The options available are RSA (Rivest Shamir Adleman) key-type and DSA (Digital Signature Algorithm) key type.
Key Module	Choose the value of a key module. The values to choose are those bits: 360, 512, 768, 1024 and 2048 . Choose the value of the key module.

Click **Generate** to generate a host key based on the content selected.

Click **Delete** to delete a host key based on the content selected.

In the section of **Host key**, you can configure the following parameter.

Parameter	Overview
Encryption Key Type	Choose the encryption-key type you use. The options available are RSA and DSA .

9.16.3 SSH Server Connection

Use the following window to display the SSH server connection table and its information.

Choose **Security > SSH > SSH Server Connection** to display the following window.



The image shows a software window titled "SSH Server Connection". Inside the window, there is a section labeled "SSH Table". Below this label, it says "Total Entries: 0". Underneath, there is a table with five columns: "Session ID", "Version", "Cipher", "User ID", and "Client IP Address". The table is currently empty.

Session ID	Version	Cipher	User ID	Client IP Address
------------	---------	--------	---------	-------------------

Figure 9-70 SSH Server Connection

9.16.4 SSH User Settings

Use the following window to implement the SSH user settings and display its settings.

Choose **Security > SSH > SSH User Settings** to display the following window.

Figure 9-71 SSH User Settings

In the section of the **SSH User Settings**, you can configure the following parameters.

Parameter	Overview
User Name	Enter the user-name of an SSH user account. The number of characters for this can be up to 32.
Authentication Method	Choose the SSH authentication method. The options available are Password , Public Key and Host-based .
Key File	If you choose Public Key or Host-based , enter the public key. The number of characters for this can be up to 779.
Host Name	If you choose a host-based, enter its host-name. The number of characters can be up to 255 for the name.
IPv4 Address	If you choose a host-based, enter an IPv4 address of an SSH user-account.
IPv6 Address	If you choose a host-based, enter an IPv6 address of an SSH user-account.

Click **Apply** to add a new entry.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

9.17 SSL (Secure Sockets Layer)

9.17.1 SSL Global Settings

Use the following window to implement the global settings, which is associated with the SSL function and to display its settings.

Choose **Security > SSL > SSL Global Settings** to display the following window.

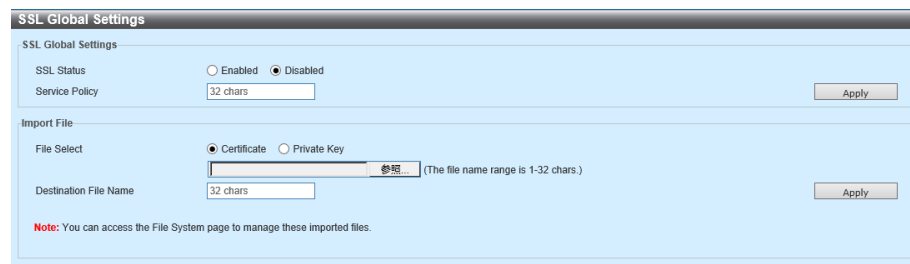


Figure 9-72 SSL Global Settings

In the section of **SSL Global Settings**, you can configure the following parameters.

Parameter	Overview
SSL Status	This parameter enables or disables to set the SSL function to global.
Service Policy	Enter the name of the service policy. The number of characters for the name can be up to 32.

Click **Apply** to reflect the change.

In the section of **Import File**, you can configure the following parameters.

Parameter	Overview
File Select	Select a file type to upload. The options available are Certificate and Private Key . After you select the file type, browse the file located on a local computer by clicking the Browser button.
Destination File Name	Enter the destination file-name you use. The number of characters for the name can be up to 32.

Click **Apply** to import an SSL file.

9.17.2 Crypto PKI Trustpoint

Use the following window to implement the settings on the SSL encrypted PKI trustpoint and display its settings. PKI stands for Public Key Infrastructure.

Choose **Security > SSL > Crypto PKI Trustpoint** to display the following window.

Figure 9-73 Crypto PKI Trustpoint

In the section of **Crypto PKI Trustpoint**, you can configure the following parameters.

Parameter	Overview
Trustpoint	Enter the name of the trustpoint, which is associated with a certificate and key-pair imported. The number of characters for the name can be up to 32.
File System Path	Enter a file system path of a certificate and a key pair.
Password	Enter an encrypted password-phrase to use for decrypting when a private key is imported. The number of characters for the password-phrase can be up to 64. If you do not specify the password phrase, the null character-string must be used.
TFTP Server Path	Enter a TFTP server path.
Type	Choose a certificate type to be imported. The options available are as follows. <ul style="list-style-type: none"> • Both - Imports a CA certificate, a local certificate, and a key pair; CA stands for certificate authority. • CA - Imports CA certificate. • Local - Imports a local certificate and a key pair.

Click **Apply** to add a new entry.

Click **Find** to search and display the entries based on the search condition specified.

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

9.17.3 SSL Service Policy

Use the following window to implement the settings on the SSL service policy and display its settings.

Choose **Security > SSL > SSL Service Policy** to display the following window.

The screenshot shows the 'SSL Service Policy' configuration window. It includes a 'Policy Name' field (32 chars), a 'Version' dropdown (TLS 1.0, TLS 1.1, TLS 1.2), a 'Session Cache Timeout (60-86400)' field (600 sec), and a 'Secure Trustpoint' field (32 chars). Below these is a list of cipher suites with checkboxes. At the bottom, there is a table with columns: Policy Name, Version, Cipher Suites, Session Cache Timeout (sec), Secure Trustpoint, and a 'Total Entries: 0' row. There are 'Apply' and 'Find' buttons.

Figure 9-74 SSL Service Policy

In the section of the **SSL Service Policy**, you can configure the following parameters.

Parameter	Overview
Policy Name	Enter the name of the SSL service policy. The number of characters for the name can be up to 32.
Version	Choose a version of Transport Layer Security (TLC). The options available are TLS 1.0 , TLS 1.1 and TLS 1.2 .
Session Cache Time-out	Enter the time-out value of a session cache. The range is from 60 to 86,400 (seconds). By default, the value is set to 600 (seconds).
Secure Trust Point	Enter the name of the secure trust point. The number of characters for the name can be up to 32.
Encryption Sweet	Choose the cipher suite to associate with this profile.

Click **Apply** to add a new entry.

Click **Find** to search and display the entries based on the search condition specified.

Click **Edit** to edit the configuration of the entry specified.

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

10 OAM (Operations, Administration & Management)

10.1 Cable Diagnostics

Use the following window to start the cable diagnostic test for the port specified and display the result.

Choose **OAM > Cable Diagnostics** to display the following window.

Port	Type	Link Status	Test Result	Cable Length (M)	
F11/0/1	5GBASE-T	Link Up	-	-	Clear
F11/0/2	5GBASE-T	Link Down	-	-	Clear
F11/0/3	5GBASE-T	Link Down	-	-	Clear
F11/0/4	5GBASE-T	Link Down	-	-	Clear
Te1/0/5	10GBASE-R	Link Down	-	-	Clear
Te1/0/6	10GBASE-R	Link Down	-	-	Clear

Figure 10-1 Cable Diagnostics

In the section of **Cable Diagnostics**, you can configure the following parameter.

Parameter	Overview
From Port/ To Port	Choose the port you use.

Click **Test** to start the cable diagnostic test on the port(s) specified.

Click **Clear All** to clear all the results regarding the cable diagnostic.

Click **Clear** to clear the result for the cable-diagnostic of the port specified.

10.2 DDM (Digital Diagnostic Monitoring)

10.2.1 DDM Settings

Use the following window to implement the settings on the global settings (which is associated with a DDM function) and DDM shutdown of the port specified, and to display the settings.

Choose **DDM > DDM Settings** to display the following window.

Figure 10-2 DDM Settings

In the section of **DDM Global Settings**, you can configure the following parameters.

Parameter	Overview
Transceiver Monitoring Traps Alarm	This parameter enables and disables the transmission of the transceiver monitoring traps alarm.
Transceiver Monitoring Traps Warning	This parameter enables and disables the transmission of the transceiver monitoring traps warning.

Click **Apply** to reflect the change.

In the section of **DDM Shutdown Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
State	This parameter enables or disables a DDM function on the port specified.
Shutdown	Choose the shutdown operation. The value and option to choose are as follows. <ul style="list-style-type: none">• Alarm - This option allows you to shutdown a port when the value exceeds the range of the alarm threshold configured.• Warning - This option allows you to shutdown a port when the value exceeds the range of the warning threshold configured.• None - This option does not make a port shutdown regardless of when the value exceeds the threshold-range. This is the default option.

Click **Apply** to reflect the change.

10.2.2 DDM Temperature Threshold Settings

Use the following window to implement the settings on the DDM temperature threshold of the port specified and display its settings.

Choose **DDM > DDM Temperature Threshold Settings** to display the following window.

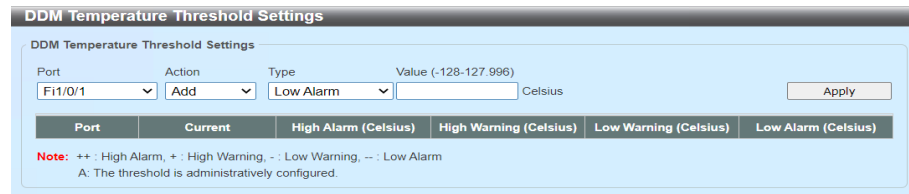


Figure 10-3 DDM Temperature Threshold Settings

In the section of **DDM Temperature Threshold Settings**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
Action	Choose an action to execute. The options available are Add and Delete .
Type	Choose the type of the temperature threshold. The options available are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold. The range is from -128 to 127.996.

Click **Apply** to reflect the change.

10.2.3 DDM Voltage Threshold Settings

Use the following window to implement the DDM voltage threshold settings on the port specified and display its settings.

Choose **DDM > DDM Voltage Threshold Settings** to display the following window.

Figure 10-4 DDM Voltage Threshold Settings

In the section of **DDM Voltage Threshold Settings**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
Action	Choose an action to execute. The options available are Add and Delete .
Type	Choose the type of the voltage threshold. The options available are Low Alarm , Low Warning , High Alarm and High Warning .
Value	Enter the threshold; its range is from 0 to 6.55 (volts).

Click **Apply** to reflect the change.

10.2.4 DDM Bias Current Threshold Settings

Use the following window to implement the settings on the DDM bias current threshold of the port specified and display its settings.

Choose **DDM > DDM Bias Current Threshold Settings** to display the following window.

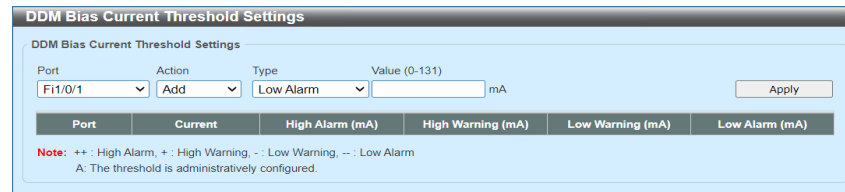


Figure 10-5 DDM Bias Current Threshold Settings

In the section of the settings on **DDM Bias Current Threshold**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
Action	Choose an action to execute. The options available are Add and Delete .
Type	Choose a type of a bias current threshold. The options available are Alarm lower-limit , Alarm Upper-limit and Warning Upper-limit .
Value	Enter the threshold; its range is from 0 to 131 (mA).

Click **Apply** to reflect the change.

10.2.5 DDM TX Power Threshold Settings

Use the following window to implement the settings on DDM TX power threshold of the port specified and display its settings.

Choose **DDM > DDM TX Power Threshold Settings** to display the following window.

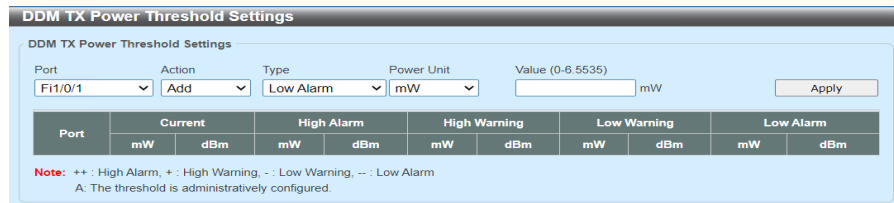


Figure 10-6 DDM TX Power Threshold Settings

In the section of **DDM TX Power Threshold Settings**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
Action	Choose the action you perform. The options available are Add and Delete .
Type	Choose the threshold type of a transmission power. The options available are Low Alarm , Low Warning , High Alarm and High Warning .
Power Unit	Choose the power unit. The options available are mW and dBm .
Value	Enter the threshold. <ul style="list-style-type: none"> If you specify the threshold with mW unit, the range is from 0 to 6.5535 (mW). If you specify the threshold with dBm unit, the range is from -40 to 8.1647 (dBm).

Click **Apply** to reflect the change.

10.2.6 DDM RX Power Threshold Settings

Use the following window to implement the settings on the DDM RX power threshold on the port specified and to display its settings.

Choose **DDM > DDM RX Power Threshold Settings** to display the following window.

Figure 10-7 DDM RX Power Threshold Settings

In the section of **DDM RX Power Threshold Settings**, you can configure the following parameters.

Parameter	Overview
Port	Choose the port you use.
Action	Choose an action to be executed. The options available are Add and Delete .
Type	Choose the type of RX power threshold. The options available are Low Alarm , Low Warning , High Alarm and High Warning .
Power Unit	Choose the power unit. The options available are mW and dBm .
Value	Enter the threshold. <ul style="list-style-type: none"> When specifying the threshold in mW, the range is from 0 to 6.5535 (mW). When specifying the threshold in dBm, the range is from -40 to 8.1647 (dBm).

Click **Apply** to reflect the change.

10.2.7 DDM Status Table

Use the following window to display the DDM status table and its information.

Choose **DDM > DDM Status Table** to display the following window.

DDM Status Table

DDM Status Table

Total Entries: 0

Port	Temperature (Celsius)	Voltage (V)	Bias Current (mA)	TX Power		RX Power	
				mW	dBm	mW	dBm
Note: ++ : High Alarm, + : High Warning, - : Low Warning, -- : Low Alarm							

Figure 10-8 DDM Status Table

11 Monitoring

11.1 Utilization

11.1.1 Port Utilization

Use the following window to display a table of port-utilization and its information.

Choose **Monitoring > Utilization > Port Utilization** to display the following window.

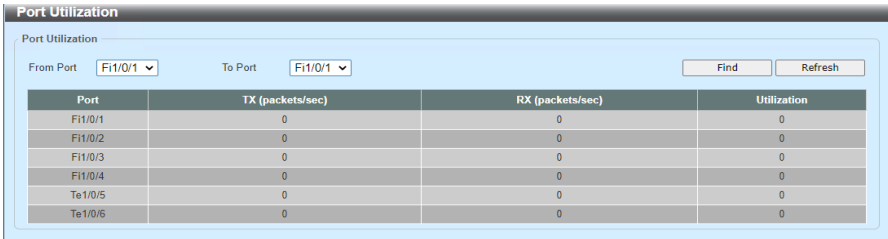


Figure 11-1 Port Utilization

In the section of the **Port Utilization**, you can configure the following parameter.

