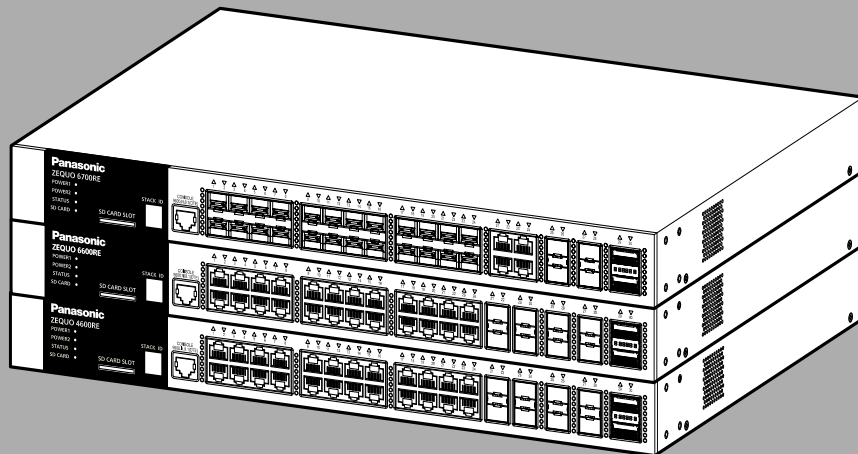




ZEQUO RE Series

WEB Reference

Model Number: PN36243E/PN36241E
PN36241L



The target model for this reference is as follows.

Model name	Model number	Firmware version
ZEQUO 6700RE	PN36243E	2.0.0.11 and above
ZEQUO 6600RE	PN36241E	2.0.0.11 and above
ZEQUO 4600RE	PN36241L	2.0.0.11 and above

Table of Contents

1	Introduction	11
1.1	Related Documentation	11
2	The Web User Interface (Web UI)	12
2.1	Connecting to the Web UI.....	12
2.2	Understanding the Web UI.....	14
3	System	15
3.1	Device Information.....	15
3.2	System Information Settings	16
3.3	Peripheral Settings	17
3.4	Port Configuration	18
3.4.1	Port Settings	18
3.4.2	Port Status	21
3.4.3	Port GBIC.....	22
3.4.4	Port Auto Negotiation.....	23
3.4.5	Error Disable Settings	24
3.4.6	Jumbo Frame	25
3.5	System Log	26
3.5.1	System Log Settings.....	26
3.5.2	System Log Discriminator Settings.....	30
3.5.3	System Log Server Settings	31
3.5.4	System Log	33
3.5.5	System Attack Log	34
3.5.6	System Authentication Log	35
3.6	Time and SNTP (Simple Network Time Protocol).....	36
3.6.1	Clock Settings	36
3.6.2	Time Zone Settings	37
3.6.3	SNTP Settings	39
3.7	Time Range.....	40
4	Management	41
4.1	Command Logging	41
4.2	User Accounts Settings	42
4.3	User Accounts Encryption.....	44
4.4	Login Method	45
4.5	SNMP (Simple Network Management Protocol)	47
4.5.1	SNMP Global Settings	47
4.5.2	SNMP Linkchange Trap Settings.....	49
4.5.3	SNMP View Table Settings	50
4.5.4	SNMP Community Table Settings.....	51
4.5.5	SNMP Group Table Settings	53
4.5.6	SNMP Engine ID Local Settings.....	55
4.5.7	SNMP User Table Settings.....	56
4.5.8	SNMP Host Table Settings.....	59
4.6	RMON (Remote Monitoring)	61
4.6.1	RMON Global Settings	61
4.6.2	RMON Statistics Settings.....	62

4.6.3	RMON History Settings	63
4.6.4	RMON Alarm Settings	65
4.6.5	RMON Event Settings	66
4.7	Telnet/Web	68
4.8	Session Timeout	69
4.9	DHCP (Dynamic Host Configuration Protocol)	70
4.9.1	Service DHCP	70
4.9.2	DHCP Class Settings	71
4.9.3	DHCP Pool Settings	73
4.9.4	DHCP Server	74
4.9.4.1	DHCP Server Global Settings	74
4.9.4.2	DHCP Server Pool Settings	75
4.9.4.3	DHCP Server Exclude Address	79
4.9.4.4	DHCP Server Manual Binding	80
4.9.4.5	DHCP Server Dynamic Binding	81
4.9.4.6	DHCP Server IP Conflict	82
4.9.4.7	DHCP Server Statistics	83
4.9.5	DHCPv6 Server	84
4.9.5.1	DHCPv6 Server Pool Settings	84
4.9.5.2	DHCPv6 Server Local Pool Settings	87
4.9.5.3	DHCPv6 Server Exclude Address	88
4.9.5.4	DHCPv6 Server Binding	89
4.9.5.5	DHCPv6 Server Interface Settings	90
4.9.5.6	DHCPv6 Server Operational Information	91
4.9.6	DHCP Relay	92
4.9.6.1	DHCP Relay Global Settings	92
4.9.6.2	DHCP Relay Pool Settings	93
4.9.6.3	DHCP Relay Information Settings	96
4.9.6.4	DHCP Relay Information Option Format Settings	97
4.9.6.5	DHCP Local Relay VLAN	98
4.9.7	DHCPv6 Relay	99
4.9.7.1	DHCPv6 Relay Global Settings	99
4.9.7.2	DHCPv6 Relay Interface Settings	101
4.10	DHCP Auto Configuration	102
4.11	DNS (Domain Name System)	103
4.11.1	DNS Global Settings	103
4.11.2	DNS Name Server Settings	104
4.11.3	DNS Host Settings	105
4.12	File System	106
4.13	Stacking	108
4.13.1	Physical Stacking	108
4.14	SMTP Settings	110
4.15	NLB FDB Settings	112
4.16	IP Setup	113
4.16.1	IP Setup Settings	113
4.16.2	IP Setup Forwarding Settings	114
5	L2 Features	116
5.1	FDB (File Database)	116
5.1.1	Static FDB	116
5.1.1.1	Unicast Static FDB	116
5.1.1.2	Multicast Static FDB	118
5.1.2	MAC Address Table Settings	119

5.1.3	MAC Address Table.....	122
5.1.4	MAC Notification	123
5.2	Link Aggregation	125
5.3	VLAN (Virtual Local Area Network).....	127
5.3.1	802.1Q VLAN.....	127
5.3.2	802.1v Protocol VLAN	128
5.3.2.1	Protocol VLAN Profile.....	128
5.3.2.2	Protocol VLAN Profile Interface	129
5.3.3	GVRP	130
5.3.3.1	GVRP Global	130
5.3.3.2	GVRP Port.....	131
5.3.3.3	GVRP Advertise VLAN	132
5.3.3.4	GVRP Forbidden VLAN	133
5.3.3.5	GVRP Statistics Table	134
5.3.4	Asymmetric VLAN	135
5.3.5	MAC VLAN	136
5.3.6	VLAN Interface	137
5.3.7	Subnet VLAN	142
5.3.8	Voice VLAN.....	143
5.3.8.1	Voice VLAN Global.....	143
5.3.8.2	Voice VLAN Port	144
5.3.8.3	Voice VLAN OUI.....	146
5.3.8.4	Voice VLAN Device.....	147
5.3.8.5	Voice VLAN LLDP-MED Device.....	148
5.3.9	Private VLAN.....	149
5.4	STP (Spanning Tree Protocol)	151
5.4.1	STP Global Settings.....	151
5.4.2	STP Port Settings.....	153
5.4.3	MST Configuration Identification.....	155
5.4.4	STP Instance	157
5.4.5	MSTP Port Information	158
5.5	Line Loopback.....	159
5.5.1	Line Loopback Settings	159
5.5.2	Line Loopback Log	161
5.6	L2 Protocol Tunnel	162
5.7	L2 Multicast Control.....	165
5.7.1	IGMP Snooping.....	165
5.7.1.1	IGMP Snooping Settings	165
5.7.1.2	IGMP Snooping Groups Settings	168
5.7.1.3	IGMP Snooping Filter Settings.....	170
5.7.1.4	IGMP Snooping Multicast Router Information	174
5.7.1.5	IGMP Snooping Statistics Settings.....	176
5.7.2	MLD Snooping	178
5.7.2.1	MLD Snooping Settings	178
5.7.2.2	MLD Snooping Groups Settings	181
5.7.2.3	MLD Snooping Filter Settings	183
5.7.2.4	MLD Snooping Multicast Router Information	186
5.7.2.5	MLD Snooping Statistics Settings	188
5.7.3	Multicast Filtering Mode	190
5.8	LLDP (Link Layer Discovery Protocol).....	191
5.8.1	LLDP Global Settings	191
5.8.2	LLDP Port Settings.....	193
5.8.3	LLDP Management Address List	195

5.8.4 LLDP Basic TLVs Settings	196
5.8.5 LLDP Dot1 TLVs Settings	197
5.8.6 LLDP Dot3 TLVs Settings	198
5.8.7 LLDP-MED Port Settings	199
5.8.8 LLDP Statistics Information.....	200
5.8.9 LLDP Local Port Information	201
5.8.10 LLDP Neighbor Port Information.....	203
5.9 UDLD (Unidirectional Link Detection).....	205
5.10 RRP (Ring Redundant Protocol).....	206
6 L3 Features.....	209
6.1 ARP (Address Resolution Protocol)	209
6.1.1 ARP Control Settings.....	209
6.1.2 ARP Aging Time	210
6.1.3 Static ARP	211
6.1.4 Proxy ARP	213
6.1.5 ARP Table	214
6.2 Gratuitous ARP	215
6.3 IPv6 Neighbor	217
6.4 Interface	218
6.4.1 IPv4 Interface.....	218
6.4.2 IPv6 Interface.....	221
6.4.3 Loopback Interface	226
6.4.4 Null Interface	228
6.5 IPv4 Static/Default Route	229
6.6 IPv4 Route Table	231
6.7 IPv6 Static/Default Route	233
6.8 IPv6 Route Table	234
6.9 Route Preference	236
6.10 ECMP Settings[ZEQUO6700RE/6600RE]	237
6.11 IPv6 General Prefix	238
6.12 RIP (Routing Information Protocol).....	239
6.12.1 RIP Settings.....	239
6.12.2 RIP Interface Settings.....	242
6.12.3 RIP Database.....	244
6.13 OSPF (Open Shortest Path First) [ZEQUO6700RE/6600RE]	245
6.13.1 OSPFv2	245
6.13.1.1 OSPFv2 Process Settings	245
6.13.1.2 OSPFv2 Passive Interface Settings	248
6.13.1.3 OSPFv2 Area Settings	249
6.13.1.4 OSPFv2 Interface Settings	251
6.13.1.5 OSPFv2 Redistribute Settings	255
6.13.1.6 OSPFv2 Virtual Link Settings.....	256
6.13.1.7 OSPFv2 LSDB Table.....	258
6.13.1.8 OSPFv2 Neighbor Table.....	260
6.13.1.9 OSPFv2 Host Route Settings.....	261
6.13.2 OSPFv3	262
6.13.2.1 OSPFv3 Process Settings	262
6.13.2.2 OSPFv3 Passive Interface Settings	264
6.13.2.3 OSPFv3 Area Settings	265
6.13.2.4 OSPFv3 Interface Settings	268
6.13.2.5 OSPFv3 Virtual link Settings	271