Parameter	Overview
From Port/ To Port	Choose the port you use.

Click **Find** to display the port utilization information regarding the specified port(s).

Click **Refresh** to refresh the information displayed in the table above.

11.2 Statistics

11.2.1 Port

Use the following window to display the statistics for sending and receiving ports and its information.

Choose **Monitoring > Statistics > Port** to display the following window.

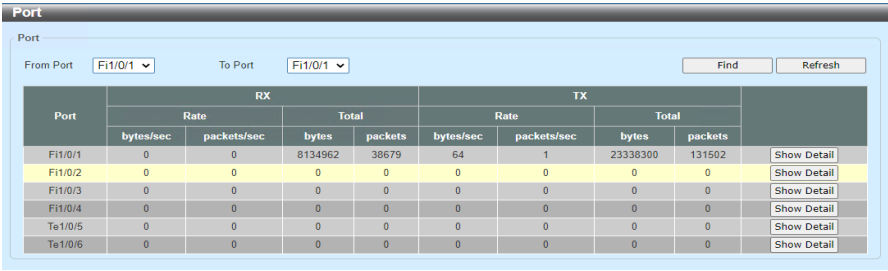


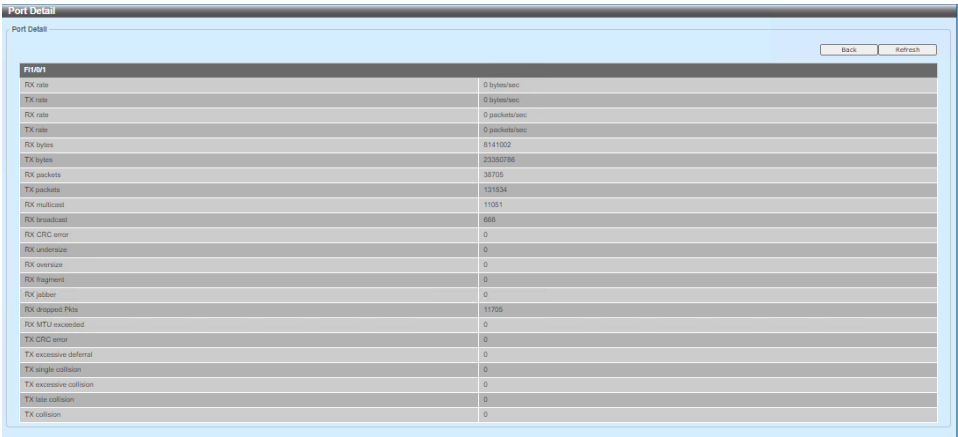
Figure 11-2 Port

In the section of **Port**, you can configure the following parameter.

Parameter	Overview
From Port/ To Port	Choose the port you use.

- Click **Find** to display the statistics information about the port specified.
- Click **Refresh** to refresh the information displayed in a table.
- Click **Show Detail** to display the details about the entry.

Click **Show Detail** to display the following window.



The screenshot shows a window titled "Port Detail" with a sub-header "Port Detail". In the top right corner, there are two buttons: "Back" and "Refresh". The main content is a table with two columns: the first column lists various network statistics, and the second column shows their corresponding values.

F1/0/1	
RX rate	0 bytes/sec
TX rate	0 bytes/sec
RX rate	0 packets/sec
TX rate	0 packets/sec
RX bytes	8141002
TX bytes	23300796
RX packets	38705
TX packets	131534
RX multicast	11051
RX broadcast	668
RX CRC error	0
RX undersize	0
RX oversize	0
RX fragment	0
RX jabber	0
RX dropped Pkts	11705
Rx MTU exceeded	0
TX CRC error	0
TX excessive deferral	0
TX single collision	0
TX excessive collision	0
TX late collision	0
TX collision	0

Figure 11-3 Port (Show Detail.)

Click **Back** to return to the previous window.

Click **Refresh** to refresh the information displayed in a table.

11.2.2 Interface Counters

Use the following window to display the interface-counter statistics and its information.

Choose **Monitoring > Statistics > Interface Counters** to display the following window.

Port	InOctets	InUcastPkts	InMcastPkts	InBeastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBeastPkts	Show Errors
Fi1/0/1	8149161	27018	11055	668	23364359	131582	0	1	Show Errors
Fi1/0/2	0	0	0	0	0	0	0	0	Show Errors
Fi1/0/3	0	0	0	0	0	0	0	0	Show Errors
Fi1/0/4	0	0	0	0	0	0	0	0	Show Errors
Te1/0/5	0	0	0	0	0	0	0	0	Show Errors
Te1/0/6	0	0	0	0	0	0	0	0	Show Errors

Figure 11-4 Interface Counters

In the section of the **Interface Counters**, you can configure the following parameter.

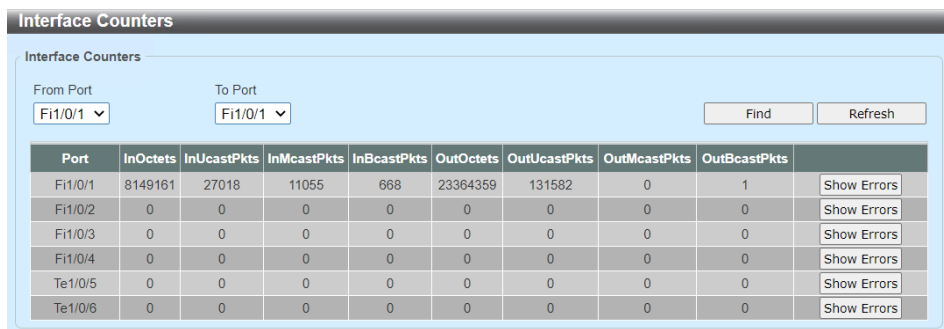
Parameter	Overview
From Port/ To Port	Choose the port you use.

Click **Find** to display the interface counter regarding the specified port(s).

Click **Refresh** to refresh the information displayed in a table.

Click **Show Errors** to display error details on this entry.

Click **Show Errors** to display the following window.



The screenshot shows a window titled "Interface Counters". Inside, there are two dropdown menus labeled "From Port" and "To Port", both set to "Fi1/0/1". To the right of these are "Find" and "Refresh" buttons. Below is a table with 9 columns: Port, InOctets, InUcastPkts, InMcastPkts, InBcastPkts, OutOctets, OutUcastPkts, OutMcastPkts, and OutBcastPkts. The table has 6 rows of data. Each row has a "Show Errors" button to its right.

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	Show Errors
Fi1/0/1	8149161	27018	11055	668	23364359	131582	0	1	Show Errors
Fi1/0/2	0	0	0	0	0	0	0	0	Show Errors
Fi1/0/3	0	0	0	0	0	0	0	0	Show Errors
Fi1/0/4	0	0	0	0	0	0	0	0	Show Errors
Te1/0/5	0	0	0	0	0	0	0	0	Show Errors
Te1/0/6	0	0	0	0	0	0	0	0	Show Errors

Figure 11-5 Interface Counters (Show Errors.)

Click **Back** to return to the previous window.

Click **Refresh** to refresh the information displayed in a table.

11.2.3 Counters

Use the following window to display and clear the link-change counters of the port specified.

Choose **Monitoring > Statistics > Counters** to display the following window.

The screenshot shows a window titled "Counters". Inside, there are two dropdown menus labeled "From Port" and "To Port", both set to "Ft1/0/1". To the right of these are four buttons: "Find", "Refresh", "Clear", and "Clear All". Below the buttons is a table with three columns: "Port", "linkChange", and a button labeled "Show Detail". The table contains six rows of data.

Port	linkChange	Show Detail
Ft1/0/1	3	Show Detail
Ft1/0/2	0	Show Detail
Ft1/0/3	0	Show Detail
Ft1/0/4	0	Show Detail
Te1/0/5	0	Show Detail
Te1/0/6	0	Show Detail

Figure 11-6 Counters

In the section of **Counters**, you can configure the following parameter.

Parameter	Overview
From Port/ To Port	Choose the port you use.

Click **Find** to display the information on the link-change counters regarding the specified port(s).

Click **Refresh** to refresh the information displayed in the table above.

Click **Clear** to clear the information on the link-change counters regarding the specified port.

Click **Clear ALL** to clear information on all the link change counters.

Click **Show Detail** to display details on the entry.

Click **Show Detail** to display the following window.

[illegible]

Figure 11-7 Counters (Show Detail.)

Click **Back** to return to the previous window.

Click **Refresh** to refresh the information displayed in the table above.

11.3 Mirror Settings

Use the following window to implement the settings on a port mirror and display its settings.

Choose **Monitoring > Mirror Settings** to display the following window.

The screenshot shows the 'Mirror Settings' window. At the top, there's a title bar 'Mirror Settings'. Below it, the 'RSPAN VLAN Settings' section includes a 'VID List (2-4094)' text box containing '3 or 2-5', with 'Add' and 'Delete' buttons. The 'Mirror Settings' section features a 'Session Number' dropdown set to '1'. It has two main columns: 'Destination' and 'Source'. Each column has a 'Port' checkbox and a dropdown menu. The 'Port' dropdowns are set to 'F11/0/1'. There are also 'From Port' and 'To Port' dropdowns, both set to 'F11/0/1', and a 'Frame Type' dropdown set to 'Both'. 'Add' and 'Delete' buttons are at the bottom right. The 'Mirror Session Table' section has a 'All Session' dropdown and a 'Find' button. Below this is a table with two columns: 'Session Number' and 'Session Type'.

Figure 11-8 Mirror Settings

In the section of **RSPAN VLAN Settings**, you can configure the following parameter.

Parameter	Overview
VID List	Enter the RSPAN VLAN ID you use. You can enter its consecutive VLAN IDs, by delimiting with a comma, or you can enter the range of VLAN IDs by delimiting with a hyphen. The range is from 2 to 4,094.

Click **Apply** to add the new entry.

Click **Delete** to delete entries based on the information specified.

In the section of **Mirror Settings**, you can configure the following parameters.

Parameter	Overview
Session Number	Choose the mirror-session number of this entry. The range of the number is from 1 to 4.
Destination	<p>Choose and configure the destination settings on this port-mirror entry. Choose Port or Remote VLAN of the destination.</p> <ul style="list-style-type: none"> • Port - Choose the destination port-number. • Remote VLAN - Choose the destination port-number. • Enter VID in the entry field displayed. The range of VID is from 2 to 4,094.
Source	<p>Choose and configure the source settings on this port-mirror entry. Choose Port, ACL or Remote VLAN of the source.</p> <ul style="list-style-type: none"> • Port - Choose the range of the port-number by using From Port to To Port. Choose a Frame Type. • The options to choose from the frame-type is as follows. <ul style="list-style-type: none"> oBoth - Traffics of both reception and transmission direction are mirrored. Traffics in both incoming and outgoing directions are mirrored. oReception (RX) - traffics in only the incoming direction are mirrored. oTransmission (TX) - traffics in only the outgoing direction are mirrored. oCPU RX - Monitors CPU RX traffics. • ACL - Enter the ACL Name in the entry field displayed. The number of characters for the name can be up to 32. • Remote VLAN - Enter a remote VID in the entry field displayed. The range is from 2 to 4,094.

Click **Apply** to add a new entry.

Click **Delete** to delete entries based on the information specified.

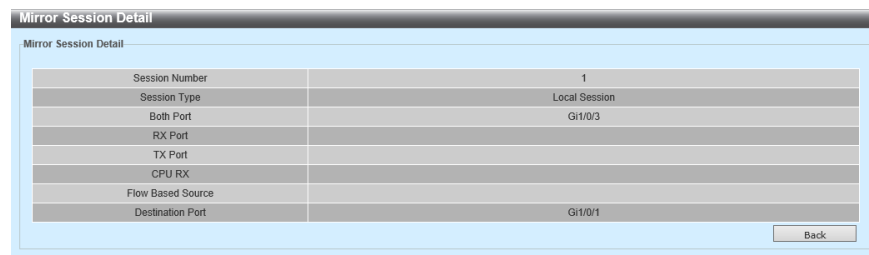
In the section of **Mirror Session Table**, you can configure the following parameter.

Parameter	Overview
Session Type	Choose the mirror-session type of information to be displayed. The options available are All Sessions , Session Number , Remote Session and Local Session . If you choose the Session Number option, choose the session number from the drop-down menu. The range is from 1 to 4.

Click **Find** to search and display the entries based on the search condition specified.

Click **Show Detail** to display details on the entry.

Click **Show Detail** to display the following window.



The screenshot shows a window titled "Mirror Session Detail". Inside, there is a table with the following data:

Mirror Session Detail	
Session Number	1
Session Type	Local Session
Both Port	Gi1/0/3
RX Port	
TX Port	
CPU RX	
Flow Based Source	
Destination Port	Gi1/0/1

At the bottom right of the window, there is a "Back" button.

Figure 11-9 Mirror Session Detail (Show Detail.)

Click **Back** to return to the previous window.

11.4 Device

Use the following window to display the value of the current temperature measurement, fan condition and power-module state in a switch.

Choose **Monitoring > Device Environment** to display the following window.

Device Environment		
Detail Temperature Status		
Unit	Temperature Description/ID	Current/Threshold Range
1	Thermal Sensor/1	39C/77C
	Thermal Sensor/2	37C/74C
Status code: * temperature is out of threshold range		
Detail Power Status		
Unit	Power Module	Power Status
Power 1	In-operation	

Figure 11-10 Device Environment

12 ECO Mode

12.1 Power-Saving

Use the following window to implement the settings on the power-saving and display its settings.

Choose **ECO Mode > Power-Saving** to display the following window.

Port	Link	Type	Mode	Power Saving Mode
Fi1/0/1	Up	5GT	Auto(1GF)	Disabled
Fi1/0/2	Down	5GT	Auto	Disabled
Fi1/0/3	Down	5GT	Auto	Disabled
Fi1/0/4	Down	5GT	Auto	Disabled
Te1/0/5	Down	10GT	Auto	Disabled
Te1/0/6	Down	10GT	Auto	Disabled

Figure 12-1 Power-Saving

In the section of **Power-Saving Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
Power-Saving Mode	<div>Choose the power-saving mode to use on the port specified. The options available are as follows.</div> <ul style="list-style-type: none">• Disabled - Disables the power-saving function.• Full - Uses the power-saving function, maximally.• Half - Uses half of the power-saving function.• This applies to all the cases; if the function is not used at all or is maximally used, normally.

Click **Apply** to reflect the change.

12.2 EEE (Energy Efficient Ethernet)

Use the following window to implement the settings on EEE of the port specified and display its settings.

Choose **ECO Mode > EEE** to display the following window.

Port	State
F11/0/1	Disabled
F11/0/2	Disabled
F11/0/3	Disabled
F11/0/4	Disabled
Te1/0/5	Disabled
Te1/0/6	Disabled

Figure 12-2 EEE

In the section of **EEE Settings**, you can configure the following parameters.

Parameter	Overview
From Port/ To Port	Choose the port you use.
State	This parameter enables or disables the EEE function on the port specified.

Click **Apply** to reflect the change.

13 Tool Bar

13.1 Save

13.1.1 Save Configuration

Use the following window to save the running configuration as the start-up configuration. Doing so prevents the loss of configuration during a power-failure.

Choose **Save > Save Configuration** in the tool-bar to display the following window.

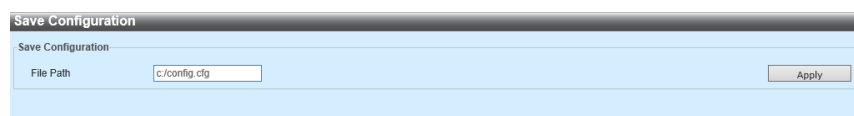


Figure 13-1 Save Configuration

In the section of **Save Configuration**, you can configure the following parameter.

Parameter	Overview
File Path	Enter a file-name and a path in the entry field displayed.

Click **Apply** to save the configuration.

13.2 Tool

13.2.1 Firmware Upgrade & Backup

13.2.1.1 Firmware Upgrade from HTTP (Servers)

Use the following window to upgrade firmware in a switch by using HTTP from a local PC.

Choose **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP** from the tool-bar to display the following window.

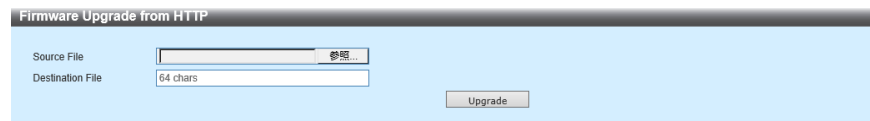


Figure 13-2 Firmware Upgrade from HTTP (Servers)

You can configure the following parameters.

Parameter	Overview
Source File	Click Browse to navigate to the location where a firmware file exists (on the local PC) for this upgrade.
Destination File	Enter the destination path and location in the switch where new firmware is stored (or saved). The number of characters for this field can be up to 64.

Click **Upgrade** to start upgrading.

13.2.1.2 Firmware Upgrade from TFTP

Use the following window to upgrade firmware in a switch from a TFTP server.

Choose **Tool > Firmware Upgrade & Backup > Firmware Upgrade from TFTP (Servers)** to display the following window.

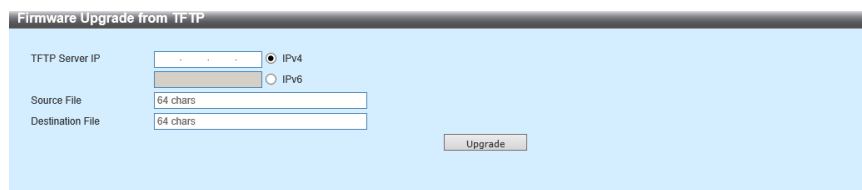


Figure 13-3 Firmware Upgrade from TFTP (Servers)

You can configure the following parameters.

Parameter	Overview
TFTP Server IP	Enter an IP address of a TFTP server. <ul style="list-style-type: none">• IPv4 - Choose and enter an IPv4 address of a TFTP server.• IPv6 - Choose and enter an IPv6 address of a TFTP server.• IPv6 - Choose and enter an IPv6 address of a TFTP server.
Source File	Enter the source file-name and path of a firmware file in a TFTP server. The number of characters for this field can be up to 64.
Destination File	Enter the destination path and location in the switch where new firmware is stored. The number of characters for this field can be up to 64.

Click **Upgrade** to start upgrading.

13.2.1.3 Firmware Upgrade from FTP Servers

Use the following window to upgrade firmware in a switch from an RCP server.

Choose **Tool >Firmware Upgrade & Backup > Firmware Upgrade from an FTP Server** on the tool-bar to display the following window.

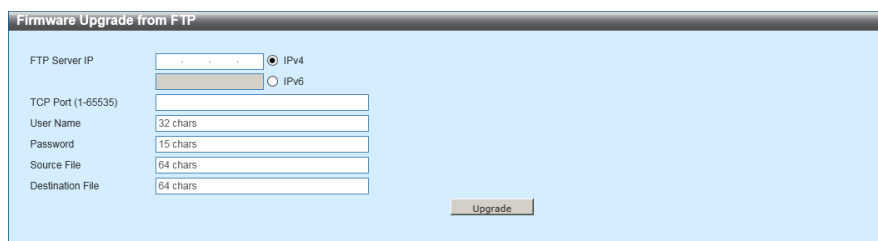


Figure 13-4 Firmware Upgrade from the FTP Server

You can configure the following parameters.

Parameter	Overview
FTP Server IP	Enter an IP address of the FTP server.
TCP Port (1-65535)	Enter the TCP port of the FTP connection.
Username	Enter the user-name of the FTP connection. The number of characters for the name can be up to 32.
Password	Enter the password of the FTP connection. The number of characters for the name can be up to 15.
Source File	Enter the path and name of a source file of the firmware file existing in an FTP server. The number of characters for this field can be up to 64.
Destination File	Enter the destination path and its location on the switch where new firmware is saved. The number of characters for this field can be up to 64.

Click **Upgrade** to start upgrading.

13.2.1.4 Firmware Upgrade from RCP

Use the following window to upgrade the firmware existing in a switch from an RCP server.

Choose **Tool > Firmware Upgrade and Backup > Firmware Upgrade from RCP (Servers)** to display the following window.

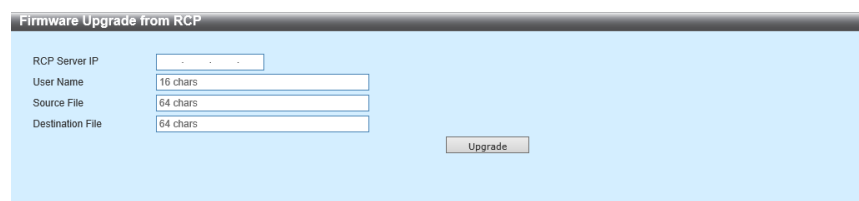


Figure 13-5 Firmware Upgrade from RCP (Servers)

You can configure the following parameters.

Parameter	Overview
RCP Server IP	Enter an IP address of one RCP server.
User Name	Enter a user-name of the RCP connection. The number of characters for the name can be up to 32.
Source File	Enter a source file-name and path of a firmware file in an RCP server. The number of characters for this field can be up to 64.
Destination File	Enter the destination path and location in the switch where new firmware is saved. The number of characters for this field can be up to 64.

Click **Upgrade** to start upgrading.

13.2.1.5 Firmware Backup to HTTP

Use the following window to save a backup copy of the firmware existing in a switch into a local PC with HTTP.

Choose **Tool > Firmware Upgrade & Backup > Firmware Backup to HTTP (Servers)** to display the following window.

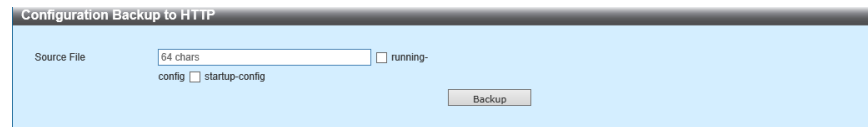


Figure 13-6 Firmware Backup to HTTP (Servers)

You can configure the following parameter.

Parameter	Overview
Source File	Enter the source file-name and path of a firmware file in a switch. The number of characters for this field can be up to 64.

Click the **Backup** button to start the backup.

13.2.1.6 Firmware Backup to TFTP

Use the following window to save the backup copy of firmware existing in a switch into a TFTP server.

Choose **Tool > Firmware Upgrade & Backup > Firmware Backup to TFTP (Servers)** on the tool-bar to display the following window.

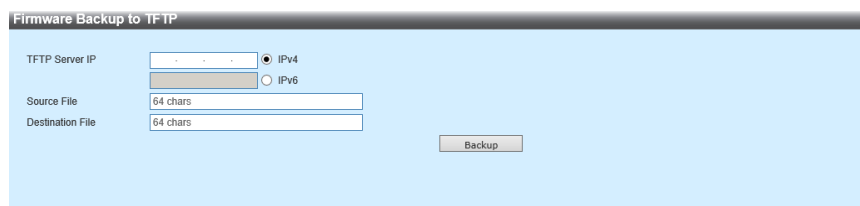


Figure 13-7 Firmware Upgrade from TFTP (Servers)

You can configure the following parameters.

Parameter	Overview
TFTP Server IP	Enter an IP address of a TFTP server. <ul style="list-style-type: none">• IPv4 - Choose and enter an IPv4 address of a TFTP server.• IPv6 - Choose and enter an IPv6 address of a TFTP server.
Source File	Enter the source file-name and path of a firmware file in a switch. The number of characters for this field can be up to 64.
Destination File	Enter the destination file-name and path of a firmware file to be backed up into a TFTP server. The number of characters for this field can be up to 64.

Click **Backup** to start performing a backup.

13.2.1.7 Firmware Backup to FTP Servers

Use the following window to save a backup copy of firmware in a switch into an RCP server.

Choose **Tool > Firmware Upgrade & Backup > Firmware Backup to an FTP Server** on the tool-bar to display the following window.

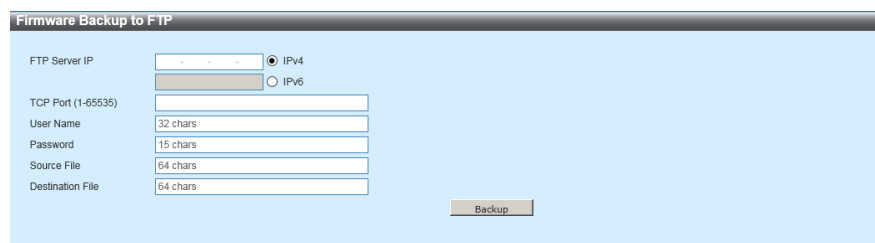


Figure 13-8 Firmware Backup to the FTP Server

You can configure the following parameters.

Parameter	Overview
FTP Server IP	Enter an IP address of an FTP server.
TCP Port (1-65535)	Enter the TCP port of the FTP connection.
Username	Enter the user-name of the FTP connection. The number of characters for the name can be up to 32.
Password	Enter the password of the FTP connection. The number of characters for the name can be up to 15.
Source File	Enter the path and name of a source file of the firmware file existing in a switch. The number of characters for this field can be up to 64.
Destination File	Enter the destination-file name and its path of a firmware file to be backed up into an FTP server. The number of characters for this field can be up to 64.

Click **Backup** to start making a backup.

13.2.1.8 Firmware Backup to RCP

Use the following window to save a backup copy of the firmware existing in a switch into an RCP server.

Choose **Tool > Firmware Upgrade & Backup > Firmware Backup to RCP (Servers)** on the tool-bar to display the following window.

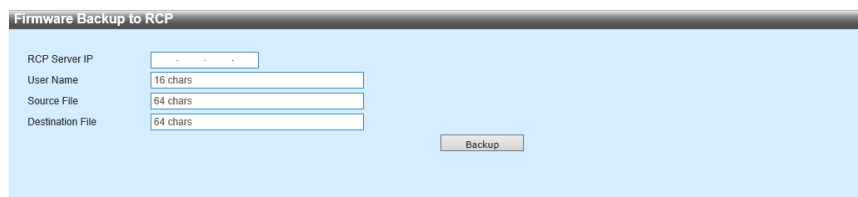


Figure 13-9 Firmware Backup to RCP (Servers)

You can configure the following parameters.

Parameter	Overview
RCP Server IP	Enter an IP address of the RCP server.
User Name	Enter the user-name of the RCP connection. The number of characters for the name can be up to 32.
Source File	Enter the source file-name and its path of a firmware file in a switch. The number of characters for this field can be up to 64.
Destination File	Enter a destination file-name and its path of a firmware file to be backed up into the RCP server. The number of characters for this field can be up to 64.

Click **Backup** to start performing a backup.

13.2.2 Configuration Restore & Backup

13.2.2.1 Configuration Restore from HTTP

Use the following window to restore the configuration in a switch by using HTTP from a local PC.

Choose **Tool > Configuration Restore & Backup > Configuration Restore from HTTP** from the tool-bar to display the following window.

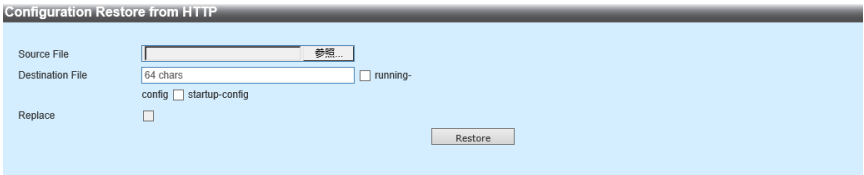


Figure 13-10 Configuration Restore from HTTP

You can configure the following parameters.

Parameter	Overview
Source File	Click Browse to move to the location where a configuration file (on the local PC) exists for the purpose of this restoration.
Destination File	Enter a destination path and a location in the switch where a configuration file is saved. The number of characters for this field can be up to 64. <ul style="list-style-type: none">If you choose the running-config option, the configuration file being executed in a switch is restored to be overwritten.If you choose the startup-config option, a start-up configuration file in a switch is restored to be overwritten.
Replace	If you choose this option, a configuration file in a switch is replaced by this file.

Click **Restore** to start restoring.

13.2.2.2 Configuration Restore from TFTP

Use the following window to recover the switch configuration from a TFTP server.

Choose **Tool > Configuration Recovery & Backup > Configuration Restore from TFTP (Servers)** to display the following window.

Figure 13-11 Configuration Restore from TFTP (Servers)

You can configure the following parameters.

Parameter	Overview
TFTP Server IP	Enter an IP address of a TFTP server. <ul style="list-style-type: none"> • IPv4 - Choose and enter an IPv4 address of a TFTP server. • IPv6 - Choose and enter an IPv6 address of a TFTP server.
Source File	Enter the source file-name and path of a configuration file in a TFTP server. The number of characters for this field can be up to 64.
Destination File	Enter a destination path and a location in the switch where a configuration file is saved. The number of characters for this field can be up to 64. <ul style="list-style-type: none"> • If you choose the running-config option, the configuration file being executed is restored to be overwritten. • If you choose the startup-config option, the start-up configuration file in a switch is restored to be overwritten.
Replace	If you use choose this option, a configuration file in a switch is replaced by this file.

Click **Restore** to start restoring.

13.2.2.3 Configuration Recovery from FTP Servers

Use the following window to recover the configuration of a switch from an FTP server.

Choose **Tool > Configuration Recovery & Backup > Configuration Recovery from an FTP Server** on the tool-bar to display the following window.

Figure 13-12 Configuration Recovery from the FTP Server

You can configure the following parameters.

Parameter	Overview
FTP Server IP	Enter an IP address of an FTP server.
TCP Port (1-65535)	Enter the TCP port of the FTP connection.
Username	Enter the username of the FTP connection. The number of characters for the name can be up to 32.
Password	Enter the password of the FTP connection. The number of characters for the name can be up to 15.
Source File	Enter the path and name of a source file of a configuration file existing in an FTP server. The number of characters for this field can be up to 64.
Destination File	<p>Enter the destination path and its location on the switch where a configuration file is saved. The number of characters for this field can be up to 64.</p> <ul style="list-style-type: none"> If you choose the running-config option, the configuration file, which is in progress of being executed by a switch, is recovered and overwritten. If you choose startup-config option, the start-up configuration file on a switch is recovered and overwritten.
Replace	If you choose this option, a configuration file on a switch is replaced using the file.

Click **Restore** to start restoring.

13.2.2.4 Configuration Restore from RCP

Use the following window to restore the configuration of a switch from an RCP server.