6.13.2.6	OSPFv3 LSDB Table	273
6.13.2.7	OSPFv3 Neighbor Table	275
6.13.2.8	OSPFv3 Border Router Table	276
6.14	IP Multicast Routing Protocol	277
6.14.1	IGMP[ZEQUO6700RE/6600RE]	277
6.14.1.1	IGMP Interface Settings	277
6.14.1.2	IGMP Static Group Settings	280
6.14.1.3	IGMP Dynamic Group Table	281
6.14.2	MLD[ZEQUO6700RE/6600RE]	282
6.14.2.1	MLD Interface Settings	282
6.14.2.2	MLD Group Table	284
6.14.3	IGMP Proxy	285
6.14.3.1	IGMP Proxy Settings	285
6.14.3.2	IGMP Proxy Group Table	287
6.14.3.3	IGMP Proxy Forwarding Table	288
6.14.4	MLD Proxy	289
6.14.4.1	MLD Proxy Settings	289
6.14.4.2	MLD Proxy Group Table	291
6.14.4.3	MLD Proxy Forwarding Table	292
6.14.5	DVMRP[ZEQUO6700RE/6600RE]	293
6.14.5.1	DVMRP Interface Settings	293
6.14.5.2	DVMRP Routing Table	295
6.14.5.3	DVMRP Neighbor Table	296
6.14.6	PIM[ZEQUO6700RE/6600RE]	297
6.14.6.1	PIM for IPv4	297
6.14.6.1.1	PIM Interface	297
6.14.6.1.2	PIM BSR Candidate	300
6.14.6.1.3	PIM RP Address	301
6.14.6.1.4	PIM RP Candidate	303
6.14.6.1.5	PIM RP Table	306
6.14.6.1.6	PIM Register Settings	307
6.14.6.1.7	PIM SPT Threshold Settings	309
6.14.6.1.8	PIM SSM Settings	310
6.14.6.1.9	PIM Neighbor Table	312
6.14.6.2	PIM for IPv6	313
6.14.6.2.1	PIM for IPv6 Interface	313
6.14.6.2.2	PIM for IPv6 BSR Candidate Settings	316
6.14.6.2.3	PIM for IPv6 BSR Table	317
6.14.6.2.4	PIM for IPv6 RP Address	318
6.14.6.2.5	PIM for IPv6 RP Candidate	320
6.14.6.2.6	PIM for IPv6 RP Embedded Settings	323
6.14.6.2.7	PIM for IPv6 RP Table	324
6.14.6.2.8	PIM for IPv6 Register Settings	325
6.14.6.2.9	PIM for IPv6 SPT Threshold Settings	327
6.14.6.2.10	PIM for IPv6 (S,G) Keepalive Time	328
6.14.6.2.11	PIM for IPv6 Multicast Route Table	329
6.14.6.2.12	PIM for IPv6 Neighbor Table	330
6.14.7	IPMC	331
6.14.7.1	IP Multicast Global Settings	331
6.14.7.2	IP Multicast Route Settings	332
6.14.7.3	IP Multicast Forwarding Cache	333
6.14.8	IPv6MC	334
6.14.8.1	IPv6 Multicast Global Settings	

[ZEQUO6700RE/6600RE].....	334
6.14.8.2 IPv6 Multicast Routing Table	
[ZEQUO6700RE/6600RE].....	335
6.14.8.3 IPv6 Multicast Routing Forwarding Cache Table	336
6.15 IP Route Filter[ZEQUO6700RE/6600RE]	337
6.15.1 Route Map.....	337
6.16 Policy Route[ZEQUO6700RE/6600RE]	341
6.17 VRRP Settings	342
7 QoS (Quality of Service).....	345
7.1 Basic Settings.....	345
7.1.1 Port Default CoS	345
7.1.2 Port Scheduler Method	347
7.1.3 Queue Settings	349
7.1.4 CoS to Queue Mapping.....	350
7.1.5 Port Rate Limiting	351
7.1.6 Queue Rate Limiting	353
7.2 Advanced Settings	355
7.2.1 DSCP Mutation Map	355
7.2.2 Port Trust State and Mutation Binding	356
7.2.3 DSCP CoS Mapping.....	357
7.2.4 CoS Color Mapping.....	358
7.2.5 DSCP Color Mapping	359
7.2.6 Class Map	360
7.2.7 Aggregate Policer	362
7.2.8 Policy Map.....	368
7.2.9 Policy Binding.....	376
7.3 WRED (Weighted Random Early Detection)	377
7.3.1 WRED Profile	377
7.3.2 WRED Queue.....	379
7.4 Egress Buffer Settings	381
8 ACL (Access Control List)	382
8.1 ACL Configuration Wizard.....	382
8.1.1 MAC ACL.....	384
8.1.2 IPv4	387
8.1.3 IPv6	392
8.2 ACL Access List	397
8.2.1 Standard IP ACL	399
8.2.2 Extended IP ACL.....	401
8.2.3 Standard IPv6 ACL	406
8.2.4 Extended IPv6 ACL.....	408
8.2.5 Extended MAC ACL.....	413
8.2.6 Extended Expert ACL.....	416
8.3 ACL Interface Access Group	422
8.4 ACL VLAN Access Map.....	424
8.5 ACL VLAN Filter.....	426
9 Security.....	427
9.1 Port Security	427
9.1.1 Port Security Global Settings	427
9.1.2 Port Security Port Settings.....	429

9.1.3	Port Security Address Entries	431
9.2	802.1X.....	432
9.2.1	802.1X Global Settings	432
9.2.2	802.1X Forced Authorized MAC Settings	434
9.2.3	802.1X Unauthorized MAC Settings.....	435
9.2.4	802.1X Port Settings	436
9.2.5	EAP Port Config	441
9.2.6	802.1X Authenticator Statistics	442
9.3	AAA (Authentication, Authorization, and Accounting)	443
9.3.1	AAA Global Settings	443
9.3.2	AAA Authentication Settings.....	444
9.3.3	AAA Authentication User Settings.....	447
9.3.4	AAA Authentication MAC Settings.....	449
9.3.5	Application Authentication Settings	450
9.3.6	Application Accounting Settings.....	451
9.3.7	Authentication EXEC Settings.....	453
9.3.8	Accounting Settings.....	455
9.4	Authentication	457
9.4.1	Authentication Dynamic VLAN Settings.....	457
9.4.2	Authentication Status Table	459
9.4.3	2-Step Authentication Settings.....	460
9.5	RADIUS (Remote Authentication Dial-In User Service).....	461
9.5.1	RADIUS Global Settings	461
9.5.2	RADIUS Server Settings.....	463
9.5.3	RADIUS Group Server Settings	464
9.5.4	RADIUS Statistics	466
9.6	TACACS+ (Terminal Access Controller Access-Control System Plus).....	467
9.6.1	TACACS+ Global Settings.....	467
9.6.2	TACACS+ Server Settings	468
9.6.3	TACACS+ Group Server Settings	469
9.6.4	TACACS+ Statistics.....	471
9.7	SAVI (Source Address Validation Improvements)	472
9.7.1	IPv4	472
9.7.1.1	DHCPv4 Snooping.....	472
9.7.1.1.1	DHCP Snooping Global Settings.....	472
9.7.1.1.2	DHCP Snooping Port Settings	473
9.7.1.1.3	DHCP Snooping VLAN Settings	474
9.7.1.1.4	DHCP Snooping Database.....	475
9.7.1.1.5	DHCP Snooping Binding Entry.....	477
9.7.1.2	Dynamic ARP Inspection	478
9.7.1.2.1	ARP Access List.....	478
9.7.1.2.2	ARP Inspection Settings	480
9.7.1.2.3	ARP Inspection Port Settings.....	483
9.7.1.2.4	ARP Inspection Statistics	484
9.7.1.2.5	ARP Inspection Log.....	485
9.7.1.3	IP Source Guard	486
9.7.1.3.1	IP Source Guard Port Settings	486
9.7.1.3.2	IP Source Guard Binding	487
9.7.1.3.3	IP Source Guard HW Entry	489
9.8	DHCP Server Protect	490
9.8.1	DHCP Server Protect Global Settings	490
9.8.2	DHCP Server Protect Port Settings.....	491
9.9	BPDU Guard.....	492

9.10	NetBIOS Filtering.....	494
9.11	MAC Authentication	495
9.12	Web Authentication	497
9.12.1	Web Authentication Settings	497
9.12.2	Web Page Contents Settings.....	499
9.13	Trusted Host	500
9.14	Traffic Segmentation Settings	501
9.15	Storm Control	502
9.16	SSH (Secure Shell).....	505
9.16.1	SSH Global Settings	505
9.16.2	Host Key	506
9.16.3	SSH Server Connection.....	507
9.16.4	SSH User Settings	508
9.17	SSL (Secure Sockets Layer)	509
9.17.1	SSL Global Settings	509
9.17.2	Crypto PKI Trustpoint.....	510
9.17.3	SSL Service Policy	511
10	OAM (Operations, Administration & Management)	512
10.1	Cable Diagnostics.....	512
10.2	1DDM (Digital Diagnostic Monitoring).....	513
10.2.1	DDM Settings	513
10.2.2	DDM Temperature Threshold Settings.....	515
10.2.3	DDM Voltage Threshold Settings.....	516
10.2.4	DDM Bias Current Threshold Settings.....	517
10.2.5	DDM TX Power Threshold Settings.....	518
10.2.6	DDM RX Power Threshold Settings	519
10.2.7	DDM Status Table	520
11	Monitoring	521
11.1	Utilization	521
11.1.1	Port Utilization	521
11.2	Statistics	522
11.2.1	Port	522
11.2.2	Interface Counters	524
11.2.3	Counters	526
11.3	Mirror Settings.....	528
11.4	Device Environment	531
12	Eco Mode	532
12.1	Power Saving	532
12.2	EEE (Energy Efficient Ethernet)	533
13	Toolbar	534
13.1	Save.....	534
13.1.1	Save Configuration	534
13.2	Tools.....	535
13.2.1	Firmware Upgrade & Backup.....	535
13.2.1.1	Firmware Upgrade from HTTP	535
13.2.1.2	Firmware Upgrade from TFTP.....	536
13.2.1.3	Firmware Upgrade from RCP.....	537
13.2.1.4	Firmware Backup to HTTP	538

13.2.1.5	Firmware Backup to TFTP	539
13.2.1.6	Firmware Backup to RCP	540
13.2.2	Configuration Restore & Backup	541
13.2.2.1	Configuration Restore from HTTP	541
13.2.2.2	Configuration Restore from TFTP	542
13.2.2.3	Configuration Restore from RCP	543
13.2.2.4	Configuration Backup to HTTP	544
13.2.2.5	Configuration Backup to TFTP	545
13.2.2.6	Configuration Backup to RCP	546
13.2.3	Log Backup	547
13.2.3.1	Log Backup to HTTP	547
13.2.3.2	Log Backup to TFTP	548
13.2.3.3	Log Backup to RCP	549
13.2.4	Ping	550
13.2.5	Trace Route	553
13.2.6	Reset	555
13.2.7	Reboot System	556
13.3	Language	557
13.4	Logout	558
14	Appendix - System Log Entries	559
14.1	802.1X	559
14.2	AAA	560
14.3	ARP	562
14.4	Authentication (2-step)	563
14.5	BPDUGuard	565
14.6	Command	566
14.7	Configuration/Firmware	567
14.8	DAD	570
14.9	DDM	571
14.10	Debug Error	572
14.11	DHCPv6 Client	573
14.12	DHCPv6 Relay	575
14.13	DHCPv6 Server	576
14.14	DNS Resolver	577
14.15	Dynamic ARP	578
14.16	Fan	579
14.17	Interface	580
14.18	IP-Directed Broadcast	581
14.19	IP Source Guard Verify	582
14.20	LACP	583
14.21	LLDP-MED	584
14.22	Loop Detection	586
14.23	MAC-based Access Control	587
14.24	MSTP Debug Enhancement	588
14.25	OSPF[ZEQUO6700RE/6600RE]	590
14.26	Port Security	592
14.27	RADIUS	593
14.28	RRP	594
14.29	SNMP	595
14.30	Stacking	596
14.31	System	597
14.32	Telnet	598

14.33	Temperature	599
14.34	Traffic Control	600
14.35	UDLD	601
14.36	Voice VLAN	602
14.37	VRRP	603
14.38	WAC	606
14.39	Web	607
15	Appendix - System Trap Entries	608
15.1	BPDGuard	608
15.2	DDM	609
15.3	DHCP Server Protect	610
15.4	Fan	611
15.5	Gratuitous ARP	612
15.6	LLDP-MED	613
15.7	Loop Detect	614
15.8	MAC-based Access Control	615
15.9	MAC Notification	616
15.10	MSTP	617
15.11	PIM6[ZEQUO6700RE/6600RE]	618
15.12	Port Security	620
15.13	Port	621
15.14	RMON	622
15.15	SNMP Authentication	623
15.16	Stacking	624
15.17	System	625
15.18	Temperature	626
15.19	Traffic Control	627
15.20	VRRP	628

1 Introduction

The Web User Interface (Web UI) manual is intended for IT professionals who are familiar with Ethernet and Computer Networking principles. This document illustrates and explains the software features available in the Web UI of switches in this series. Switches in this series (**ZEQUO6600RE** and **ZEQUO6700RE**) are equipped with an identical set of software features available in the Web UI and will simply be referred to as the 'switch' in this document.