Choose **Tools > Configuration Restore & Backup > Configuration Restore from RCP (Servers)** from the tool-bar to display the following window.

Figure 13-13 Configuration Restore from RCP (Servers)

You can configure the following parameters.

Parameter	Overview
RCP Server IP	Enter an IP address of the RCP server.
User Name	Enter the user-name of the RCP connection. The number of characters for the name can be up to 32.
Source File	Enter the source file-name and path of a configuration file in an RCP server. The number of characters for this field can be up to 64.
Destination File	<p>Enter the destination path and location in a switch that saves a configuration file. The number of characters for this field can be up to 64.</p> <ul style="list-style-type: none"> If you choose the running-config option, the configuration file being executed in a switch is restored to be overwritten. If you choose the startup-config option, a start-up configuration file in a switch is restored to be overwritten.
Replace	If you choose this option, a configuration file in a switch is replaced by this file.

Click **Restore** to start restoring.

13.2.2.5 Configuration Backup to HTTP

Use the following window to save a backup copy of a switch configuration into a local PC by using HTTP.

Choose **Tools > Configuration Restore & Backup > Configuration Backup to HTTP (Servers)** from the tool-bar to display the following window.

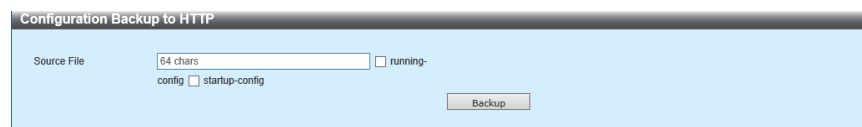


Figure 13-14 Configuration Backup to HTTP (Servers)

You can configure the following parameter.

Parameter	Overview
Source File	<p>Enter the source file-name and path of a configuration file in a switch. The number of characters for this field can be up to 64.</p> <ul style="list-style-type: none">• If you choose the running-config option, the configuration file being executed in a switch is backed up.• If you choose the startup-config option, a start-up configuration file in a switch is backed up.

Click **Backup** to start performing a backup.

13.2.2.6 Configuration Backup to TFTP

Use the following window to save a backup copy of a switch configuration into a TFTP server.

Choose **Tool > Configuration Restore & Backup > Configuration Backup to TFTP (Servers)** from the tool-bar to display the following window.

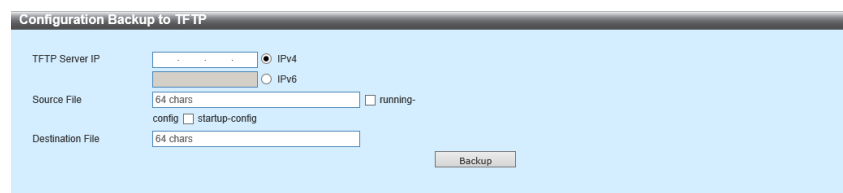


Figure 13-15 Configuration Backup to TFTP (Servers)

You can configure the following parameters.

Parameter	Overview
TFTP Server IP	Enter an IP address of a TFTP server. <ul style="list-style-type: none">• IPv4 - Choose and enter an IPv4 address of a TFTP server.• IPv6 - Choose and enter an IPv6 address of a TFTP server.
Source File	Enter the source file-name and path of a configuration file in a switch. The number of characters for this field can be up to 64. <ul style="list-style-type: none">• If you choose the running-config option, a backup of the configuration file being executed in a switch is created.• If you choose the startup-config option, a startup configuration file in a switch is backed up.
Destination File	Enter a destination path and a location on the TFTP server where a configuration file is saved. The number of characters for this field can be up to 64.

Click **Backup** to start performing a backup.

13.2.2.7 Configuration Backup to FTP Servers

Use the following window to save a backup copy of the switch configuration into an FTP server.

Choose **Tool > Configuration Recovery & Backup > Configuration Backup to an FTP Server** on the tool-bar to display the following window.

Figure 13-16 Configuration Backup to the FTP Server

You can configure the following parameters.

Parameter	Overview
FTP Server IP	Enter an IP address of an FTP server.
TCP Port (1-65535)	Enter the TCP port of the FTP connection.
Username	Enter the user-name of the FTP connection. The number of characters for the name can be up to 32.
Password	Enter the password of the FTP connection. The number of characters for the name can be up to 15.
Source File	Enter the source-file name and its path of a configuration file on a switch. The number of characters for this field can be up to 64. <ul style="list-style-type: none"> If you choose the running-config option, the configuration file, which is in progress of being executed by a switch, is backed up. If you choose startup-config option, the start-up configuration file on a switch is backed up.
Destination File	Enter the destination path and its location on the RCP server where a configuration file is saved. The number of characters for this field can be up to 64.

Click **Backup** to start making a backup.

13.2.2.8 Configuration Backup to RCP

Use the following window to save a backup copy of a switch configuration into an RCP server.

Choose **Tools > Configuration Restore & Backup > Configuration Backup to RCP** from the tool-bar to display the following window.

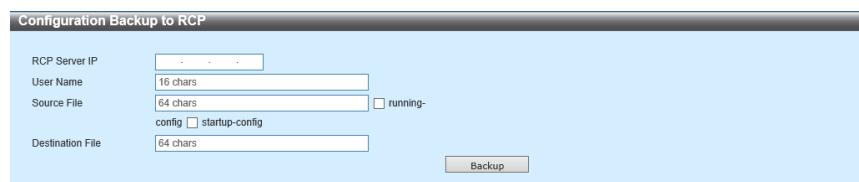


Figure 13-17 Configuration Backup to RCP

You can configure the following parameters.

Parameter	Overview
RCP Server IP	Enter an IP address of an RCP server.
User Name	Enter the user-name of the RCP connection. The number of characters for the name can be up to 32.
Source File	<div>Enter the source file-name and path of a configuration file in a switch. The number of characters for this field can be up to 64.</div> <ul style="list-style-type: none">• If you choose the running-config option, a backup of the configuration file being executed in a switch is made.• If you choose the startup-config option, a backup of a start-up configuration file in a switch is made.
Destination File	Enter a destination path and a location on the RCP server, where a configuration file is saved. The number of characters for this field can be up to 64.

Click **Backup** to start the backup.

13.2.3 Log Backup

13.2.3.1 Log Backup to HTTP

Use the following window to save system-logs of a switch or a copy of attack-logs into a local PC by using HTTP.

Choose **Tool > Log Backup > Log Backup to HTTP** in the tool-bar to display the following window.

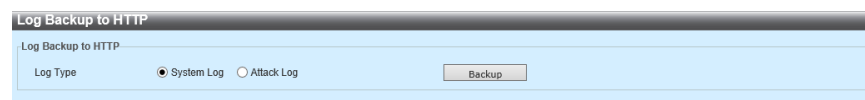


Figure 13-18 Log Backup to HTTP

You can configure the following parameter.

Parameter	Overview
Log Type	Choose the log-type, which is backed up to the local PC by using HTTP. <ul style="list-style-type: none">• System Log - Ensures to back up system-logs.• Attack Log - Ensures to back up attack-logs.

Click **Backup** to start performing a backup.

13.2.3.2 Log-backup to TFTP

Use the following window to save a copy of system-logs or attack-logs of a switch into a TFTP server.

Choose **Tools > Log Backup > Log Backup to TFTP (Servers)** from the tool-bar to display the following window.

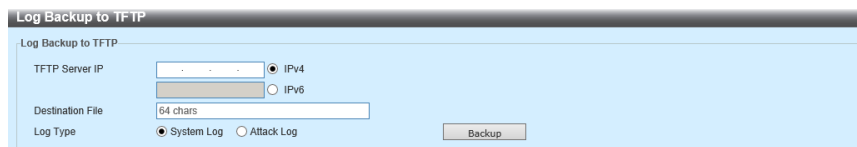


Figure 13-19 Log Backup to TFTP (Servers)

You can configure the following parameters.

Parameter	Overview
TFTP Server IP	Enter an IP address of a TFTP server. <ul style="list-style-type: none">• IPv4 - Choose and enter an IPv4 address of the TFTP server.• IPv6 - Choose and enter an IPv6 address of the TFTP server.
Destination File	Enter the destination path and location on the TFTP server where log files are saved. The number of characters for this field can be up to 64.
Log Type	Choose the log type, which is backed up to the TFTP server. <ul style="list-style-type: none">• System Log - The system log is backed up.• Attack Log - Ensures that the attack-logs are backed up.

Click **Backup** to start performing a backup.

13.2.3.3 Log Backup to RCP

Use the following to save a copy of system-logs or attack-logs on the switch into an RCP server.

Choose **Tools > Log Backup > Log Backup to RCP** from the tool-bar to display the following window.

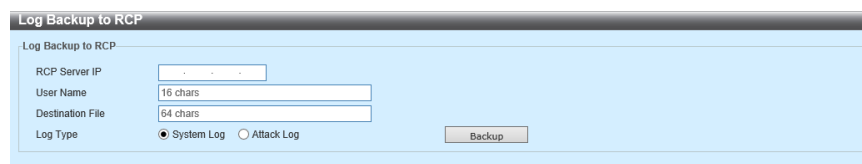


Figure 13-20 Log Backup to RCP

You can configure the following parameters.

Parameter	Overview
RCP Server IP	Enter an IP address of the RCP server.
User Name	Enter the user-name of the RCP connection. The number of characters for the name can be up to 32.
Destination File	Enter the destination path and location on the RCP server where a log-file is saved (or stored). The number of characters for this field can be up to 64.
Log Type	Choose the log type to save its backup into an RCP server. <ul style="list-style-type: none">• System Log - The system log is backed up.• Attack Log - The attack log is backed up.

Click **Backup** to start performing a backup.

13.2.4 Ping

Use the following window to ping a destination IPv4/IPv6 address or a domain-name and to perform a test for the network connection. The access list can be applied to a ping request.

Choose **Tool > Ping** in the tool-bar to display the following window.

Figure 13-21 Ping

In the section of **Ping Access Class**, you can configure the following parameters.

Parameter	Overview
ACL Name	Enter the ACL name you use. The number of characters for the name can be up to 32. Click Please Select to choose the existing ACL from a related list.
Action	Choose the action you take. The options available are Add and Clear .

Click **Apply** to use the access control list selected.

In the section of **IPv4 Ping**, you can configure the following parameters.

Parameter	Overview
Target IPv4 Address	Choose and enter a destination IPv4 address.
Domain Name	Choose and enter the name of a destination domain. The number of characters for this can be up to 255.
Number of Pings	Enter the number of Ping-trials on the IPv4 address, which is configured in this window. The range is from 1 to 255. If you check (or tick) the Unlimited , keep transmitting ICMP echo packets to the IPv4 address specified until a program stops.
Time-out	Enter the time-out time of Ping messages. If packets cannot detect an IPv4 address within the time specified, Ping packets are dropped (or removed). The range is from 1 to 99 (seconds).
Source IPv4 Address	Enter a source IPv4 address. If two or more IPv4 addresses are allocated to a switch, you can enter one of them. The IPv4 address entered is used as the source IPv4 address of packets, which are transmitted to a remote host.

Click **Start** to start the IPv4 Ping.

In the section of **IPv6 Ping**, you can configure the following parameters.

Parameter	Overview
Target IPv6 Address	Choose and enter a destination IPv6 address.
Domain Name	Choose and enter the name of a destination domain. The number of characters for this can be up to 255.
Number of Pings	Enter the number of Ping-trials in the IPv6 address, which is configured in this window. The range is from 1 to 255. If you check (or tick) the Unlimited check-box, keep transmitting ICMP echo packets to the IPv6 address specified until a program stops.
Time-out	Enter the time-out time for a Ping message. If packets cannot detect an IPv6 address within the time specified, Ping packets are dropped (or removed). The range is from 1 to 99 (seconds).
Source IPv6 Address	Enter a source IPv6 address. If two or more IPv6 addresses are allocated to a switch, you can enter one of them. The IPv6 address entered is used as the source IPv6 address of packets, which are transmitted to a remote host.

Click **Start** to start the IPv6 Ping.

Choose and enter the **IPv4 Ping** parameter, and then click **Start** to display the following window.

The screenshot shows the 'Ping' window with the 'IPv4 Ping Result' section expanded. It displays the following text:

```
[1] Reply from 172.16.254.254, times=10ms
[2] Reply from 172.16.254.254, times<10ms
[3] Reply from 172.16.254.254, times<10ms
Ping Statistics for 172.16.254.254
Packets: Sent = 3, Received = 3, Lost = 0
```

Below the text are 'Stop' and 'Back' buttons. The 'IPv6 Ping' section is also visible at the bottom, with options for 'Target IPv6 Address' (2233::1), 'Domain Name' (255 chars), 'Ping Times (1-255)' (Infinite), and 'Timeout (1-99)' (1 sec). A 'Start' button is at the bottom right.

Figure 13-22 Ping (Result)

Click **Stop** to stop the ping process.

Click **Back** to return to the previous ping window.

Click **Please Select** to display the following window.

The screenshot shows the 'Ping' window with the 'ACL Access List' dialog box open. The dialog box displays a table with the following data:

ID	ACL Name	ACL Type
11000	std_ipv6_acl	Standard IPv6 ACL
1999	std_ip_acl	Standard IP ACL

Below the table is a pagination control showing '1/1' and a 'Go' button. An 'OK' button is at the bottom right of the dialog box. The background window shows the same 'IPv6 Ping' configuration as Figure 13-22.

Figure 13-23 Ping (Please Select.)

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click **OK** to use the access control list selected.

13.2.5 Trace Route

Use the following window to trace a route to either a destination IPv4/IPv6 address or a domain-name and to perform a test for the network connection.

Choose **Tools > Trace Route** from a tool-bar to display the following window.

The screenshot shows a 'Trace Route' window with two sections: 'IPv4 Trace Route' and 'IPv6 Trace Route'. Each section has radio buttons for 'IPv4 Address' and 'Domain Name', and input fields for 'Max TTL (1-255)', 'Port (1-65535)', 'Timeout (1-65535) sec', and 'Probe Number (1-1000)'. A 'Start' button is located at the bottom right of each section. In the IPv4 section, the 'Domain Name' option is selected, and the 'Port' field contains '33434'. In the IPv6 section, the 'IPv6 Address' option is selected, and the 'Port' field contains '2233:1'.

Figure 13-24 Trace Route

In the section of **IPv4 Trace Route**, you can configure the following parameters.

Parameter	Overview
IPv4 Address	Choose and enter a destination IPv4 address.
Domain-Name	Choose and enter the domain-name of a destination. The number of characters for it can be up to 255.
Max TTL	Enter the maximum value for Time-To-Live (TTL) of the trace route request. This is the maximum number of routers, which allow trace-route packets to pass (or flow). The trace-route option passes while investigating the network path between two devices. The range is from 1 to 255 (hops).
Port	Enter the port-number whose range is from 1 to 65,535.
Time-out	Enter the time-out period while waiting for a response coming from a remote device. The range is from 1 to 65,535 (seconds). The default value is 5 (seconds).
Probe Number	Enter the number of probe-times. The range is from 1 to 1,000. The default value is 1.

Click **Start** to start the IPv4 trace-route.

In the section of **IPv6 Trace Route**, you can configure the following parameters.

Parameter	Overview
IPv6 Address	Choose and enter a destination IPv6 address.
Domain Name	Choose and enter a destination domain-name. The number of characters for it can be up to 255.
Max TTL	Enter the maximum value of TTL of a trace-route request. This is the maximum number of routers where trace-route packets can pass. The trace-route option passes when seeking the network path between two devices. The range is from 1 to 255 (hops).
Port	Enter the port-number whose range is from 1 to 65,535.
Time-out	Enter the time-out period (needed) when waiting for the response coming from a remote device. The range is from 1 to 65,535 (seconds). The default value is 5 seconds.
Probe Number	Enter the number of probe times. The range is from 1 to 1,000. The default value is 1 (second).

Click **Start** to start the IPv6 trace-route.

Choose and enter the **IPv4 Trace Route** parameter and click **Start** to display the following window.

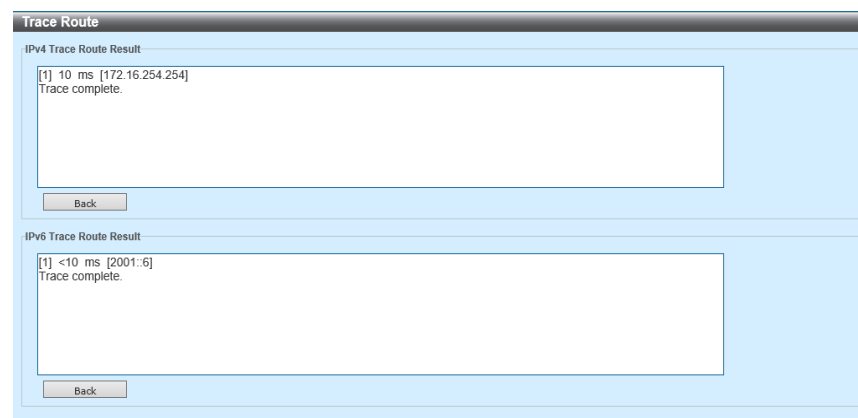


Figure 13-25 Trace Route (Result)

Click **Back** to return to the previous **Trace-Route** window.

13.2.6 Reset

Use the following window to reset the value (of a switch) to the value of a factory default settings on a switch software configuration.

Choose **Tools > Reset** from the tool-bar to display the following window.

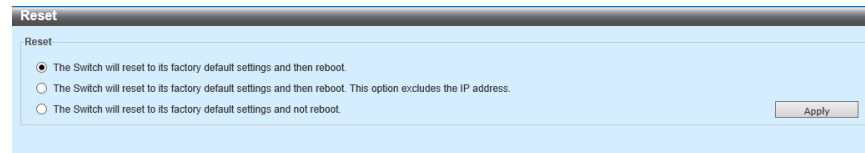


Figure 13-26 Reset

You can configure the following parameter.

Parameter	Overview
Reset	<p>Choose one of the following reset options.</p> <ul style="list-style-type: none"> Your switch is reset to the factory default settings to restart. This option excludes an IP Address from the reset target. Your switch is reset to the factory default settings, but does not restart.

Click **Apply** to reset to the factory default settings.

13.2.7 Reboot System

Use the following window to reboot a switch. New configuration changes are made as the last (or previous) reboot or power-on becomes lost if the changes were not saved during the last time.

Choose **Tools > Reboot System** from the tool-bar to display the following window.

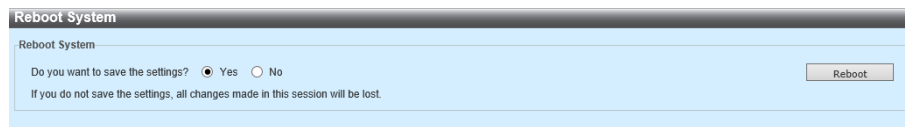


Figure 13-27 Reboot System

Click **Yes** to save the new configurations changed before rebooting.

Click **No** to discard the new configurations changed before rebooting.

Click **Reboot** to reboot the device.

13.3 Language

Choose a language of Web UI. By default, you can choose either English or Japanese.

Choose a language as illustrated in the screen below.



Figure 13-28 Language

14.4 Log Out

Click **Log Out** on the tool-bar to log out from Web UI of a switch.

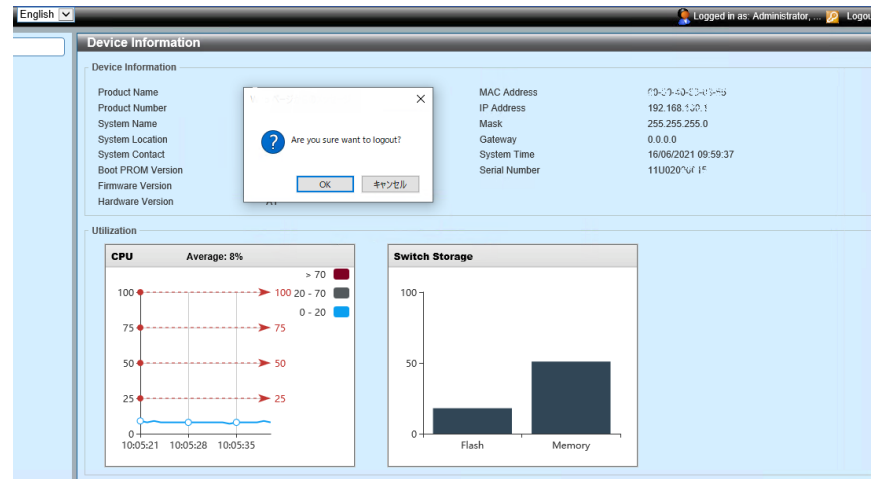


Figure 14-29 Log Out

15 Appendix - System Log Entries

15.1 802.1X

ID	Overview of Logs	Severity
1.	<p>Overview of events: 802.1X authentication is successful to implement. Log message: 802.1X](<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> Overview of parameters: method: indicates either local or RADIUS. username: the user to be authenticated macaddr: a MAC address of a device to be authenticated. portNum: the port-number of a switch vid: the VLAN ID to be allowed</p>	Information
2.	<p>Overview of events: a 802.1X authentication failure occurs. Log message: 802.1X](<method>)Rejected user <username> (<macaddr>) on Port <portNum> Overview of parameters: method: indicates either local or RADIUS. username: the user to be authenticated macaddr: a MAC address of a device to be authenticated portNum: the port-number of a switch</p>	Notice
3.	<p>Overview of events: as the 802.1X authentication table is full, a new address cannot be authenticated. Log message: 802.1X]Rejected <macaddr> on Port <portNum> (auth table was full) Overview of parameters: macaddr: a MAC address of a device to be authenticated. portNum: the port-number of a switch</p>	Notice

15.2 AAA

ID	Overview of Logs	Severity
1.	Overview of events: log-in is successful. Log message: successful login through <Console Telnet SSH>(Username: <username>, IP: <ipaddr ipv6address>) Overview of parameters: ipaddr: indicates an IP address. username: indicates a user-name. ipv6address: indicates an IPv6 address.	Information
2.	Overview of events: log-in failed. Log message: log-in failed through <Console Telnet SSH> (Username: <username>, IP: <ipaddr ipv6address>) Overview of parameters: ipaddr: indicates an IP address. username: indicates a user-name. ipv6address: indicates an IPv6 address.	Warning
3.	Overview of events: log-out Log message: logout through <Console Telnet SSH> (Username: <username>, IP: <ipaddr ipv6address>) Overview of parameters: ipaddr: indicates an IP address. username: indicates a user-name. ipv6address: indicates an IPv6 address.	Information
4.	Overview of events: session timed out. Log message: <Console Telnet > session timed out (Username: <username>, IP: <ipaddr ipv6address>) Overview of parameters: ipaddr: indicates an IP address. username: indicates a user-name. ipv6address: indicates an IPv6 address.	Information
5.	Overview of events: an SSH server is enabled. Log message: SSH server is enabled.	Information
6.	Overview of events: an SSH server is disabled. Log message: SSH server is disabled	Information
7.	Overview of events: an authentication policy is enabled. Log message: authentication policy is enabled (Module: AAA).	Information
8.	Overview of events: an authentication policy is disabled. Log message: authentication policy is disabled (Module: AAA).	Information
9.	Overview of events: log-in failed because of the AAA server time-out or inaccurate configuration. Log message: login failed through <Console Telnet SSH> from <ipaddr ipv6address> due to AAA server <ipaddr ipv6address> timeout or improper configuration (Username: <username>) Overview of parameters: ipaddr: indicates an IP address. ipv6address: indicates an IPv6 address. username: indicates a user-name.	Warning

ID	Overview of Logs	Severity
10.	<p>Overview of events: the migration of administrative privileges is successful with the AAA local authentication, the server authentication or without an authentication.</p> <p>Log message: Successful Enable Admin through <Console Telnet SSH> from <ipaddr ipv6address> authenticated by AAA <local none server <ipaddr ipv6address>> (Username: <username>)</p> <p>Overview of parameters:</p> <p>local: migrates administrative privileges by the AAA local authentication.</p> <p>none: migrates the administrative privileges without an AAA authentication.</p> <p>server: migrates administrative privileges by an AAA server authentication.</p> <p>ipaddr: indicates an IP address.</p> <p>ipv6address: indicates an IPv6 address.</p> <p>username: indicates a user-name.</p>	Information
11.	<p>Overview of events: migrating administrative privileges privilege failed because of the AAA server time-out or improper configuration.</p> <p>Log message: Enable Admin failed through <Console Telnet SSH> from <ipaddr ipv6address> due to AAA server <ipaddr ipv6address> timeout or improper configuration (Username: <username>)</p> <p>Overview of parameters:</p> <p>ipaddr: indicates an IP address.</p> <p>ipv6address: indicates an IPv6 address.</p> <p>username: indicates a user-name.</p>	Warning
12.	<p>Overview of events: the migration of administrative privileges failed because of the AAA local authentication or AAA server authentication.</p> <p>Log message: Enable Admin failed through <Console Telnet SSH> from <ipaddr ipv6address> authenticated by AAA <local server <ipaddr ipv6address>> (Username: <username>)</p> <p>Overview of parameters:</p> <p>local: migrates administrative privileges with an AAA local authentication.</p> <p>server: migrates administrative privileges with an AAA server authentication.</p> <p>ipaddr: indicates an IP address.</p> <p>ipv6address: indicates an IPv6 address.</p> <p>username: indicates an user-name.</p>	Warning
13.	<p>Overview of events: log-in is successful with an AAA local authentication, sever authentication or without any authentication.</p> <p>Log message: successful login through <Console Telnet SSH> from <ipaddr ipv6address> authenticated by AAA <local none server <ipaddr ipv6address>> (Username: <username>)</p> <p>Overview of parameters:</p> <p>local: specifies an AAA local authentication.</p> <p>none: this specifies no authentication.</p> <p>server: specifies an AAA server authentication.</p> <p>ipaddr: indicates an IP address.</p> <p>ipv6address: indicates an IPv6 address.</p> <p>username: indicates a user-name.</p>	Information

ID	Overview of Logs	Severity
14.	<p>Overview of events: log-in failure occurs because of the authentication of either AAA local or AAA server.</p> <p>Log message: log-in failed through <Console Telnet SSH> from <ipaddr ipv6address> authenticated by AAA <local server <ipaddr ipv6address>> (Username: <username>)</p> <p>Overview of parameters:</p> <p>local: specifies an AAA local authentication.</p> <p>server: specifies an AAA server authentication.</p> <p>ipaddr: indicates an IP address.</p> <p>ipv6address: indicates an IPv6 address.</p> <p>username: indicates a user-name.</p>	Warning

15.3 ARP

ID	Overview of Logs	Severity
1.	<p>Overview of events: duplicated IPs are detected in gratuitous ARP.</p> <p>Log message: a conflicting IP is detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>, Interface: <ipif_name>)</p> <p>Overview of parameters:</p> <p>ipaddr: duplicated IP addresses with the device (in the progress of) being used.</p> <p>macaddr: a MAC address of a device with an IP address that overlaps with the device in use.</p> <p>portNum: this indicates an integer and the logical port-number of a device.</p> <p>ipif_name: the interface name of a switch with a conflicting IP address.</p>	Warning

15.4 Authentication (2 Steps)

ID	Overview of Logs	Severity
1.	<p>Overview of events: 2-step authentication is successful. Log message: <step-mode>] (<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> Overview of parameters: step-mode: indicates the 2-step authentication mode. method: indicates either local or RADIUS. username: the user that is being authenticated. macaddr: a MAC address of a device to be authenticated. portNum: the port-number of a switch. vid: indicates a VLAN ID to be authorized.</p>	Information
2.	<p>Overview of events: MAC WEB authenticaiton failures. Log message: MAC-WEB] (<method>) Rejected at MAC auth <macaddr> on Port <portNum> Overview of parameters: method: indicates either local or RADIUS. macaddr: a MAC address of a device to be authenticated. portNum: the port-number of a switch.</p>	Notice
3.	<p>Overview of events: failing to implement the MAC WEB authenticaiton Log message: MAC-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum> Overview of parameters: method: indicates either local or RADIUS. username: the user that is being rejected. macaddr: a MAC address of a device to be authenticated. portNum: the port-number of a switch.</p>	Notice
4.	<p>Overview of events: MAC-802.1X authenticaiton failures. Log message: MAC-802.1X] (<method>) Rejected at MAC auth <macaddr> on Port <portNum> Overview of parameters: method: indicates either local or RADIUS. macaddr: a MAC address of a device to be authenticated. portNum: the port-number of a switch.</p>	Notice
5.	<p>Overview of events: failing to implement the MAC-802.1X authenticaiton Log message: MAC-802.1X] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum> Overview of parameters: method: indicates either local or RADIUS. username: indicates rejected users. macaddr: a MAC address of a device to be authenticated. portNum: the port-number of a switch.</p>	Notice
6.	<p>Overview of events: 802.1X-WEB authentication failures. Log message: 802.1X-WEB] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum> Overview of parameters: method: indicates either local or RADIUS. username: indicates rejected users. macaddr: a MAC address of a device to be authenticated. portNum: the port-number of a switch.</p>	Notice

ID	Overview of Logs	Severity
7.	<p>Overview of events: 802.1X-WEB authentication failures.</p> <p>Log message: 802.1X-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum></p> <p>Overview of parameters:</p> <p>method: indicates either local or RADIUS.</p> <p>username: indicates rejected users.</p> <p>macaddr: a MAC address of a device to be authenticated.</p> <p>portNum: the port-number of a switch.</p>	Notice

15.5 BPDU Guard

ID	Overview of Logs	Severity
1.	Overview of events: BPDU attacks have occurred. Log message: Port<portNum> enter BPDU under attacking state (mode: drop / block / shutdown) Overview of parameters: portNum: indicates the port-number. mode: the current condition regarding BPDU.	Information
2.	Overview of events: recovering from BPDU attacks automatically is successful. Log message: Port <portNum> recovers from BPDU under attacking state automatically. Overview of parameters: portNum: indicates the port-number.	Information
3.	Overview of events: recovering from BPDU attacks manually is successful. Log message: Port<portNum> recovers from BPDU under attacking state manually. Overview of parameters: portNum: indicates the port-number.	Information