1.1 Related Documentation

The switch can be configured and managed not only through the Web UI, but also through the Command Line Interface (CLI). For more information about the CLI, refer to the *Panasonic ZEQUO6600RE/6700RE Command Line Interface Manual*.

2 The Web User Interface (Web UI)

2.1 Connecting to the Web UI

The Web UI of the switch can be accessed using a standard Web browser on any networking node connected to the Ethernet ports of the switch directing or indirectly. Additional security configurations can be made in the Web UI to restrict access to the switch.

The default **IPv4 Address** of the switch is 0.0.0.0 (not configured). Out of the box, the CLI should be used, through the Console port, to configure the IPv4 address of the switch. Refer to the *Panasonic ZEQUO6600RE/6700RE Command Line Interface Manual* for more information.

Open the Web browser, enter the IPv4 address of the switch into the Uniform Resource Locator (URL) address bar and press **Enter**.

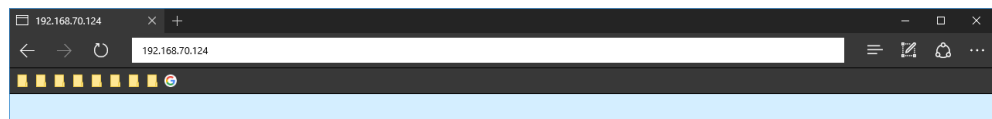


Figure 2-1 Enter IPv4 Address

The default **User Name** and **Password** is 'manager'.

Enter the **User Name** and **Password** in the spaces provided and click the Login button.

A screenshot of a web browser window displaying the login page for a switch. The page title is 'Connect to 192.168.70.125'. Below the title, the switch model 'ZEQUO 6700RE' is displayed. The login form contains three fields: 'User Name' with the value 'manager', 'Password' with masked characters (dots), and 'Language' with a dropdown menu set to 'English'. At the bottom of the form are two buttons: 'Login' and 'Reset'.

Figure 2-2 Login Window

Access to the Web UI will be given after a successful login.

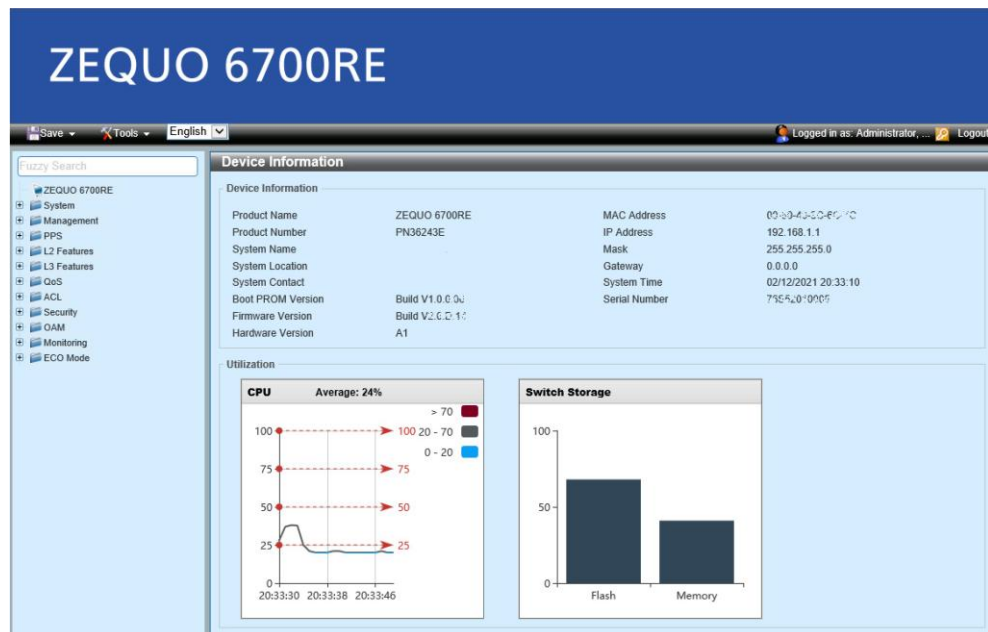


Figure 2-3 Main Web UI Window

2.2 Understanding the Web UI

The Web UI is divided into two main sections (Frame A and Frame B as illustrated in the figure below).

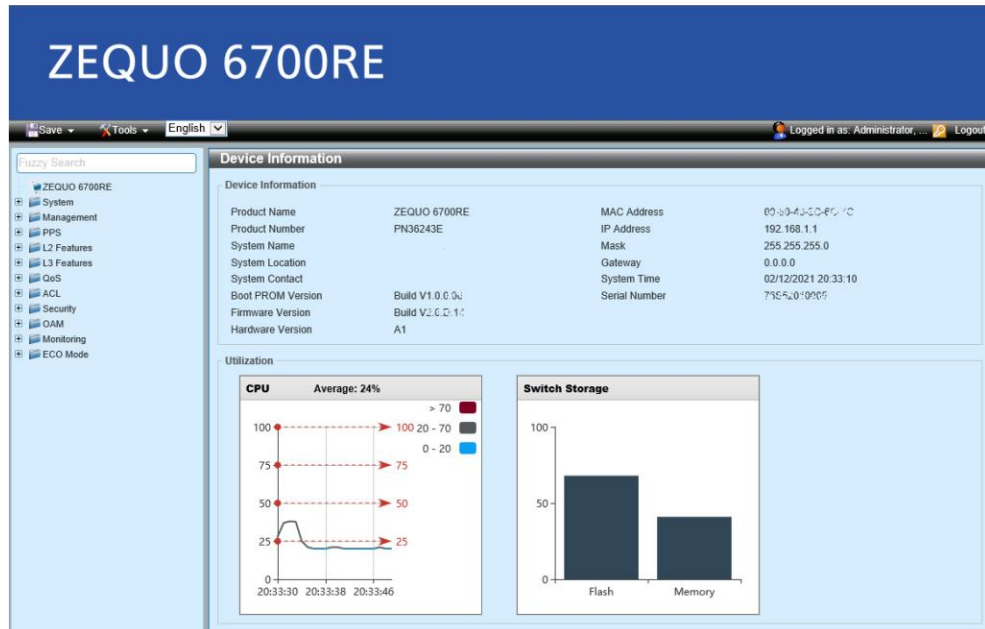


Figure 2-4

All the features available in the Web UI of the switch are grouped into folders in Frame A. In Frame A, click the folder (for example **System**) and then click the feature link (for example **System Information Settings**) to access the configuration window in Frame B. Configuration and management can be done in Frame B.

The following chapters will discuss all the software features in the order they are presented in Frame A.

3 System

3.1 Device Information

This window is used to display general switch information and utilization. This is the first window that will be displayed after logging in to the Web UI of the switch.

Click the **ZEQUO6600RE** link (in Frame A) to view the following window:

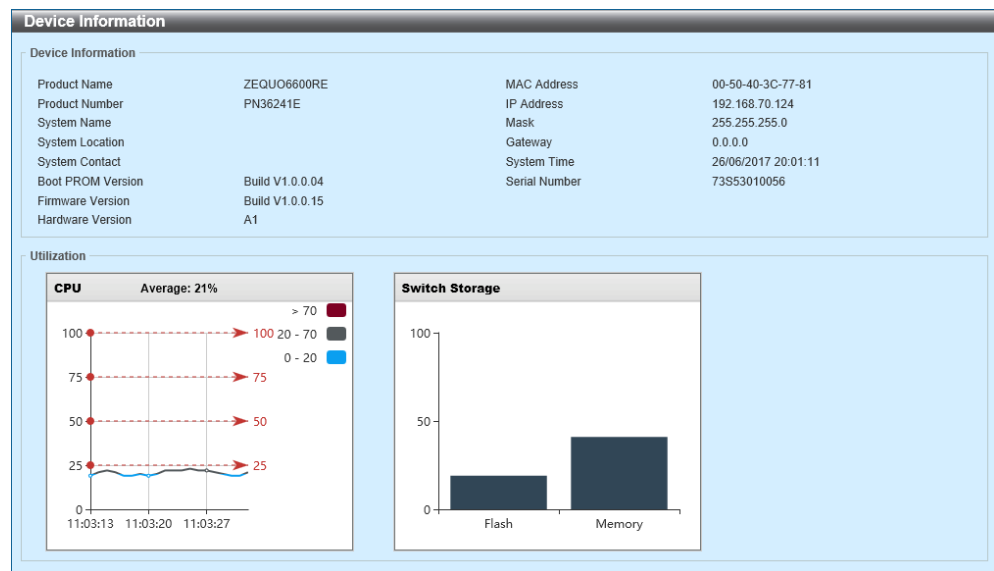


Figure 3-1 Device Information

3.2 System Information Settings

This window is used to configure and display the system information settings.

Click **System > System Information Settings** to view the following window:

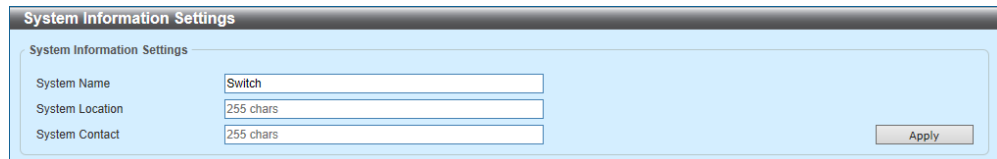


Figure 3-2 System Information Settings

The following parameters can be configured in the **System Information Settings** section:

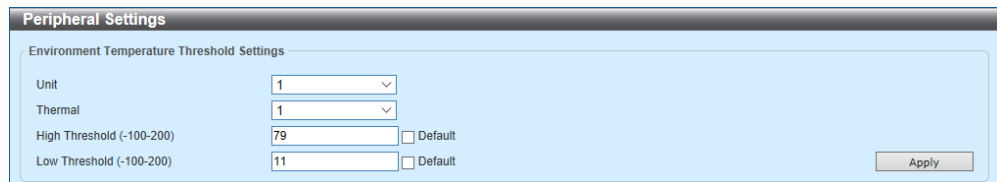
Parameter	Description
System Name	Enter a system name for the switch. This name can be used to identify the switch in the network.
System Location	Enter the location description of the switch.
System Contact	Enter a contact name for the switch. Generally, this is the name of the person or company responsible for configuring and maintaining the switch.

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

3.3 Peripheral Settings

This window is used to configure and display the peripheral settings.

Click **System > Peripheral Settings** to view the following window:



The screenshot shows a window titled "Peripheral Settings". Inside, there is a section titled "Environment Temperature Threshold Settings". This section contains four configuration items: "Unit" with a dropdown menu showing "1", "Thermal" with a dropdown menu showing "1", "High Threshold (-100-200)" with a text input field containing "79" and an unchecked "Default" checkbox, and "Low Threshold (-100-200)" with a text input field containing "11" and an unchecked "Default" checkbox. An "Apply" button is located in the bottom right corner of the settings area.

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 Configuration

3.4.1 Port Settings

This window is used to configure and display the port settings on the switch.

Click **System > Port Configuration > Port Settings** to view the following window:

Port	Link Status	Medium	State	MDIX	Flow Control	Duplex	Speed	Description
Gi1/0/1	Up	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	
Gi1/0/2	Down	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	
Gi1/0/3	Down	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	
Gi1/0/4	Down	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	
Gi1/0/5	Down	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	
Gi1/0/6	Down	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	
Gi1/0/7	Down	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	
Gi1/0/8	Down	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	
Gi1/0/9	Down	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	
Gi1/0/10	Down	Enabled	Enabled	Auto-MDIX	Off	Auto-duplex	Auto-speed	

Figure 3-4 Port Settings

The following parameters can be configured in the **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.
Medium Selecting	Select the port medium type here. Options to choose from are Auto , RJ45 and SFP . SFP stands for Small Form-factor Pluggable. Selecting the SFP option includes the use of SFP+ transceivers for 10G connectivity.
Medium Type	Select the port medium type here. Options to choose from are RJ45 and SFP . Selecting the SFP option includes the use of SFP+ transceivers for 10G connectivity.
State	Select this option to enable or disabled the physical port here.

Parameter	Description
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are: <ul style="list-style-type: none">• Auto - Select this option for auto-sensing of the optimal type of cabling.• Normal - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC LAN adapter using a straight-through cable or a port (in the MDI mode) on another Switch through a cross-over cable.• Cross - Select this option for cross-over cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another Switch through a straight cable.
Flow Control	Select to turn flow control On or Off here. Ports configured for full-duplex use 802.3x flow control and Auto ports use an automatic selection of the two. This feature will not work through Switches that are physically stacked.
Duplex	Select the duplex mode used here. Options to choose from are Auto and Full .
Speed	Select the port speed option here. This option will manually force the connection speed on the selected port to connect only at the speed specified here. The Master setting will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The Slave setting uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for master, the other side of the connection must be set for slave. Any other configuration will result in a 'link down' status for both ports.

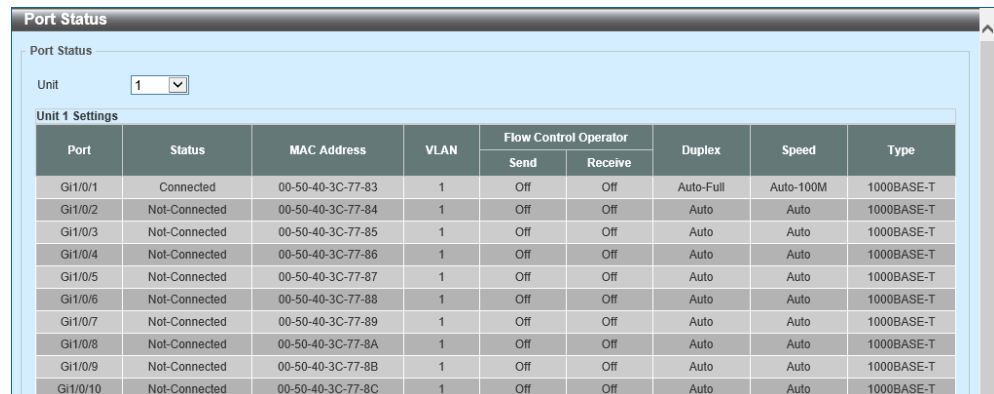
Parameter	Description
Speed	Options to choose from are: <ul style="list-style-type: none"> • Auto - Specifies that for copper ports, auto-negotiation will start to negotiate the speed and flow control with its link partner. For fiber ports, auto-negotiation will start to negotiate the clock and flow control with its link partner. • 10M - Specifies to force the port speed to 10Mbps. This option is only available for 10Mbps copper connections. • 100M - Specifies to force the port speed to 100Mbps. This option is only available for 100Mbps copper connections. • 1000M - Specifies to force the port speed to 1Gbps. This option is only available for 1Gbps fiber connections. • 1000M Master - Specifies to force the port speed to 1Gbps and operates as the master, to facilitate the timing of transmit and receive operations. This option is only available for 1Gbps copper connections. • 1000M Slave - Specifies to force the port speed to 1Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. This option is only available for 1Gbps copper connections. • 10G - Specifies to force the port speed to 10Gbps. This option is only available for 10Gbps fiber connections. • 10G Master - Specifies to force the port speed to 10Gbps and operates as the master, to facilitate the timing of transmit and receive operations. This option is only available for 10Gbps fiber connections. • 10G Slave - Specifies to force the port speed to 10Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. This option is only available for 10Gbps fiber connections.
Capability Advertised	When the Speed is set to Auto , these capabilities are advertised during auto-negotiation.
Description	Enter a description for the corresponding port here. This can be up to 64 characters.

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

3.4.2 Port Status

This window is used to display the physical port status and settings on the switch.

Click **System > Port Configuration > Port Status** to view the following window:



The screenshot shows the 'Port Status' window. At the top, there is a 'Unit' dropdown menu set to '1'. Below it, the 'Unit 1 Settings' section contains a table with the following data:

Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
Gi1/0/1	Connected	00-50-40-3C-77-83	1	Off	Off	Auto-Full	Auto-100M	1000BASE-T
Gi1/0/2	Not-Connected	00-50-40-3C-77-84	1	Off	Off	Auto	Auto	1000BASE-T
Gi1/0/3	Not-Connected	00-50-40-3C-77-85	1	Off	Off	Auto	Auto	1000BASE-T
Gi1/0/4	Not-Connected	00-50-40-3C-77-86	1	Off	Off	Auto	Auto	1000BASE-T
Gi1/0/5	Not-Connected	00-50-40-3C-77-87	1	Off	Off	Auto	Auto	1000BASE-T
Gi1/0/6	Not-Connected	00-50-40-3C-77-88	1	Off	Off	Auto	Auto	1000BASE-T
Gi1/0/7	Not-Connected	00-50-40-3C-77-89	1	Off	Off	Auto	Auto	1000BASE-T
Gi1/0/8	Not-Connected	00-50-40-3C-77-8A	1	Off	Off	Auto	Auto	1000BASE-T
Gi1/0/9	Not-Connected	00-50-40-3C-77-8B	1	Off	Off	Auto	Auto	1000BASE-T
Gi1/0/10	Not-Connected	00-50-40-3C-77-8C	1	Off	Off	Auto	Auto	1000BASE-T

Figure 3-5 Port Status

The following parameters can be configured in the **Port Status** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.

3.4.3 Port GBIC

This window is used to display information related to the transceivers plugged into the physical ports on the switch. GBIC stands for Gigabit Interface Converter.

Click **System > Port Configuration > Port GBIC** to view the following window:

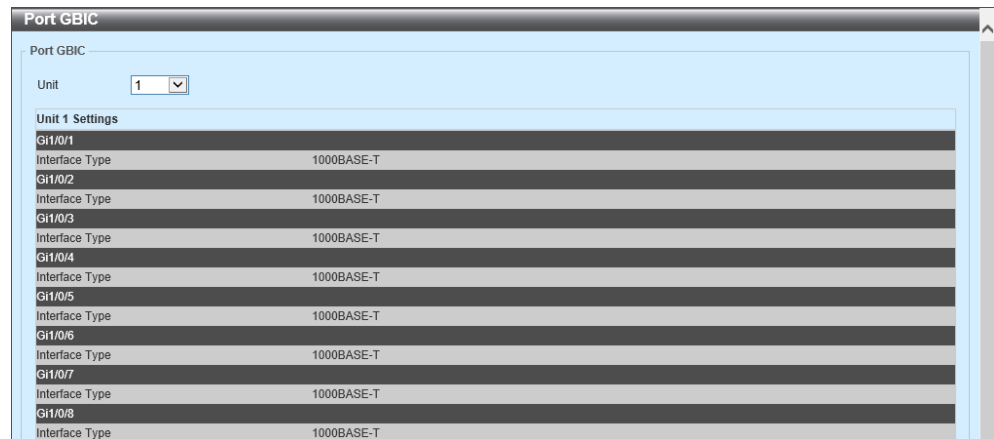


Figure 3-6 Port GBIC

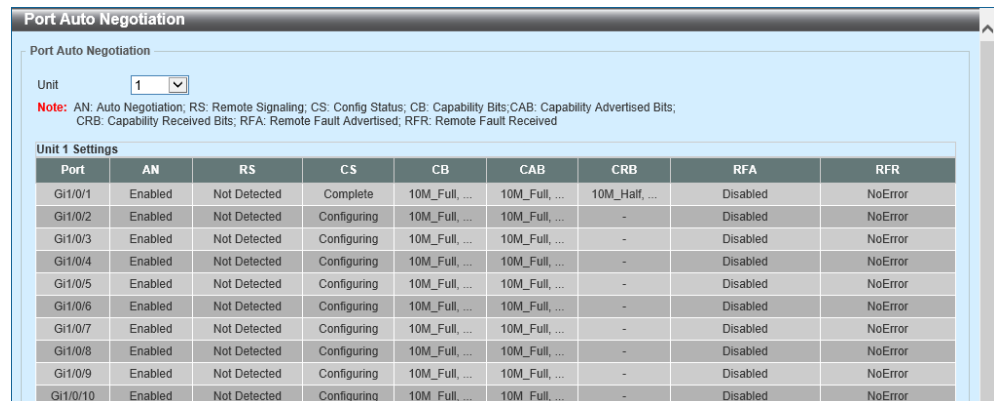
The following parameters can be configured in the **Port GBIC** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.

3.4.4 Port Auto Negotiation

This window is used to display the port auto-negotiation table and information.

Click **System > Port Configuration > Port Auto Negotiation** to view the following window:



The screenshot shows a web interface titled "Port Auto Negotiation". It includes a "Unit" dropdown menu set to "1". Below this is a "Note" explaining the abbreviations: AN (Auto Negotiation), RS (Remote Signaling), CS (Config Status), CB (Capability Bits), CAB (Capability Advertised Bits), CRB (Capability Received Bits), RFA (Remote Fault Advertised), and RFR (Remote Fault Received). The main section is "Unit 1 Settings", which contains a table with 10 columns: Port, AN, RS, CS, CB, CAB, CRB, RFA, and RFR. The table lists settings for ports Gi1/0/1 through Gi1/0/10.

Port	AN	RS	CS	CB	CAB	CRB	RFA	RFR
Gi1/0/1	Enabled	Not Detected	Complete	10M_Full, ...	10M_Full, ...	10M_Half, ...	Disabled	NoError
Gi1/0/2	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
Gi1/0/3	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
Gi1/0/4	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
Gi1/0/5	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
Gi1/0/6	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
Gi1/0/7	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
Gi1/0/8	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
Gi1/0/9	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
Gi1/0/10	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError

Figure 3-7 Port Auto Negotiation

The following parameters can be configured in the **Port Auto Negotiation** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.

3.4.5 Error Disable Settings

This window is used to configure and display the settings related to the Error Disable feature.

Click **System > Port Configuration > Error Disable Settings** to view the following window:

Figure 3-8 Error Disable Settings

The following parameters can be configured in the **Error Disable Recovery Settings** section:

Parameter	Description
ErrDisable Cause	Select the error disabled cause here. Options to choose from are All, Port Security, Storm Control, BPDU Attack Protection, Dynamic ARP Inspection, DHCP Snooping, and L2PT Guard.
State	Select to enable or disable the error disabled recovery feature here.
Interval	Enter the time, in seconds, to recover the port from the error state caused by the specified module. The range is from 5 to 86400.