15.6 Command

ID	Overview of Logs	Severity
1.	<p>Overview of events: command-logging.</p> <p>Log message: "<command-str>" executed by <username> from <line>, IP: <ip-address>]</p> <p>Overview of parameters:</p> <p>username: the account-name that has executed this command.</p> <p>command-str: the command strings, which is executed successfully and makes a change to a switch configuration.</p> <p>line: this parameter indicates the line mode, which executes these commands (e.g. console, telnet and SSH).</p> <p>ip-address: (optional) If you type the command from a remote terminal (e.g. telnet and SSH), this parameter is needed.</p>	Information

15.7 Configuration/Firmware

ID	Overview of Logs	Severity
1.	<p>Overview of events: upgrading firmware is successful.</p> <p>Log message: irmware upgraded by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Overview of parameters:</p> <p>session: indicates a user-session.</p> <p>username: indicates a current log-in user.</p> <p>ipaddr: indicates a client IP address.</p> <p>macaddr: indicates a client MAC address.</p> <p>serverIP: indicates a server IP address.</p> <p>pathFile: indicates a path and the name of a file on a server.</p>	Information
2.	<p>Overview of events: a failure of upgrading firmware occurs.</p> <p>Log message: Firmware upgraded by <session> unsuccessfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Overview of parameters:</p> <p>session: indicates a user-session.</p> <p>username: indicates a current log-in user.</p> <p>ipaddr: indicates a client IP address.</p> <p>macaddr: indicates a client MAC address.</p> <p>serverIP: indicates a server IP address.</p> <p>pathFile: indicates a path and the name of a file on a server.</p>	Warning
3.	<p>Overview of events: uploading firmware is successful.</p> <p>Log message: Firmware uploaded by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Overview of parameters:</p> <p>session: indicates a user-session.</p> <p>username: indicates a current log-in user.</p> <p>ipaddr: indicates a client IP address.</p> <p>macaddr: indicates a client MAC address.</p> <p>serverIP: indicates a server IP address.</p> <p>pathFile: indicates a path and the name of a file on a server.</p>	Information
4.	<p>Overview of events: a failure of uploading firmware occurs.</p> <p>Log message: Firmware uploaded by <session> unsuccessfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Overview of parameters:</p> <p>session: indicates a user-session.</p> <p>username: indicates a current log-in user.</p> <p>ipaddr: indicates a client IP address.</p> <p>macaddr: indicates a client MAC address.</p> <p>serverIP: indicates a server IP address.</p> <p>pathFile: indicates a path and the name of a file on a server.</p>	Warning

ID	Overview of Logs	Severity
5.	<p>Overview of events: downloading a configuration is successful.</p> <p>Log message: Configuration downloaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Overview of parameters:</p> <p>session: indicates a user-session.</p> <p>username: indicates a current log-in user.</p> <p>ipaddr: indicates a client IP address.</p> <p>macaddr: indicates a client MAC address.</p> <p>serverIP: indicates a server IP address.</p> <p>pathFile: indicates a path and the name of a file on a server.</p>	Information
6.	<p>Overview of events: a failure of downloading a configuration occurs.</p> <p>Log message: Configuration downloaded by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Overview of parameters:</p> <p>session: indicates a user-session.</p> <p>username: indicates a current log-in user.</p> <p>ipaddr: indicates a client IP address.</p> <p>macaddr: indicates a client MAC address.</p> <p>serverIP: indicates a server IP address.</p> <p>pathFile: indicates a path and the name of a file on a server.</p>	Warning
7.	<p>Overview of events: uploading a configuration is successful.</p> <p>Log message: Configuration uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Overview of parameters:</p> <p>session: indicates a user-session.</p> <p>username: indicates a current log-in user.</p> <p>ipaddr: indicates a client IP address.</p> <p>macaddr: indicates a client MAC address.</p> <p>serverIP: indicates a server IP address.</p> <p>pathFile: indicates a path and the name of a file on a server.</p>	Information
8.	<p>Overview of events: a failure of uploading a configuration occurs</p> <p>Log message: Configuration uploaded by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Overview of parameters:</p> <p>session: indicates a user-session.</p> <p>username: indicates a current log-in user.</p> <p>ipaddr: indicates a client IP address.</p> <p>macaddr: indicates a client MAC address.</p> <p>serverIP: indicates a server IP address.</p> <p>pathFile: indicates a path and the name of a file on a server.</p>	Warning
9.	<p>Overview of events: a failure of downloading a unknown type of files occurs.</p> <p>Log message: Downloaded by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Overview of parameters:</p> <p>session: indicates a user-session.</p> <p>username: indicates a current log-in user.</p> <p>ipaddr: indicates a client IP address.</p> <p>macaddr: indicates a client MAC address.</p> <p>serverIP: indicates a server IP address.</p> <p>pathFile: indicates a path and the name of a file on a server.</p>	Warning

ID	Overview of Logs	Severity
10.	Overview of events: uploading log-messages is successful. Log message: Log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)) Overview of parameters: session: indicates a user-session. username: indicates a current log-in user. ipaddr: indicates a client IP address. macaddr: indicates a client MAC address.	Information
11.	Overview of events: a failure of uploading log-messages occurs. Log message: Log message uploaded by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)) Overview of parameters: session: indicates a user-session. username: indicates a current log-in user. ipaddr: indicates a client IP address. macaddr: indicates a client MAC address.	Information

15.8 DAD

ID	Overview of Logs	Severity
1.	Overview of events: as DUT receives Neighbor Solicitation (NS) messages with duplicated addresses during the DAD period, logs are added. Log message: duplicate address <ipv6address > on <interface-id> via receiving neighbor solicitation messages. Overview of parameters: ipv6address: indicates an IPv6 address in neighbor solicitation messages. interface-id: indicates a port-interface ID.	Warning
2.	Overview of events: as DUT receives Neighbor Advertisement (NA) messages with duplicated addresses during the DAD period, logs are added. Log message: duplicate address <ipv6address > on <interface-id> via receiving neighbor advertisement messages. Overview of parameters: ipv6address: indicates an IPv6 address in neighbor advertisement messages. interface-id: indicates a port-interface ID.	Warning

15.9 DDM

ID	Overview of Logs	Severity
1.	<p>Overview of events: the SFP parameter exceeding the warning threshold exists.</p> <p>Log message: optical transceiver <interface-id> <component> <high-low> warning threshold exceeded</p> <p>Overview of parameters:</p> <p>interface-id: indicates a port-interface ID.</p> <p>component: DDM-threshold type-one of the following can be this type.</p> <p>Temperature</p> <p>Supply voltage</p> <p>Bias current</p> <p>Transmission power</p> <p>Reception power</p> <p>high-low: indicates the high threshold or low threshold.</p>	Warning
2.	<p>Overview of events: the SFP parameter exceeding the alarm threshold exists.</p> <p>Log message: optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded</p> <p>Overview of parameters:</p> <p>interface-id: indicates a port-interface ID.</p> <p>component: DDM threshold type - one of the following can be this type.</p> <p>Temperature</p> <p>Supply voltage</p> <p>Bias current</p> <p>Transmission power</p> <p>Reception power</p> <p>high-low: indicates the upper threshold or lower threshold.</p>	Critical
3.	<p>Overview of events: the SFP parameter, which has recovered from the warning threshold, exists.</p> <p>Log message: Optical transceiver <interface-id> <component> back to normal</p> <p>Overview of parameters:</p> <p>interface-id: indicates a port-interface ID.</p> <p>component: DDM threshold type - one of the following can be this type.</p> <p>Temperature</p> <p>Supply voltage</p> <p>Bias current</p> <p>Transmission power</p> <p>Reception power</p>	Warning

15.10 Debug Error

ID	Overview of Logs	Severity
1.	Overview of events: as a vital error of a system occurs, you need to restart the system. Log message: system re-start reason: system fatal error	Urgent
2.	Overview of events: as an exception of CPU occurs, you need to restart the system. Log message: system re-start reason: CPU exception	Urgent

15.11 DHCPv6 Client

ID	Overview of Logs	Severity
1.	Overview of events: the administrator state of a DHCPv6 client-interface becomes changed. Log message: a DHCPv6 client on interface <ipif-name> changed state to enabled disabled] Overview of parameters: <ipif-name>: the name of the DHCPv6 client interface	Information
2.	Overview of events: a DHCPv6 client is obtained from a DHCPv6 server. Log message: a DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name> Overview of parameters: ipv6address: the IPv6 address obtained from a DHCPv6 server ipif-name: the name of the DHCPv6 client interface	Information
3.	Overview of events: started to update the IPv6 address, which is obtained from a DHCPv6 server. Log message: an IPv6 address < ipv6address > on interface <ipif-name> starts renewing Overview of parameters: ipv6address: the IPv6 address obtained from a DHCPv6 server ipif-name: the name of the DHCPv6 client interface	Information
4.	Overview of events: updating the IPv6 address obtained from a DHCPv6 server is successful. Log message: an IPv6 address < ipv6address > on interface <ipif-name> renews success Overview of parameters: ipv6address: the IPv6 address obtained from a DHCPv6 server ipif-name: the name of the DHCPv6 client interface	Information
5.	Overview of events: started to rebind the IPv6 address, which is obtained from a DHCPv6 server. Log message: an IPv6 address < ipv6address > on interface <ipif-name> starts rebinding Overview of parameters: ipv6address: the IPv6 address obtained from a DHCPv6 server ipif-name: the name of the DHCPv6 client interface	Information
6.	Overview of events: rebinding the IPv6 address, which is obtained from a DHCPv6 server, is successful. Log message: an IPv6 address < ipv6address > on interface <ipif-name> rebinds success Overview of parameters: ipv6address: the IPv6 address obtained from a DHCPv6 server ipif-name: the name of the DHCPv6 client interface	Information
7.	Overview of events: the IPv6 address, which is obtained from a DHCPv6 server, is deleted. Log message: an IPv6 address < ipv6address > on interface <ipif-name> was deleted Overview of parameters: ipv6address: the IPv6 address obtained from a DHCPv6 server ipif-name: the name of the DHCPv6 client interface	Information

ID	Overview of Logs	Severity
8.	Overview of events: the administrator state of the DHCPv6 client PD interface becomes changed. Log message: the DHCPv6 client PD on interface <intf-name> changed state to <enabled disabled> Overview of parameters: intf-name: the name of the DHCPv6 client PD interface	Information
9.	Overview of events: the DHCPv6 client PD obtained an IPv6 prefix from a delegation router. Log message: the DHCPv6 client PD obtains an IPv6 prefix <ipv6networkaddr> on interface <intf-name> Overview of parameters: ipv6networkaddr: the IPv6 prefix obtained from a delegation router intf-name: the name of the DHCPv6 client PD interface	Information
10.	Overview of events: started to update the IPv6 prefix, which is obtained from a delegation router. Log message: an IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing Overview of parameters: ipv6networkaddr: the IPv6 prefix obtained from a delegation router intf-name: the name of the DHCPv6 client PD interface	Information
11.	Overview of events: Updating the IPv6 prefix, which is obtained from a delegation router, is successful. Log message: an IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success Overview of parameters: ipv6networkaddr: the IPv6 prefix obtained from a delegation router intf-name: the name of the DHCPv6 client PD interface	Information
12.	Overview of events: started to rebind the IPv6 prefix, which is obtained from a delegation router. Log message: an IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding Overview of parameters: ipv6address: the IPv6 prefix obtained from a delegation router intf-name: the name of the DHCPv6 client PD interface	Information
13.	Overview of events: rebinding the IPv6 prefix, which is obtained from a delegation router, is successful. Log message: an IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success Overview of parameters: ipv6address: the IPv6 prefix obtained from a delegation router intf-name: the name of the DHCPv6 client PD interface	Information
14.	Overview of events: the IPv6 prefix, which is obtained from a delegation router, is deleted. Log message: an IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted Overview of parameters: ipv6address: the IPv6 prefix obtained from a delegation router intf-name: the name of the DHCPv6 client PD interface	Information

15.12 Dynamic ARP

ID	Overview of Logs	Severity
1.	<p>Overview of events: this log is generated if ARP packets with disabled DAI are detected.</p> <p>Log message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)</p> <p>Overview of parameters:</p> <p>type: ARP packet type. This indicates that the ARP packets are either ARP requests or ARP responses.</p> <p>ip-address: indicates an IP address.</p> <p>mac-address: indicates a MAC address.</p> <p>vlan-id: indicates a VLAN ID.</p> <p>interface-id: indicates the interface-number.</p>	Warning
2.	<p>Overview of events: this log is generated if ARP packets with enabled DAI are detected.</p> <p>Log message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)</p> <p>Overview of parameters:</p> <p>type: ARP packet type. This indicates that the ARP packets are either ARP requests or ARP responses.</p> <p>ip-address: indicates an IP address.</p> <p>mac-address: indicates a MAC address.</p> <p>vlan-id: indicates a VLAN ID.</p> <p>interface-id: indicates the interface-number.</p>	Information

15.13 Interface

ID	Overview of Logs	Severity
1.	Overview of events: the port becomes link-up. Log message: Port <port> link up, <nway> Overview of parameters: Port: indicates the logical port-number. nway: indicates the link-speed and duplex mode.	Information
2.	Overview of events: the port becomes link-down. Log message: Port <port> link down Overview of parameters: Port: indicates the logical port-number.	Information

15.14 PoE

ID	Overview of Logs	Severity
1.	Overview of Events: the power-supply for ports becomes ON. Log Message: Port-<port> Power OFF notification Overview of Parameters: port: indicates the logical port-number.	Information
2.	Overview of Events: the power-supply for ports becomes OFF. Log Message: Port-<port> Power On notification Overview of Parameters: port: indicates the logical port-number.	Information
3.	Overview of Events: the power-supply for PoE (has) exceeded the threshold. Log Message: Usage power is above the threshold	Information
4.	Overview of Events: the PoE power-supply becomes lowered to the value, which is less than the threshold after exceeding the threshold. Log Message: Usage power is below the threshold	Information
5.	Overview of Events: the initialization of PoE IC becomes failed. Log Message: PoE IC Reinit Fail	Information
6.	Overview of Events: PoE IC is reset. Log Message: PoE IC Reset	Information

15.15 PoE Scheduler

ID	Overview of Logs	Severity
1.	Overview of Events: the PoE scheduler (has) set a PoE power-supply to ON. Log Message: (PoE) PoE port is changed to ON by PoE Scheduler. Overview of Parameters : port: indicates the logical port-number.	Warning
2.	Overview of Events: the PoE scheduler (has) set the PoE power-supply to OFF. Log Message: (PoE) PoE port is changed to OFF by PoE Scheduler. Overview of Parameters: port: indicates the logical port-number.	Warning
3.	Overview of Events: the PoE scheduler (has) set the PoE power-supply to OFF/ON. Log Message: (PoE) PoE port is reset by PoE Scheduler.	Warning