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

3.4.6 Jumbo Frame

This window is used to configure and display the jumbo frame settings. Jumbo frames are Ethernet frames with more than 1518 bytes of payload.

Click **System > Port Configuration > Jumbo Frame** to view the following window:

Port	Maximum Receive Frame Size (bytes)
Gi1/0/1	1518
Gi1/0/2	1518
Gi1/0/3	1518
Gi1/0/4	1518
Gi1/0/5	1518
Gi1/0/6	1518
Gi1/0/7	1518
Gi1/0/8	1518
Gi1/0/9	1518
Gi1/0/10	1518

Figure 3-9 Jumbo Frame

The following parameters can be configured in the **Jumbo Frame** 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.
Maximum receive frame size	Receive Frame SizeEnter the maximum receive frame size value here. The range is from 64 to 9216 bytes. By default, this value is 1518 bytes.

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

3.5 System Log

3.5.1 System Log Settings

This window is used to configure and display the system log settings.

Click **System > System Log > System Log Settings** to view the following window:

The screenshot shows the 'System Log Settings' window with the following configurations:

- Log State:** Log State is set to 'Enabled'.
- Source Interface Settings:** Source Interface State is 'Disabled', Type is 'VLAN' (1-4094).
- Buffer Log Settings:** Buffer Log State is 'Enabled', Severity is '6(Informational)', Discriminator Name is '15 chars', Write Delay is '300' sec.
- Console Log Settings:** Console Log State is 'Disabled', Severity is '4(Warnings)', Discriminator Name is '15 chars'.
- SMTP Log Settings:** SMTP Log State is 'Disabled', Severity is '4(Warnings)', Discriminator Name is '15 chars'.
- Log Trap Link Change Delay Settings:** Log Trap Link Change Delay is set to '3' sec.

Figure 3-10 System Log Settings

The following parameters can be configured in the **Log State** section:

Parameter	Description
Log State	Select the enable or disable the global system log state here.

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

The following parameters can be configured in the **Source Interface Settings** section:

Parameter	Description
Source Interface State	Select this option to enable or disable the global source interface state.
Type	Select the type of interface that will be used. Options to choose from are Loopback and VLAN .
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. The range of loopback interfaces are from 1 to 8.

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

The following parameters can be configured in the **Buffer Log Settings** section:

Parameter	Description
Buffer Log State	Select to enable or disable the global buffer log state here. Options to choose from are Enable , Disabled , and Default . When selecting the Default option, the global buffer log state will follow the default behavior.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) .
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long. This specifies the name of the discriminator profile that will be used to filter buffer log messages based on the filtering criteria specified within that profile.
Write Delay	Enter the write delay value for the log here. The range is from 0 to 65535 seconds. By default, this value is 300 seconds. Select the Infinite option, to disable the write delay feature.

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

The following parameters can be configured in the **Console Log** Settings section:

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

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

The following parameters can be configured in the **SMTP Log Settings** section:

Parameter	Description
SMTP Log State	Select to enable or disable the global Simple Mail Transfer Protocol (SMTP) log state here.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) .
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long. This specifies the name of the discriminator profile that will be used to filter SMTP log messages based on the filtering criteria specified within that profile.

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.

3.5.2 System Log Discriminator Settings

This window is used to configure and display the discriminator settings used in the system log.

Click **System > System Log > System Log Discriminator Settings** to view the following window:

Figure 3-11 System Log Discriminator Settings

The following parameters can be configured in the **Discriminator Log Settings** section:

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

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

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

3.5.3 System Log Server Settings

This window is used to configure and display the server settings used by the system log.

Click **System > System Log > System Log Server Settings** to view the following window:

Figure 3-12 System Log Server Settings

The following parameters can be configured in the **Log Server** section:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address for the system log server here.
Host IPv6 Address	Enter the IPv6 address for the system log server here.
UDP Port	Enter the User Datagram Protocol (UDP) port number for the system log server here. This value must be either 514 or between 1024 and 65535. By default, this value is 514.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) .

Parameter	Description		
Facility	Select the facility number that will be logged here. The range is from 0 to 23. Each facility number is associated with a specific facility. See the table below:		
	Facility Number	Facility Name	Facility Description
	1	user	User-level messages
	2	mail	Mail system
	3	daemon	System daemons
	4	auth1	Security/authorization messages
	5	syslog	Messages generated internally by the SYSLOG
	6	lpr	Line printer sub-system
	7	news	Network news sub-system
	8	uucp	UUCP sub-system
	9	clock1	Clock daemon
	10	auth2	Security/authorization messages
	11	ftp	FTP daemon
	12	ntp	NTP subsystem
	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 the name of the discriminator that will be used to filter messages sent to the log server here. This name can be up to 15 characters long.		

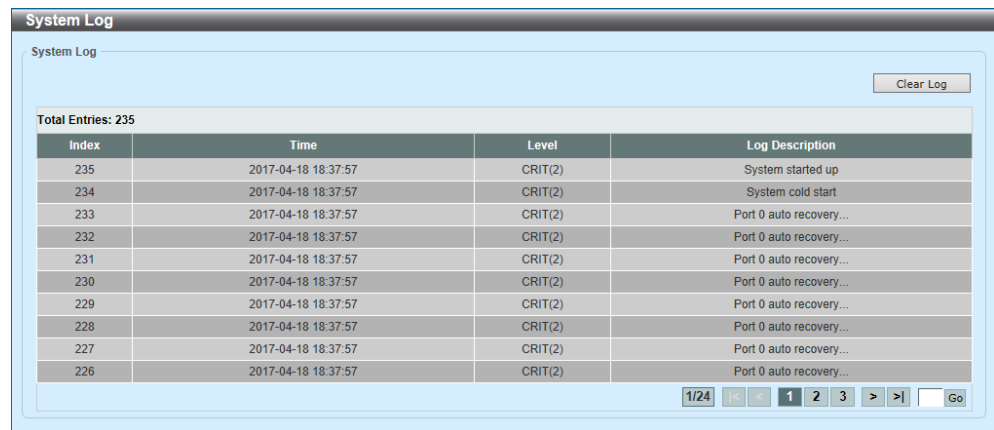
Click the **Apply** button to add a new entry based on the information specified.

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

3.5.4 System Log

This window is used to display and clear the system log.

Click **System > System Log > System Log** to view the following window:



The screenshot shows a web interface titled "System Log". It features a "Clear Log" button in the top right corner. Below the button, it states "Total Entries: 235". A table displays log entries with columns for Index, Time, Level, and Log Description. The table shows entries from index 235 down to 226. At the bottom right, there is a pagination control showing "1/24" and buttons for navigating between pages (1, 2, 3, etc.) and a "Go" button.

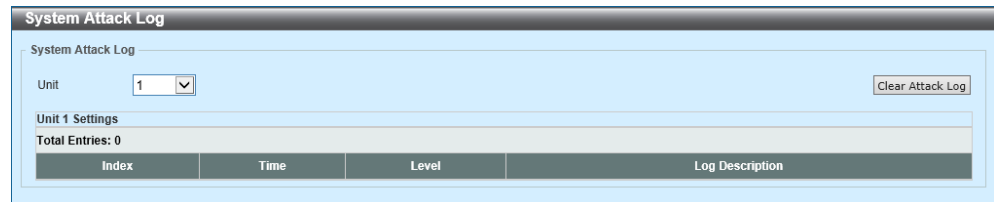
Index	Time	Level	Log Description
235	2017-04-18 18:37:57	CRIT(2)	System started up
234	2017-04-18 18:37:57	CRIT(2)	System cold start
233	2017-04-18 18:37:57	CRIT(2)	Port 0 auto recovery...
232	2017-04-18 18:37:57	CRIT(2)	Port 0 auto recovery...
231	2017-04-18 18:37:57	CRIT(2)	Port 0 auto recovery...
230	2017-04-18 18:37:57	CRIT(2)	Port 0 auto recovery...
229	2017-04-18 18:37:57	CRIT(2)	Port 0 auto recovery...
228	2017-04-18 18:37:57	CRIT(2)	Port 0 auto recovery...
227	2017-04-18 18:37:57	CRIT(2)	Port 0 auto recovery...
226	2017-04-18 18:37:57	CRIT(2)	Port 0 auto recovery...

Figure 3-13 System Log

Click the **Clear Log** button to clear the log entries from the table.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

3.5.5 System Attack Log

This window is used to display and clear the system attack log. Click **System > System Log > System Attack Log** to view the following window:



The screenshot shows a web interface for the 'System Attack Log'. At the top, there's a title bar. Below it, a section titled 'System Attack Log' contains a 'Unit' dropdown menu with '1' selected and a 'Clear Attack Log' button. Below this is a section titled 'Unit 1 Settings' which shows 'Total Entries: 0'. At the bottom, there's a table with four columns: 'Index', 'Time', 'Level', and 'Log Description'.

Figure 3-14 System Attack Log

The following parameters can be configured in the **System Attack Log** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.

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

3.5.6 System Authentication Log

This window is used to configure and display the system authentication log.

Click **System > System Log > System Authentication Log** to view the following window:

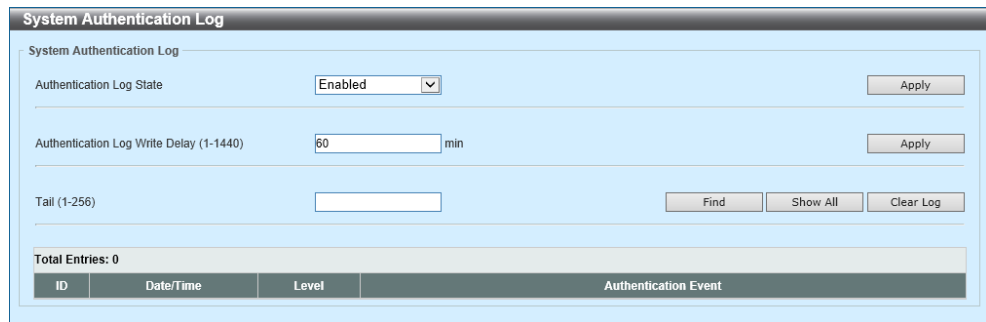


Figure 3-15 System Authentication Log

The following parameters can be configured in the **System Authentication Log** section:

Parameter	Description
Authentication Log State	Select to enable or disable the authentication log here.
Authentication Log Write Delay	Enter the write delay value for the authentication log here. The range is from 1 to 1440 minutes.
Tail	Enter the number of the latest authentication log entries that will be displayed. The range is from 1 to 256.

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

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

3.6 Time and SNTP (Simple Network Time Protocol)

3.6.1 Clock Settings

This window is used to configure and display the time and date settings used by time dependent features on the switch.

Click **System > Time and SNTP > Clock Settings** to view the following window:

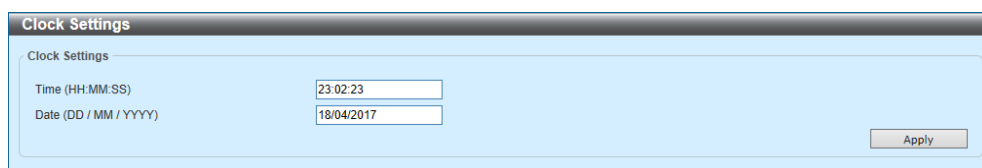


Figure 3-16 Clock Settings

The following parameters can be configured in the **Clock Settings** section:

Parameter	Description
Time	Enter the current time in hours (HH), minutes (MM), and seconds (SS) here. For example, 19:20:20.
Date	Enter the current day (DD), month (MM), and year (YYYY) here. For example, 25/04/2017.

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

3.6.2 Time Zone Settings

This window is used to configure and display the Daylight Savings Time (DST) and Time Zone settings.