15.16 PoE Auto Reboot

ID	Overview of Logs	Severity
1.	Overview of events: OFF/ON for a PoE power-supply is executed. Log Message: Execute PoE OFF/ON Port-<port> Overview of Parameters: port: indicates the logical port-number.	Information
2.	Overview of events: After monitoring Pings, an abnormality of a PoE terminal is detected. Log Message: Detect equipment failure by ICMP <IP> Overview of Parameters: IP: indicates an IP address.	Information
3.	Overview of events: After monitoring LLDP, an abnormality of a PoE terminal is detected. Log Message: Detect equipment failure by LLDP Port-<port> Overview of Parameters: port: indicates the logical port-number.	Information
4.	Overview of events: monitoring traffics After monitoring traffics, an abnormality of a PoE terminal is detected. Log Message: Detect equipment failure by Traffic Port-<port> Overview of Parameters: port: indicates the logical port-number.	Information

15.17 Verifying IP Source Guard

ID	Overview of Logs	Severity
1.	<p>Overview of events: this message indicates that hardware-rule resources for setting DHCP Snooping entry to an IPSG table do not exist.</p> <p>Log message: Failed to set IPSG entry due to no hardware-rule resources. (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Interface <INTERFACE-ID>)</p> <p>Overview of parameters:</p> <p>ipaddr: indicates an IP address.</p> <p>Macaddr: indicates a MAC address.</p> <p>VLANID: indicates a VLAN ID.</p> <p>INTERFACE-ID: indicates the interface-number.</p>	Warning

15.18 LLDP-MED

ID	Overview of Logs	Severity
1.	<p>Overview of events: a network device has detected a change in an LLDP-MED topology.</p> <p>Log message: an LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)</p> <p>Overview of parameters:</p> <p>portNum: indicates the port-number.</p> <p>chassisType: indicates a sub-type of chassis.</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: indicates a chassis ID.</p> <p>portType: indicates the port ID sub-type.</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: indicates a port ID.</p> <p>deviceClass: indicates the LLDP-MED device-type.</p>	Notice

ID	Overview of Logs	Severity
2.	<p>Overview of events: a network device has detected the conflicting LLDP-MED device-type.</p> <p>Log message: the conflicting LLDP-MED device-type is detected (on port <portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)</p> <p>Overview of parameters:</p> <p>portNum: indicates the port-number.</p> <p>chassisType: indicates a sub-type of chassis.</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: indicates a chassis ID.</p> <p>portType: indicates the port ID sub-type.</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: indicates a port ID.</p> <p>deviceClass: indicates the LLDP-MED device-type.</p>	Notice
3.	<p>Overview of events: a network device has detected the incompatible LLDP-MED TLV set.</p> <p>Log message: the incompatible LLDP-MED TLV set is detected (on port <portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)</p> <p>Overview of parameters:</p> <p>portNum: indicates the port-number.</p> <p>chassisType: indicates a sub-type of chassis.</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: indicates a chassis ID.</p> <p>portType: indicates the port ID sub-type.</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: indicates a port ID.</p> <p>deviceClass: indicates the LLDP-MED device-type.</p>	Notice

15.19 LACP

ID	Overview of Logs	Severity
1.	Overview of events: a link-aggregation group becomes link-up. Log Message: Link Aggregation Group < group_id > link up Overview of Parameters: group_id: a group ID of an aggregation group that becomes link-up.	Information
2.	Overview of events: a link-aggregation group becomes link-down. Log Message: Link Aggregation Group < group_id > link down Overview of Parameters: group_id: a group ID of an aggregation group that becomes link-down.	Information
3.	Overview of events: a member-port belongs to a link-aggregation group. Log Message: <ifname> attach to Link Aggregation Group <group_id> Overview of Parameters: ifname: the interface-name of ports that belong to an aggregation-group. group_id: a group ID of the aggregation-group where a port belongs to.	Information
4.	Overview of events: a member-port (has) deactivated to belong to a link-aggregation group. Log Message: <ifname> detach from Link Aggregation Group <group_id> Overview of Parameters: ifname: the interface-name of ports that deactivate to belong to an aggregation-group. group_id: a group ID of an aggregation-group where a port deactivates to belong to.	Information

15.20 Detecting Loops

ID	Overview of Logs	Severity
1.	Overview of events: a loop is detected between two ports or two LACP interfaces. Log message: the loop detected between port/port-channel <portNum> and <portNum> Overview of parameters: portNum: indicates the port-number or an LACP interface ID	Warning
2.	Overview of events: a loop is detected on one port or one LACP interface. Log message: the loop detected on port/port-channel <portNum> Overview of parameters: portNum: indicates the port-number or an LACP interface ID	Warning
3.	Overview of events: a loop is detected between a port and an LACP interface. Log message: the loop detected between port/port-channel <portNum> and port/port-channel <portNum> Overview of parameters: portNum: indicates the port-number or port-channel number	Warning
4.	Overview of events: the port being a loop or an LACP interface becomes recovered, automatically. Log message: Port/Port-channel <portNum> auto recovery Overview of parameters: portNum: indicates the port-number or an LACP interface ID	Information

15.21 MAC-based Access Control

ID	Overview of Logs	Severity
1.	Overview of events: a MAC authentication is successful. Log message: MAC[<method>)Authorized <macaddr> on Port <portNum> to VLAN <vid> Overview of parameters: method: indicates either local or RADIUS. macaddr: indicates a MAC address of a device to be authenticated. portNum: indicates the port-number of a switch. vid: indicates the VLAN ID allowed.	Information
2.	Overview of events: a MAC authentication failed. Log message: MAC[<method>)Rejected <macaddr> on Port <portNum> Overview of parameters: method: indicates either local or RADIUS. macaddr: indicates a MAC address of a device to be authenticated. portNum: indicates the port-number of a switch.	Notice
3.	Overview of events: as a MAC authentication table is full, and a new address cannot be authenticated. Log message: MAC]Rejected <macaddr> on Port <portNum> (auth table was full) Overview of parameters: macaddr: indicates a MAC address of a device to be authenticated. portNum: indicates the port-number of a switch.	Notice

15.22 MSTP Debug Extension

ID	Overview of Logs	Severity
1.	Overview of events: a topology becomes changed. Log message: topology changed (Instance : <Instance-id>, <interface-id>, MAC:<macaddr>) Overview of parameters: Instance-id: indicates an instance ID. interface-id: indicates a port ID. Macaddr: indicates a MAC address.	Notice
2.	Overview of events: this is a new root bridge of a spanning-tree. Log message: CIST CIST Regional MSTI Regional] New root bridge selected (Instance: <Instance-id>] MAC: <macaddr> Priority :< priority>) Overview of parameters: Instance-id: indicates an instance ID. Macaddr: indicates a MAC address. priority: indicates a priority value.	Notice
3.	Overview of events: a spanning-tree protocol becomes enabled. Log message: Spanning Tree Protocol is enabled	Information
4.	Overview of events: a spanning-tree protocol becomes disabled. Log message: Spanning Tree Protocol is disabled	Information
5.	Overview of events: this is a new root port. Log message: new root port is selected (Instance:<instance-id>, <interface-id >) Overview of parameters: instance-id: indicates an instance ID. interface-id: indicates a port ID.	Notice
6.	Overview of events: the state of a spanning-tree port becomes changed. Log message: spanning tree port status change (Instance :< instance-id>, <interface-id>) <old-status> -> <new-status> Overview of parameters: instance-id: indicates an instance ID. interface-id: indicates a port ID. old_status: the status before any changes are made. new_status: the status after any changes are made.	Notice
7.	Overview of events: a spanning-tree port-roll becomes changed. Log message: spanning tree port role change (Instance :< instance-id>, <interface-id>) <old-role> -> <new-role> Overview of parameters: instance-id: indicates an instance ID. interface-id: indicates a port ID. old_role: the roll before any changes are made. new_status: the roll after any changes are made.	Information
8.	Overview of events: a spanning-tree instance is created. Log message: a spanning tree instance is created. (Instance :< instance-id>) Overview of parameters: instance-id: indicates an instance ID.	Information
9.	Overview of events: a spanning-tree instance is deleted. Log message: a spanning tree instance is deleted. (Instance :< instance-id >) Overview of parameters: instance-id: indicates an instance ID.	Information

ID	Overview of Logs	Severity
10.	Overview of events: a spanning-tree version becomes changed. Log message: spanning tree version change (new version :< new-version>) Overview of parameters: new_version: indicates an STP version with changes made.	Information
11.	Overview of events: the name of a spanning-tree MST configuration ID and a revision level become changed. Log message: spanning tree MST configuration ID name and revision level change (name :< name>, revision level <revision-level>) Overview of parameters: name: indicates a name with changes made. revision_level: indicates a revision level with changes made.	Information
12.	Overview of events: a VLAN mapping table of a spanning-tree MST configuration ID is deleted. Log message: spanning-tree MST configuration ID VLAN mapping table change (instance: < instance-id > delete vlan <startvlanid> - <endvlanid>]) Overview of parameters: instance-id: indicates an instance ID. startvlanid-endvlanid: indicates a VLAN list.	Information
13.	Overview of events: a VLAN mapping table of a spanning-tree MST configuration ID is added. Log message: spanning tree MST configuration ID VLAN mapping table change (instance: < instance-id > add vlan <startvlanid> - <endvlanid>]) Overview of parameters: instance-id: indicates an instance ID. startvlanid-endvlanid: indicates a VLAN list.	Information
14.	Overview of events: a spanning-tree roll becomes changed due to the guard root function. Log message: spanning tree port role change (Instance : < instance-id >, <interface-id>) to alternate port due to the guard root Overview of parameters: instance-id: indicates an instance ID. interface-id: indicates a port ID.	Information

15.23 Port Security

ID	Overview of Logs	Severity
1.	Overview of events: an address is full on a port. Log message: MAC address <mac-address> causes the port security violation on <interface-id> Overview of parameters: macaddr: indicates a violative MAC address. interface-id: the interface on which the violation occurs.	Warning
2.	Overview of events: an address is full on a system. Log message: limit on system entry number has been exceeded	Warning

15.24 RADIUS

ID	Overview of Logs	Severity
1.	<p>Overview of events: this log is generated if RADIUS allocates the VLAN ID attribute.</p> <p>Log message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>)</p> <p>Overview of parameters:</p> <p>server-ip: indicates an IP address of a RADIUS server.</p> <p>vid: the VLAN ID allowed and allocated by a RADIUS server.</p> <p>interface-id: indicates the client port-number, which is authenticated.</p> <p>username: indicates a user-name to be authenticated.</p>	Information
2.	<p>Overview of events: this log is generated if RADIUS allocates the effective bandwidth attribute.</p> <p>Log message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface-id> (Username: <username>)</p> <p>Overview of parameters:</p> <p>server-ip: indicates an IP address of a RADIUS server.</p> <p>direction: indicates a direction of a bandwidth control (entry or exit).</p> <p>threshold: the bandwidth thresholdNotice, which is permittedNotice and allocated Noticeby a RADIUS server Notice</p> <p>interface-id: indicates the client port-number, which is authenticated.</p> <p>username: indicates a user-name to be authenticated.</p>	Information
3.	<p>Overview of events: this log is generated if RADIUS allocates the effective priority attribute.</p> <p>Log message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port < interface-id> (Username: <username>)</p> <p>Overview of parameters:</p> <p>server-ip: indicates an IP address of a RADIUS server.</p> <p>priority: the priority, which is allowed and allocated by a RADIUS server.</p> <p>interface-id: indicates the client port-number, which is authenticated.</p> <p>username: indicates a user-name to be authenticated.</p>	Information
4.	<p>Overview of events: this log is generated if RADIUS allocates an ACL script and then the script is not applied to a system because of having insufficient resources.</p> <p>Log message: RADIUS server <server-ip> assigns <username> ACL failure at port < interface-id> (<acl-script>)</p> <p>Overview of parameters:</p> <p>server-ip: indicates an IP address of a RADIUS server.</p> <p>username: indicates a user-name to be authenticated.</p> <p>interface-id: the client port-number, which is authenticated.</p> <p>acl-script: indicates the ACL scriptNotice, which is permittedNotice and allocatedNotice by a RADIUS serverNotice.</p>	Warning
5.	<p>Overview of events: this log is generated if you fail to allocate the access-list number.</p> <p>Log message: local assigns USERNAME] filter-id ID failure at port-interface-ID</p> <p>Overview of parameters:</p> <p>username: indicates the user-name to be authenticated.</p> <p>filter-id: indicates the access-list number.</p> <p>interface-id: the client port-number, which is authenticated.</p>	Warning

15.25 RRP

ID	Overview of Logs	Severity
1.	Overview of events: the state of a master-node becomes changed from "Failed" to "Complete". Log message: ring-topology was recovered to complete.	Notice
2.	Overview of events: the state of a master-node becomes changed from "Complete" to "Failed". Log message: ring-topology was failed.	Warning
3.	Overview of events: the master node or transit node flashes the forwarding database based on the RRP packets or state-machine. Log message: FDB was flushed.	Information
4.	Overview of events: the RRP state of a transit-node becomes changed to "Link-Up". Log message: RRP ring-status was changed to link-up.	Warning
5.	Overview of events: the RRP state of a transit-node becomes changed to "Link-Down". Log message: RRP ring-status was changed to link-down.	Notice
6.	Overview of events: the RRP state of a transit-node becomes changed to "Pre-Forwarding". Log message: RRP ring-status was changed to pre-forwarding.	Information
7.	Overview of events: a ring-guard function becomes enabled on a specific domain and port. Log message: ring-guard was activated on "<domain-name>" domain at port <port> Overview of parameters: <domain name>: a target domain-name <port num>: the target port-number whose ring-guard function becomes enabled.	Information

15.26 SNMP

ID	Overview of Logs	Severity
1.	Overview of events: an SNMP request, including the invalid community strings, is received. Log message: SNMP request received from <ipaddr> with invalid community string Overview of parameters: ipaddr: indicates an IP address.	Information

15.27 System

ID	Overview of Logs	Severity
1.	Overview of events: a system has started up. Log message: System started up.	Critical
2.	Overview of events: a current configuration is stored on a flash. Log message: Configuration saved to flash by console (Username: <username>). Overview of parameters: username: indicates a user-name.	Information
3.	Overview of events: a system configuration is stored, remotely. Log message: Configuration saved to flash (Username: <user-name>, IP: <ipaddr>) username: indicates a user-name. ipaddr: indicates an IP address.	Information
4.	Overview of events: as the power of a system turned on to start up. Log message: System cold start.	Critical
5.	Overview of events: a system restarts to start up. Log message: System warm start.	Critical

15.28 Telnet

ID	Overview of Logs	Severity
1.	Overview of events: logging in with Telnet is successful. Log message: successful login through Telnet (Username: <username>, IP: <ipaddr>) Overview of parameters: ipaddr: indicates an IP address of Telnet client. username: indicates the user-name, which is used to log into a Telnet server.	Information
2.	Overview of events: Logging in with Telnet is failed. Log message: login failed through Telnet (Username: <username>, IP: <ipaddr>) Overview of parameters: ipaddr: indicates an IP address of Telnet client. username: indicates the user-name, which is used to log into a Telnet server.	Warning
3.	Overview of events: logged out with Telnet. Log message: logout through Telnet (Username: <username>, IP: <ipaddr>) Overview of parameters: ipaddr: indicates an IP address of Telnet client. username: indicates the user-name, which is used to log into a Telnet server.	Information
4.	Overview of events: (Telnet) the session has become time-out. Log message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Overview of parameters: ipaddr: indicates an IP address of Telnet client. username: indicates the user-name, which is used to log into a Telnet server.	Information