Click **System > Time and SNTP > Time Zone Settings** to view the following window:

Figure 3-17 Time Zone Settings

The following parameters can be configured in the first section:

Parameter	Description
Summer Time State	Select the summer time setting. Options to choose from are: <ul style="list-style-type: none"> • Disabled - Select to disable the summer time setting. • Recurring Setting - Select to configure the summer time that should start and end on the specified weekday of the specified month. • Date Setting - Select to configure the summer time that should start and end on the specified date of the specified month.
Time Zone	Select to specify the local time zone offset from Coordinated Universal Time (UTC).

The following parameters can be configured in the **Recurring Setting** section:

Parameter	Description
From: Week of the Month	Select week of the month that summer time will start.
From: Day of the Week	Select the day of the week that summer time will start.
From: Month	Select the month that summer time will start.
From: Time	Select the time of the day that summer time will start.
To: Week of the Month	Select week of the month that summer time will end.
To: Day of the Week	Select the day of the week that summer time will end.
To: Month	Select the month that summer time will end.
To: Time	Select the time of the day that summer time will end.
Offset	Enter the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

The following parameters can be configured in the **Date Setting** section:

Parameter	Description
From: Date of the Month	Select date of the month that summer time will start.
From: Month	Select the month that summer time will start.
From: Year	Enter the year that the summer time will start.
From: Time	Select the time of the day that summer time will start.
To: Date of the Month	Select date of the month that summer time will end.
To: Month	Select the month that summer time will end.
To: Year	Enter the year that the summer time will end.
To: Time	Select the time of the day that summer time will end.
Offset	Enter the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

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

3.6.3 SNTP Settings

This window is used to configure and display the Simple Network Time Protocol (SNTP) settings. SNTP is used to synchronize the date and time settings of the switch with the settings hosted by an SNTP server automatically and periodically.

Click **System > Time and SNTP > SNTP Settings** to view the following window:

Figure 3-18 SNTP Settings

The following parameters can be configured in the **SNTP Global Settings** section:

Parameter	Description
SNTP State	Select to globally enable or disable SNTP here.
Poll Interval	Enter the synchronizing interval in seconds. The value is from 30 to 99999 seconds. The default interval is 720 seconds.

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

The following parameters can be configured in the **SNTP Server Setting** section:

Parameter	Description
IPv4 Address	Enter the IPv4 address of the SNTP server here.
IPv6 Address	Enter the IPv6 address of the SNTP server here.

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

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

3.7 Time Range

This window is used to configure and display time range profiles.

Click **System > Time Range** to view the following window:

Figure 3-19 Time Range

The following parameters can be configured in the **Time Range** section:

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

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

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

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.

4 Management

4.1 Command Logging

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

Click **Management > Command Logging** to view the following window:

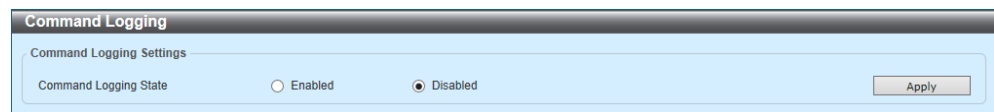


Figure 4-1 Command Logging

The following parameters can be configured in the **Command Logging Settings** section:

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

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.

Click **Management > User Accounts Settings** to view the following window:

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

The following parameters can be configured in the **User Management Settings** section:

Parameter	Description
User Name	Enter the user account name here. This name can be up to 32 characters long.
Privilege	Enter the privilege level for this account here. 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 view the following window:

User Accounts Settings

User Management Settings

Session Table

Total Entries: 2

ID	Type	User Name	Privilege	Login Time	IP Address
0	console	Anonymous	1	1M30S	
19	* web	manager	15	1M17S	192.168.70.14

1/1

<<

<

1

>

>>

Go

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

This window is used to enable or disable user account encryption.

Click **Management > User Accounts Encryption** to view the following window:

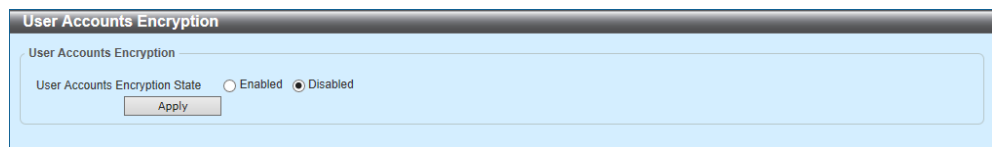


Figure 4-4 User Accounts Encryption

The following parameters can be configured in the **User Accounts Encryption** section:

Parameter	Description
User Accounts Encryption State	Select to enable or disable user account encryption here.

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

4.4 Login Method

This window is used to configure and display the login method for each login application supported on the switch.

Click **Management > Login Method** to view the following window:

Figure 4-5 Login Method

The following parameters can be configured in the **Enable Password** section:

Parameter	Description
Level	Select the privilege level for the user account here. The range is from 1 to 15.
Password Type	Select the password type for the user here. Options to choose from are: <ul style="list-style-type: none"> Plain Text - Specifies that the password will be in plain text. This is the default option. Encrypted - Specifies that the password will be encrypted based on SHA-1.
Password	Enter the password for the user account here. <ul style="list-style-type: none"> In the plain-text form, the password can be up to 32 characters long, is case-sensitive, and can contain spaces. In the encrypted form, the password must be 35 bytes long and is case-sensitive.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to edit the settings of the entry.

The following parameters can be configured in the **Login Method** section:

Parameter	Description
Login Method	<p>After clicking the Edit button, this parameter can be configured. Select the login method for the specified application here. Options to choose from are:</p> <ul style="list-style-type: none"> • No Login - This requires no login authentication to access the specified application. • Login - This requires the user to enter a password when trying to access the specified application. • Login Local - This requires the user to enter a username and a password to access the specified application.

The following parameters can be configured in the **Login Password** section:

Parameter	Description
Application	Select the application that will be configured here. Options to choose from are Console , Telnet and Secure Shell (SSH) .
Password Type	Select the password encryption type that will be used here. Options to choose from are Plain Text and Encrypted .
Password	<p>Enter the password for the selected application here. This password will be used when the Login Method for the specified application is set as Login.</p> <ul style="list-style-type: none"> • In the plain-text form, the password can be up to 32 characters long, is case-sensitive, and can contain spaces. • In the encrypted form, the password must be 35 bytes long and is case-sensitive.

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

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

4.5 SNMP (Simple Network Management Protocol)

4.5.1 SNMP Global Settings

This window is used to configure and display the global SNMP settings.

Click **Management > SNMP > SNMP Global Settings** to view the following window:

Figure 4-6 SNMP Global Settings

The following parameters can be configured in the **SNMP Global Settings** section:

Parameter	Description
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 65535.
Trap Source Interface	Enter the interface whose IP address will be used as the source address for sending the SNMP trap packet.

The following parameters can be configured in the **Trap Settings** section:

Parameter	Description
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

This window is used to configure and display the SNMP Linkchange trap settings.

Click **Management > SNMP > SNMP Linkchange Trap Settings** to view the following window:

Port	Trap Sending	Trap State
Gi1/0/1	Enabled	Enabled
Gi1/0/2	Enabled	Enabled
Gi1/0/3	Enabled	Enabled
Gi1/0/4	Enabled	Enabled
Gi1/0/5	Enabled	Enabled
Gi1/0/6	Enabled	Enabled
Gi1/0/7	Enabled	Enabled
Gi1/0/8	Enabled	Enabled
Gi1/0/9	Enabled	Enabled
Gi1/0/10	Enabled	Enabled

Figure 4-7 SNMP Linkchange Trap Settings

The following parameters can be configured 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

This window is used 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.

Click **Management > SNMP > SNMP View Table Settings** to view the following window:

The screenshot shows the 'SNMP View Table Settings' window. It has three input fields at the top: 'View Name *' with a placeholder '32 chars', 'Subtree OID *' with a placeholder 'N.N.N..N', and 'View Type' with a dropdown menu set to 'Included'. Below these fields is an 'Add' button. A table below shows 'Total Entries: 8'. The table has four columns: 'View Name', 'Subtree OID', 'View Type', and a 'Delete' button for each entry.

View Name	Subtree OID	View Type	Delete
restricted	1.3.6.1.2.1.1	Included	Delete
restricted	1.3.6.1.2.1.1.1	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

The following parameters can be configured in the **SNMP View Settings** section:

Parameter	Description
View Name	Enter the SNMP view name here. 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 here. 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 here. Options to choose from 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.

Click **Management > SNMP > SNMP Community Table Settings** to view the following window:

Community Name	View Name	Access Right	IP Access-List Name	
public	CommunityView	ro		Delete
private	CommunityView	rw		Delete

Figure 4-9 SNMP Community Table Settings

The following parameters can be configured in the **SNMP Community Settings** section:

Parameter	Description
Key Type	Select the key type for the SNMP community. Options to choose from are Plain Text and Encrypted .
Community Name	Enter the SNMP community name here. This is used 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. This is used 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	Description
Access Right	Select the access right here. Options to choose from 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

This window is used to configure and display the SNMP group table settings. SNMP groups map SNMP users to SNMP views.

Click **Management > SNMP > SNMP Group Table Settings** to view the following window:

Group Name	Read View Name	Write View Name	Notify View Name	Security Model	Security Level	IP Address-List Name	Delete
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

The following parameters can be configured in the **SNMP Group Settings** section:

Parameter	Description
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 to choose from 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	Description
Security Level	After selecting to use SNMPv3 as the User-based Security Model , select the security level here. Options to choose from 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.

Click **Management > SNMP > SNMP Engine ID Local Settings** to view the following window:

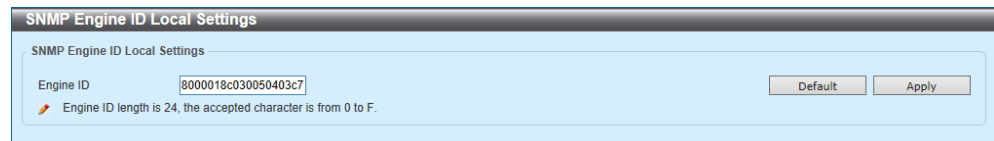
The image shows a web-based configuration window titled "SNMP Engine ID Local Settings". Inside the window, there is a label "Engine ID" followed by a text input field containing the hexadecimal string "8000018c030050403c7". To the right of the input field are two buttons: "Default" and "Apply". Below the input field, there is a small red pencil icon and a message: "Engine ID length is 24, the accepted character is from 0 to F."

Figure 4-11 SNMP Engine ID Local Settings

The following parameters can be configured in the **SNMP Engine ID Local Settings** section:

Parameter	Description
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.

Click **Management > SNMP > SNMP User Table Settings** to view the following window:

Figure 4-12 SNMP User Table Settings

The following parameters can be configured in the **SNMP User Settings** section:

Parameter	Description
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 to choose from are v1 , v2c , and v3 .
SNMP V3 Encryption	After selecting v3 as the SNMP Version , select the SNMPv3 encryption here. Options to choose from 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 to choose from 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	Description
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 to choose from 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 to choose from 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 to choose from 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.

Click **Management > SNMP > SNMP Host Table Settings** to view the following window:

Figure 4-13 SNMP Host Table Settings

The following parameters can be configured in the **SNMP Host Settings** section:

Parameter	Description
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 to choose from 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 to choose from 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	Description
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

This window is used to enable or disable the rising and falling alarm trap states for RMON.

Click **Management > RMON > RMON Global Settings** to view the following window:



Figure 4-14 RMON Global Settings

The following parameters can be configured in the **RMON Global Settings** section:

Parameter	Description
RMON Rising Alarm Trap	Select to enable or disable the RMON Rising Alarm Trap feature.
RMON Falling Alarm Trap	Select to enable or disable the RMON Falling Alarm Trap feature.

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

4.6.2 RMON Statistics Settings

This window is used to configure and display the RMON statistics and settings for the specified port.

Click **Management > RMON > RMON Statistics Settings** to view the following window:

Figure 4-15 RMON Statistics Settings

The following parameters can be configured in the **RMON Statistics Settings** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Index	Enter the RMON table index. The value is from 1 to 65535.
Owner	Enter the owner string. The string can be up to 127 characters.

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

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

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to view the following window:

Figure 4-16 RMON Statistics Settings (Show Detail)

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

4.6.3 RMON History Settings

This window is used to configure and display the RMON history settings for the specified port.

Click **Management > RMON > RMON History Settings** to view the following window:

Figure 4-17 RMON History Settings

The following parameters can be configured in the **RMON History Settings** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Index	Enter the index number of the entry in the history group table here. The range is from 1 to 65535.
Bucket Number	Enter the number of buckets specified for the RMON collection history group of statistics. The range is from 1 to 65535. The default value is 50.
Interval	Enter interval time for each polling cycle here. The range is from 1 to 3600 seconds.
Owner	Enter the owner string here. The string can be up to 127 characters long.

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

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

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to view 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
<div>Back</div>													

Figure 4-18 RMON History Settings (Show Detail)

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

4.6.4 RMON Alarm Settings

This window is used to configure and display the RMON alarm settings.

Click **Management > RMON > RMON Alarm Settings** to view the following window:

Figure 4-19 RMON Alarm Settings

The following parameters can be configured in the **RMON Alarm Settings** section:

Parameter	Description
Index	Enter the alarm index. The range is from 1 to 65535.
Interval	Enter the interval in seconds for the sampling of the variable and checking against the threshold. The valid range is from 1 to 2147483648 seconds.
Variable	Enter the object identifier of the variable to be sampled.
Type	Select the monitoring type. Options to choose from are Absolute and Delta .
Rising Threshold	Enter the rising threshold value between 0 and 2147483647.
Falling Threshold	Enter the falling threshold value between 0 and 2147483647.
Rising Event Number	Enter the index of the event entry that is used to notify the rising threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the rising threshold.
Falling Event Number	Enter the index of the event entry that is used to notify the falling threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the falling threshold.
Owner	Enter the owner string up to 127 characters.

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

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

4.6.5 RMON Event Settings

This window is used to configure and display the RMON event settings.

Click **Management > RMON > RMON Event Settings** to view the following window:

Figure 4-20 RMON Event Settings

The following parameters can be configured in the **RMON Event Settings** section:

Parameter	Description
Index	Enter the index value of the alarm entry here. The range is from 1 to 65535.
Description	Enter a description for the RMON event entry. The string is up to 127 characters long.
Type	Select the RMON event entry type. Options to choose from are None , Log , Trap , and Log and Trap .
Community	Enter the community string. The string can be up to 127 characters.
Owner	Enter the owner string. The string can be up to 127 characters.

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

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

Click the **View Logs** button to display the log entries associated with the specified entry.

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

Click the **View Logs** button to view the following window:

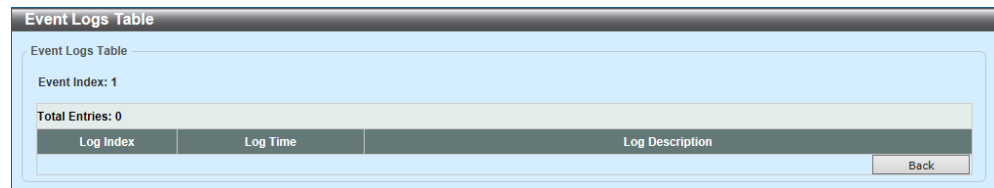


Figure 4-21 RMON Event Settings (View Logs)

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

4.7 Telnet/Web

This window is used to configure and display the Telnet and Web settings on the switch.

Click **Management > Telnet/Web** to view the following window:

Figure 4-22 Telnet/Web

The following parameters can be configured in the **Telnet Settings** section:

Parameter	Description
Telnet State	Select to enable or disable the Telnet server feature here.
Port	Enter the Transmission Control Protocol (TCP) port number used for Telnet management of the Switch. The well-known TCP port for the Telnet protocol is 23.

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

The following parameters can be configured in the **Web Settings** section:

Parameter	Description
Web State	Select this option to enable or disable the configuration through the web.
Port	Enter the TCP port number used for Telnet management of the Switch. The well-known TCP port for the Telnet protocol is 80.

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

4.8 Session Timeout

This window is used to configure and display the session timeout settings for Web, Console, Telnet, and SSH connections.

Click **Management > Session Timeout** to view the following window:

Session Timeout	Value	Unit	Default
Web Session Timeout (60-36000)	60	sec	<input type="checkbox"/>
Console Session Timeout (0-1439)	3	min	<input type="checkbox"/>
Telnet Session Timeout (0-1439)	3	min	<input checked="" type="checkbox"/>
SSH Session Timeout (0-1439)	3	min	<input checked="" type="checkbox"/>

Figure 4-23 Session Timeout

The following parameters can be configured in the **Session Timeout** section:

Parameter	Description
Web Session Timeout	Enter the time in seconds of the web session timeout. Tick the Default check box to return to the default setting. The value is from 60 to 36000 seconds. The default value is 180 seconds.
Console Session Timeout	Enter the time in minutes of the console session timeout. Tick the Default check box to return to the default setting. The value is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes.
Telnet Session Timeout	Enter the time in minutes of the Telnet session timeout. Tick the Default check box to return to the default setting. The value is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes.
SSH Session Timeout	Enter the time in minutes of the SSH session timeout. Tick the Default check box to return to the default setting. The value is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes.

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

4.9 DHCP (Dynamic Host Configuration Protocol)

4.9.1 Service DHCP

This window is used to enable or disable the DHCP and DHCPv6 service features. DHCPv6 stands for Dynamic Host Configuration Protocol Version 6 or the Dynamic Host Configuration Protocol for IPv6.

Click **Management > DHCP > Service DHCP** to view the following window:



Figure 4-24 Service DHCP

The following parameters can be configured in the **Service DHCP** section:

Parameter	Description
Service DHCP State	Select this option to enable or disable the DHCP service feature.

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

The following parameters can be configured in the **Service IPv6 DHCP** section:

Parameter	Description
Service IPv6 DHCP State	Select this option to enable or disable the DHCPv6 service feature.

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

4.9.2 DHCP Class Settings

This window is used to configure and display the DHCP class settings.

Click **Management > DHCP > DHCP Class Settings** to view the following window:

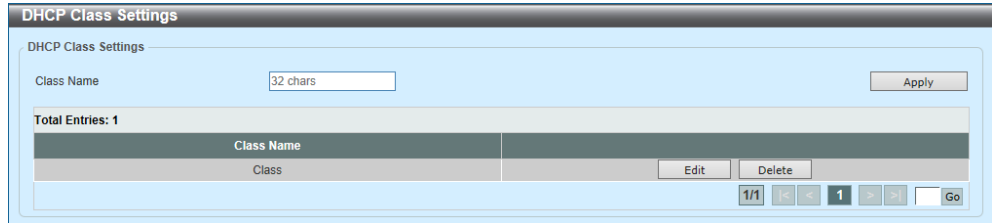


Figure 4-25 DHCP Class Settings

The following parameters can be configured in the **DHCP Class Settings** section:

Parameter	Description
Class Name	Enter the DHCP class name with a maximum of 32 characters.

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

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

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 **Edit** button to view the following window:

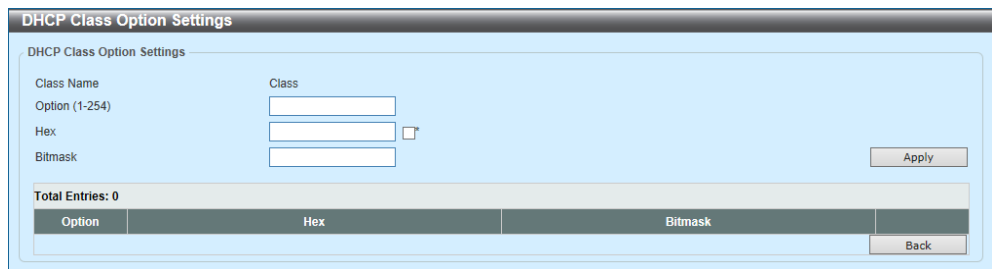


Figure 4-26 DHCP Class Settings (Edit)

The following parameters can be configured in the **DHCP Class Option Settings** section:

Parameter	Description
Option	Enter the DHCP option number. The range is from 1 to 255.
Hex	Enter the hex pattern of the specified DHCP option. Select the check box ignore the remaining bits of the option.
Bitmask	Enter the hex bit mask for masking of the pattern. The masked pattern bits will be matched. If not specified, all bits entered in the Hex field will be checked.

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

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

4.9.3 DHCP Pool Settings

This window is used to configure and display the DHCP pool settings.

Click **Management > DHCP > DHCP Pool Settings** to view the following window:

Figure 4-27 DHCP Pool Settings

The following parameters can be configured in the **DHCP Pool** section:

Parameter	Description
DHCP Pool Name	Enter the DHCP pool name here. This can be up to 32 characters long.

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

The following parameters can be configured in the **DHCP Pool Table** section:

Parameter	Description
DHCP Pool Name	Enter the DHCP pool name here. This can be up to 32 characters long.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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.

4.9.4 DHCP Server

4.9.4.1 DHCP Server Global Settings

This window is used to configure and display the global DHCP server settings.

Click **Management > DHCP > DHCP Server > DHCP Server Global Settings** to view the following window:

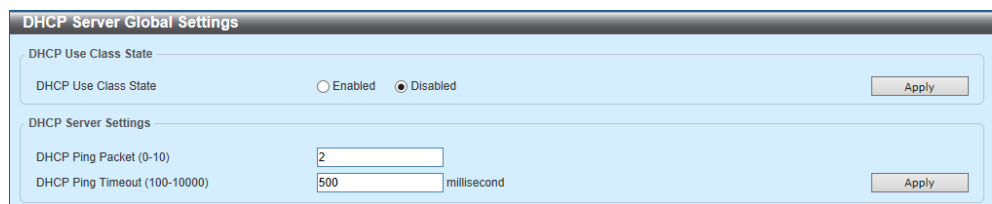


Figure 4-28 DHCP Server Global Settings

The following parameters can be configured in the **DHCP Use Class State** section:

Parameter	Description
DHCP Use Class State	Select to enable or disable the DHCP Use Class State here. When enabled, the DHCP server will use DHCP classes for address allocation.

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

The following parameters can be configured in the **DHCP Server Settings** section:

Parameter	Description
DHCP Ping Packet	Enter the number of ping packets that the Switch will send out on the network containing the IP address to be allotted. If the ping request is not returned, the IP address is considered unique to the local network and then allotted to the requesting client. A value of 0 means there is no ping test. The range is from 0 to 10. The default value is 2.
DHCP Ping Timeout	Enter the amount of time the DHCP server must wait before timing out a ping packet. The range is from 100 to 10000 milliseconds. The default value is 500 milliseconds.

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

4.9.4.2 DHCP Server Pool Settings

This window is used to configure and display the DHCP server pool settings.

Click **Management > DHCP > DHCP Server > DHCP Server Pool Settings** to view the following window:

Figure 4-29 DHCP Server Pool Settings

The following parameters can be configured in the **DHCP Server Pool Settings** section:

Parameter	Description
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

Click the **Edit Class** button to edit the DHCP class settings related to the specified entry.

Click the **Edit Option** button to edit the DHCP Option settings related to the specified entry.

Click the **Configure** button to configure the DHCP settings related to the specified entry.