15.29 Temperature

ID	Overview of Logs	Severity
1.	Overview of events: a temperature sensor has migrated to the alarm state. Log message: Unit <unitID> Sensor:<sensorID> detects abnormal temperature <temperature> Overview of parameters: unitID: indicates a unit ID. sensorID: indicates a sensor ID. temperature: indicates a the current temperature of a sensor.	Critical
2.	Overview of events: the temperature has been recovered to a normal temperature. Log message: Unit <unitID> Sensor:<sensorID> temperature back to normal Overview of parameters: unitID: indicates a unit ID. sensorID: indicates a sensor ID. temperature: indicates the temperature.	Critical

15.30 Traffic Control

ID	Overview of Logs	Severity
1.	Overview of events: a storm of Broadcast, Multicast or Unicast occurs. Log message: Broadcast Multicast Unicast> storm is occurring on <interface-id>. Overview of parameters: interface-id: indicates the interface ID where a storm occurs.	Warning
2.	Overview of events: a storm of Broadcast, Multicast or Unicast storm is cleared. Log message: <Broadcast Multicast Unicast> storm is cleared on <interface-id>. Overview of parameters: interface-id: indicates the interface ID where a storm is cleared.	Information
3.	Overview of events: the port-shutdown has occurred because of a packet storm. Log message: <interface-id> is currently shut down due to the <Broadcast Multicast Unicast> storm. Overview of parameters: Interface-id: indicates the interface ID, which is migrated to error-disabled by a storm.	Warning

15.31 Voice VLAN

ID	Overview for Logs	Severity
1.	Overview of events: a new voice device is detected on an interface. Log message: New voice device detected (<interface-id>, MAC: < mac-address >). Overview of parameters: interface-id: indicates the name of an interface. mac-address: indicates a MAC address of a voice device.	Information
2.	Overview of events: the interface of the automatic voice VLAN mode participates in the voice VLAN. Log message: < interface-id > add into voice VLAN <vid >. Overview of parameters: interface-id: indicates the name of an interface. vid: indicates a VLAN ID.	Information
3.	Overview of events: this log message is sent if an interface leaves the voice VLAN and does not detect a voice device during the aging period of the interface. Log message: < interface-id > remove from voice VLAN <vid > Overview of parameters: interface-id: indicates the name of an interface. vid: indicates a LAN ID.	Information

15.32 WAC

ID	Overview of Logs	Severity
1.	Overview of events: a client host fails to be authenticated. Log message: WEB](RADIUS/Local) Rejected user <string> (<macaddr>) on Port <portNum>. Overview of parameters: string: indicates a user-name. Macaddr: indicates a MAC address. portNum: indicates the port-number.	Warning
2.	Overview of events: a client host is authenticated, successfully. Log message: WEB](RADIUS/Local)Authorized user <string> (<macaddr>) on Port <portNum> to VLAN <vlanNum>. Overview of parameters: string: indicates a user-name. Macaddr: indicates a MAC address. portNum: indicates the port-number. vlanNum: indicates the VLAN-number.	Information
3.	Overview of events: a client table is full. Log message: WEB]Rejected <macaddr> on Port <portNum> (auth table was full). Overview of parameters: Macaddr: indicates a MAC address. portNum: indicates the port-number.	Notice

15.33 Web

ID	Overview of Logs	Severity
1.	Overview of events: log-in from Web is successful. Log message: "Successful login through Web (Username: <username>, IP: <ipaddr>)" Overview of parameters: username: indicates a user-name. ipaddr: indicates the IP address of the user who accessed to a switch from Web.	Information
2.	Overview of events: failing to log-in from Web. Log message: Login failed through Web (Username: <username>, IP: <ipaddr>)" Overview of parameters: username: indicates a user-name. ipaddr: indicates the IP address of users who accessed to a switch from Web.	Warning
3.	Overview of events: log-in from HTTPS is successful. Log message: Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>) Overview of parameters: username: indicates a user-name. ipaddr: indicates the IP address of the user who accessed to a switch from secure Web.	Information
4.	Overview of Event: log-in from secure Web failed. Log message: Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>) Overview of parameters: username: indicates a user-name. ipaddr: indicates the IP address of the user who accessed to a switch from secure Web.	Warning
5.	Overview of events: Uploading a log is successful. Log message: Log message uploaded by WEB successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <ipaddr>, File Name: <filename>) Overview of parameters: username: indicates a user-name. ipaddr: indicates the IP address of the user who accessed to a switch. macaddr: indicates a MAC address of a client. server IP: indicates an IP address of a TFTP server. filename: indicates the name of a log-file.	Information
6.	Overview of events: uploading a log failed. Log message: Log message uploaded by WEB unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <ipaddr>, File Name: <filename>) Overview of parameters: username: indicates a user-name. ipaddr: indicates an access-source IP address of the user who accessed to a switch. macaddr: indicates a MAC address of a client. server IP: indicates an IP address of a TFTP server. filename: indicates the name of a log-file.	Information

16 Appendix - System Trap Entries

16.1 BPDU Guard

ID	Trap Name	Overview of Traps	OID
1.	mnoBpduProtectionUnderAttackingTrap	BPDU attacks occur, and then migrate to the drop/block / shutdown mode. Binding objects: mnoBpduProtectionPortIndex Port interface (2) mnoBpduProtectionPortMode drop/block/shutdown-mode	1.3.6.1.4.1.396. 5.5.3.4.0.1
2.	mnoBpduProtectionRecoveryTrap	Automatically recovered from BPDU attacks Binding objects: mnoBpduProtectionPortIndex Port interface mnoBpduProtectionRecoveryMethod Automatic /recovering manual	1.3.6.1.4.1.396. 5.5.3.4.0.2

16.2 DDM

ID	Trap Name	Overview of Traps	OID
1.	mnoDdmAlarmTrap	<p>If the parameter value exceeds the alarm threshold or recovers to the normal state, this trap is sent, depending on the configuration of a trap action.</p> <p>Binding objects:</p> <p>mnoDdmPort port-number mnoDdmThresholdType DDM threshold type temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType Check if the exceeding-threshold is the threshold (value) of either high-threshold or alarm low-threshold.</p> <p>(4) mnoDdmThresholdExceedOrRecover Check if GBIC exceeds the DDM threshold or becomes recovered to the normal state.</p>	1.3.6.1.4.1.396.5.5.1.4.0.1
2.	mnoDdmWarningTrap	<p>If the parameter value exceeds the warning threshold or recovers to the normal state, this trap is sent depending on the configuration of a trap action.</p> <p>Binding objects:</p> <p>mnoDdmPort port-number mnoDdmThresholdType DDM threshold type temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType Check if the exceeding-threshold is the threshold of either warning high-threshold or warning low-threshold.</p> <p>(4) mnoDdmThresholdExceedOrRecover Check if GBIC exceeds the DDM threshold or becomes recovered to the normal state.</p>	1.3.6.1.4.1.396.5.5.1.4.0.2

16.3 DHCP Server Protect

ID	Trap Name	Overview of Traps	OID
1.	mnoFilterDetectedTrap	<p>If unauthorized DHCP servers are detected, this trap is transmitted. An IP address of the unauthorized DHCP server detected is transmitted to a trap-receiver (once) during the unauthorized period of log-stopping.</p> <p>Binding objects: mnoFilterDetectedIP The IP addresses of unauthorized DHCP servers mnoFilterDetectedport Port interface</p>	1.3.6.1.4.1.396. 5.5.3.7.0.1

16.4 Gratuitous ARP

ID	Trap Name	Overview of Traps	OID
1.	mnoAgentGratuitousARPTrap	<p>Traps are sent if IP addresses conflict each other.</p> <p>Binding objects:</p> <ul style="list-style-type: none">agentGratuitousARPIpAddr The conflicted IP address received in the gratuitous ARPagentGratuitousARPMacAddr The sender's MAC address of the gratuitous ARP packetsagentGratuitousARPPortNumber This indicates the switch port-number, which received the gratuitous ARP packets.agentGratuitousARPInterfaceName This indicates the IP interface-name of the switch, which received the Gratuitous ARP.	1.3.6.1.4.1.396.5.5.3.6.0.1

16.5 LLDP-MED

ID	Trap Name	Overview of Traps	OID
1.	IldpRemTablesChange	The IldpRemTablesChange notification is sent if the value of IldpStatsRemTableLastChangeTime becomes changed. Binding objects: (1) IldpStatsRemTablesInserts (2) IldpStatsRemTablesDeletes (3) IldpStatsRemTablesDrops (4) IldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2.	IldpXMedTopologyChangeDetected	The notification indicates that a new remote device is connected to a local port after the generation done by a local device that detects a topology change. In addition, the notification indicates that a remote device is disconnected or the device moves among ports. Binding objects: (1) IldpRemChassisIdSubtype (2) IldpRemChassisId (3) IldpXMedRemDeviceClass	1.0.8808.1.1.2.1.5.4795.0.1

16.6 Detecting Loops

ID	Trap Name	Overview of Traps	OID
1.	mnoLoopDetectNotification	This indicates that a network group has occurred.	1.3.6.1.4.1.396.5.5.2.1
2.	mnoLoopRecoveryNotification	This indicates that a network group has been deleted (or removed).	1.3.6.1.4.1.396.5.5.2.2

16.7 MAC Based Access Control

ID	Trap Name	Overview of Traps	OID
1.	mnoMacBasedAccessControlLoggedSuccess	If you log into the MAC based access-control host successfully, this trap is sent. Binding objects: mnoMacBasedAuthInfoMacIndex Host MAC address mnoMacBasedAuthInfoPortIndex Port interface mnoMacBasedAuthVID VLAN ID	1.3.6.1.4.1.396.5.5.3.2.0.1
2.	mnoMacBasedAccessControlLoggedFail	If you fail to log into the MAC based access-control host, this trap is sent. Binding objects: mnoMacBasedAuthInfoMacIndex Host MAC address mnoMacBasedAuthInfoPortIndex Port interface mnoMacBasedAuthVID VLAN ID	1.3.6.1.4.1.396.5.5.3.2.0.2
3.	mnoMacBasedAccessControlAgesOut	If the MAC based access-control host ages out, this trap is sent. Binding objects: mnoMacBasedAuthInfoMacIndex Host MAC address (2) mnoMacBasedAuthInfoMacIndex Port interface (3) mnoMacBasedAuthVID VLAN ID	1.3.6.1.4.1.396.5.5.3.2.0.3

16.8 MAC Notification

ID	Trap Name	Overview of Traps	OID
1.	mnoL2macNotification	<p>This trap indicates that a change is made in a MAC address of an address table.</p> <p>Binding objects: mnoL2macNotifyInfo</p> <p>The changed information regarding a MAC address of a device. The details include the following contents.</p> <p>Operation Code + MAC address + Box ID + Interface ID + Zero.</p> <p>Operation code: 1, 2</p> <p>One (1) indicates that a new MAC address is learned.</p> <p>Two (2) indicates that an old MAC address is deleted.</p> <p>Box ID: The switch box ID</p> <p>Interface ID: The Interface ID learned or deleted on the box.</p> <p>Zero: Uses to delimit each message (operation code + MAC address + Box ID + Port Number).</p>	1.3.6.1.4.1.396 .5.5.3.1.0.1

16.9 MSTP

ID	Trap Name	Overview of Traps	OID
1.	newRoot	This trap indicates that a sending agent has become a new root of the spanning tree. A bridge sends this trap right after the trap is selected as a new root (e.g. after the expiration of the topology change timer, and immediately after choosing). The implementation of this trap is optional.	1,3,6,1,2,1,17.0.1
2.	topologyChange	A bridge sends traps if one of the ports configured migrates from the learning state to forwarding state or from the forwarding state to blocking state. This trap is not sent if newRoot traps are sent in such a migration (as described above). The implementation of this trap is optional.	1,3,6,1,2,1,17.0.2

16.10 Port Security

ID	Trap Name	Overview of Traps	OID
1.	mnoL2PortSecurityViolationTrap	<p>A new MAC address that violates the port-security configuration defined, in advance, triggers to send trap messages.</p> <p>Binding objects: mnoPortSecPortIndex Port interface mnoL2PortSecurityViolationMac Host MAC Address</p>	1.3.6.1.4.1.396. 5.5.3.3.0.1

16.11 Port

ID	Trap Name	Overview of Traps	OID
1.	linkUp	This notification is generated if a port becomes link-up. Binding objects: (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6. 3.1.1.5.4
2.	linkDown	This notification is generated if a port becomes link-down. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6. 3.1.1.5.3

16.12 RMON

ID	Trap Name	Overview of Traps	OID
1.	risingAlarm	SNMP traps are generated if an alarm entry exceeds the upper-threshold. Then the event, which is configured to send SNMP traps, is generated. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16 .0.1
2.	fallingAlarm	SNMP traps are generated if an alarm entry exceeds the lower-threshold. Then the event, which is configured to send SNMP traps, is generated. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16 .0.2

16.13 SNMP Authentication

ID	Trap Name	Overview of Traps	OID
1.	authenticationFailure	<p>authenticationFailure traps indicate that the SNMPv2 entity operating as an agent roll has received the protocol message, which is not accurately authenticated.</p> <p>The function of generating the traps is necessary for all the implementation of SNMPv2, but an object of snmpEnableAuthenTraps shows if the traps are generated.</p>	1.3.6.1.6. 3.1.1.5.5

16.14 System

ID	Trap Name	Overview of Traps	OID
1.	coldStart	coldStart traps indicate the possibility that the SNMPv2 entity operating with an agent-role becomes reinitialized and its configuration becomes changed.	1.3.6.1.6.3.1.1.5.1
2.	warmStart	warmStart traps indicate that an SNMPv2 entity operating as the agent role becomes reinitialized so as its configuration does not become changed.	1.3.6.1.6.3.1.1.5.2

16.15 Temperature

ID	Trap Name	Overview of Traps	OID
1.	mnoTemperatureRising Alarm	This notification is sent if the current temperature exceeds the upper-threshold.	1.3.6.1.4.1.396.5.5.1.2.1
2.	mnoTemperatureFalling Alarm	This notification is sent if the current temperature lowers from the upper-threshold.	1.3.6.1.4.1.396.5.5.1.2.2

16.16 Traffic Control

ID	Trap Name	Overview of Traps	OID
1.	mnoPktStormOccurred	If the packet-storm mechanism detects the packet storm, and if you shutdown as an action, the following is the related information. Binding objects: mnoPktStormCtrlPortIndex Port Interface	1.3.6.1.4.1.396.5.5.3.5.0.1
2.	mnoPktStormCleared	If a packet storm is resolved, the following is the related information. Binding objects: mnoPktStormCtrlPortIndex Port interface	1.3.6.1.4.1.396.5.5.3.5.0.2
3.	mnoPktStormDisablePort	If a port becomes disabled because of the packet storm mechanism, the following is the related information. Binding objects: mnoPktStormCtrlPortIndex Port interface	1.3.6.1.4.1.396.5.5.3.5.0.3

© Panasonic Electric Works Networks Co., Ltd. 2021-2023

Panasonic Electric Works Networks Co.,Ltd.

2-12-7, Higashi-Shimbashi, Minato-ku, Tokyo Japan, 105-0021
URL: <https://panasonic.co.jp/ew/pewnw/english/index.html>

P0721-5023