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

Click the **Edit Class** button to view the following window:

Figure 4-30 DHCP Server Pool Settings (Edit Class)

The following parameters can be configured in the **DHCP Server Pool Class Settings** section:

Parameter	Description
Class Name	Select an existing DHCP class name here that will be associated with this DHCP pool.
Start Address	Enter the starting IPv4 address that will be associated with the DHCP class in the DHCP pool here.
End Address	Enter the ending IPv4 address that will be associated with the DHCP class in the DHCP pool here.

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

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

Click the **Delete by Address** button to remove the configured start and end addresses from the entry.

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

Click the **Edit Option** button to view the following window:

Figure 4-31 DHCP Server Pool Settings (Edit Option)

The following parameters can be configured in the **DHCP Server Pool Option Settings** section:

Parameter	Description
Option	Enter the DHCP option number here. The range is from 1 to 254.
Type	<p>Select the DHCP option type here. Options to choose from are:</p> <ul style="list-style-type: none"> • ASCII - Enter the American Standard Code for Information Interchange (ASCII) string in the space provided. This string can be up to 255 characters long. • HEX - Enter the hexadecimal string in the space provided. This string can be up to 254 characters long. Select the None option to specify a zero-length hexadecimal string. • IP - Enter the IPv4 address(es) in the space(s)

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

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

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

Click the **Configure** button to view the following window:

Figure 4-32 DHCP Server Pool Settings (Configure)

The following parameters can be configured in the **DHCP Server Pool Configure** section:

Parameter	Description
Boot File	Enter the boot file name here. This can be up to 64 characters long.
Domain Name	Enter the domain name for the DHCP client here. This can be up to 64 characters long.
Network (IP/Mask)	Enter the network IPv4 address and subnet mask for the DHCP client here.
Next Server	Enter the next server IPv4 address here. The boot image file is stored on this server and can be retrieved by DHCP clients using this IP address. The server is typically a Trivial File Transfer Protocol (TFTP) server. Only one next server IP address can be specified.
Default Router	Enter the IPv4 address of the default router for the DHCP client here. Up to 8 IPv4 address can be entered here. The IP address of the router should be on the same subnet as the client's subnet. Routers are listed in the order of preference. If default routers are already configured, the default routers configured later will be added to the default interface list.

Parameter	Description
DNS Server	Enter the IPv4 address to be used by the DHCP client as the Domain Name System (DNS) server here. Up to 8 IPv4 address can be entered here. Servers are listed in the order of preference. If DNS servers are already configured, the DNS servers configured later will be added to the DNS server list.
NetBIOS Name Server	Enter the Windows Internet Name Service (WINS) name server IPv4 address for the DHCP client here. Up to 8 IPv4 address can be entered here. Servers are listed in the order of preference. If name servers are already configured, the name server configured later will be added to the default interface list. NetBIOS stands for Network Basic Input/Output System.
NetBIOS Node Type	Select the NetBIOS node type for Microsoft DHCP clients here. The node type determines the method that NetBIOS uses to register and resolve names. Options to choose from are: <ul style="list-style-type: none"> • Broadcast - A Broadcast system uses broadcasts. • Peer To Peer - A Peer To Peer (p-node) system uses only point-to-point name queries to a name server (WINS). • Mixed - A Mixed (m-node) system broadcasts first, and then queries the name server. • Hybrid - A Hybrid (h-node) system queries the name
Lease	Enter and select the lease time for an IPv4 address that is assigned from the address pool here. <ul style="list-style-type: none"> • Enter the Days in the range from 0 to 365. • Select the Hours and Minutes from the drop-down menus. • Alternatively, the Infinite option can be selected to specify that the lease time is unlimited.

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

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

4.9.4.3 DHCP Server Exclude Address

This window is used to configure and display the range of IPv4 addresses that will be excluded from being allocated to DHCP clients. Multiple IPv4 addresses can be excluded.

Click **Management > DHCP > DHCP Server > DHCP Server Exclude Address** to view the following window:

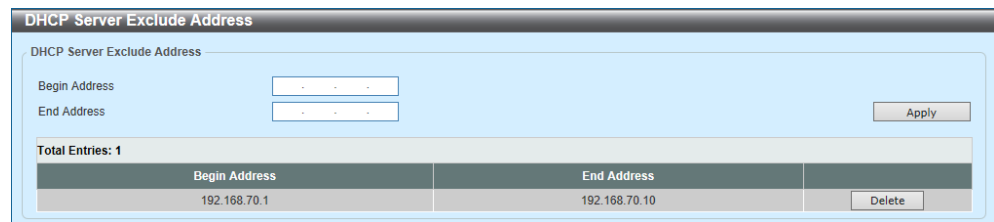


Figure 4-33 DHCP Server Exclude Address

The following parameters can be configured in the **DHCP Server Exclude Address** section:

Parameter	Description
Begin Address	Enter the first IPv4 address of a range of addresses to be excluded here.
End Address	Enter the last IPv4 address of a range of addresses to be excluded here.

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

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

4.9.4.4 DHCP Server Manual Binding

This window is used to configure and display the DHCP server manual binding settings. An IP address can be bound to a client identifier or the hardware address of the host.

Click **Management > DHCP > DHCP Server > DHCP Server Manual Binding** to view the following window:

Pool Name	Host	Mask	Hardware Address	Client Identifier	
Pool	192.168.70.85	255.255.255.0	00-11-22-33-44-55	-	Delete

Figure 4-34 DHCP Server Manual Binding

The following parameters can be configured in the **DHCP Server Manual Binding** section:

Parameter	Description
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long.
Host	Enter the IPv4 address for the DHCP host here.
Mask	Enter the subnet mask for the DHCP host network here.
Hardware Address	Enter the MAC address for the DHCP host here.
Client Identifier	Enter the identifier for the DHCP host in hexadecimal notation here. The client identifier is formatted by the media type and the MAC address.

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

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

4.9.4.5 DHCP Server Dynamic Binding

This window is used to display and clear DHCP server dynamic bindings.

Click **Management > DHCP > DHCP Server > DHCP Server Dynamic Binding** to view the following window:

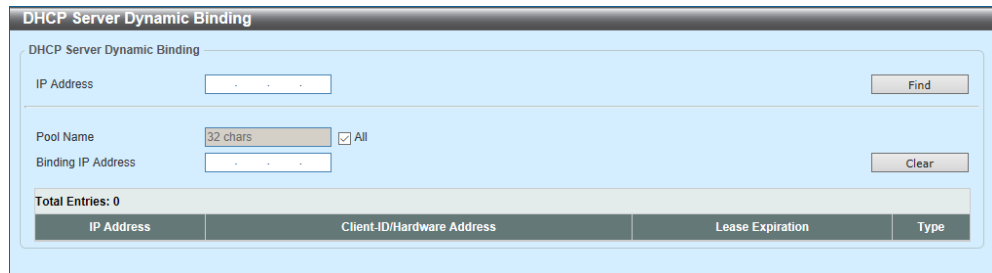


Figure 4-35 DHCP Server Dynamic Binding

The following parameters can be configured in the **DHCP Server Dynamic Binding** section:

Parameter	Description
IP Address	Enter the binding entry IPv4 address here.
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long. Select the All option to clear the binding entries for all pools.
Binding IP Address	Enter the binding entry IPv4 address here.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

Click the **Clear** button to clear the entries from the table based on the criteria specified.

4.9.4.6 DHCP Server IP Conflict

This window is used to display and clear the DHCP conflict entries from the DHCP server database.

Click **Management > DHCP > DHCP Server > DHCP Server IP Conflict** to view the following window:

Figure 4-36 DHCP Server IP Conflict

The following parameters can be configured in the **DHCP Server IP Conflict** section:

Parameter	Description
IP Address	Enter the IPv4 address of the conflict entry to be located or cleared.
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long. Select the All option to clear the conflict entries for all pools.
Conflict IP Address	Enter the IPv4 address of the conflict entry to be located or cleared.

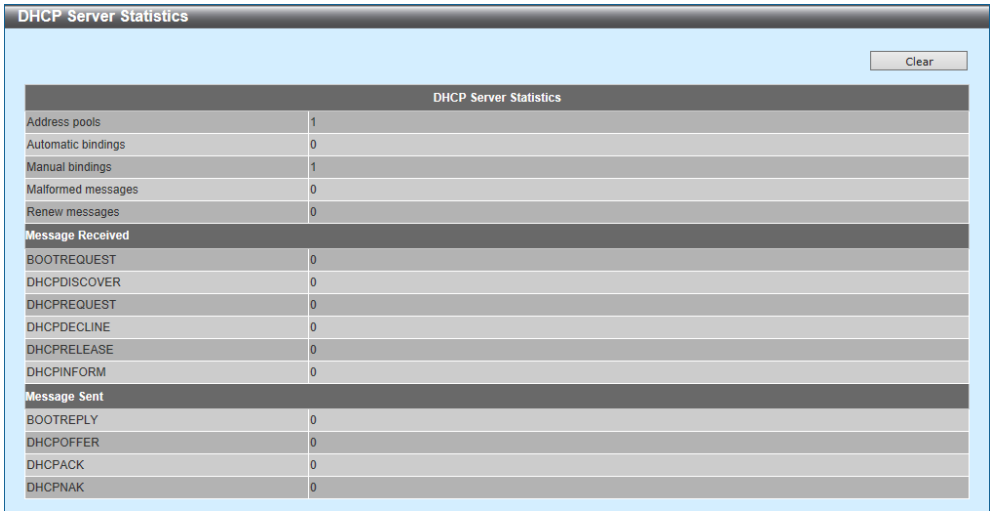
Click the **Find** button to find and display entries in the table based on the search criteria specified.

Click the **Clear** button to clear the entries from the table based on the criteria specified.

4.9.4.7 DHCP Server Statistics

This window is used to display DHCP server statistics.

Click **Management > DHCP > DHCP Server > DHCP Server Statistics** to view the following window:



DHCP Server Statistics	
Address pools	1
Automatic bindings	0
Manual bindings	1
Malformed messages	0
Renew messages	0
Message Received	
BOOTREQUEST	0
DHCPDISCOVER	0
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
Message Sent	
BOOTREPLY	0
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

Figure 4-37 DHCP Server Statistics

Click the **Clear** button to clear the statistics information.

4.9.5 DHCPv6 Server

4.9.5.1 DHCPv6 Server Pool Settings

This window is used to configure and display the DHCPv6 server pool settings.

Click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Pool Settings** to view the following window:

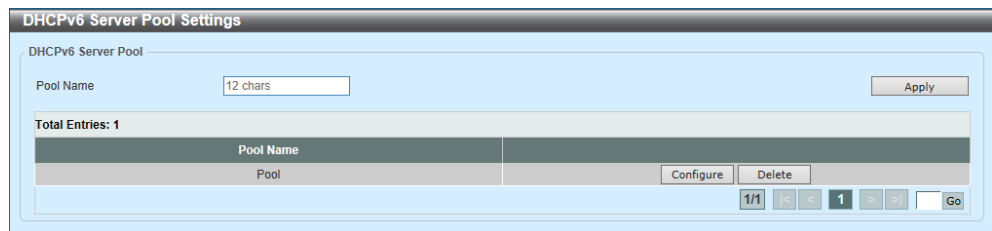


Figure 4-38 DHCPv6 Server Pool Settings

The following parameters can be configured in the **DHCPv6 Server Pool** section:

Parameter	Description
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.

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

Click the **Configure** button to configure the settings related to the specified entry.

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 **Configure** button to view the following window:

Figure 4-39 DHCPv6 Server Pool Settings (Configure)

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

The following parameters can be configured in the **DHCPv6 Server Pool Configure** section:

Parameter	Description
Address Prefix	Select and enter the DHCPv6 server pool IPv6 network address and prefix length here. For example, 2015::0/64.
Prefix Delegation Pool	Select and enter the DHCPv6 server pool prefix delegation name here. This name can be up to 12 characters long.
Valid Lifetime	Enter the valid lifetime value here. The range is from 60 to 4294967295 seconds. The valid lifetime should be greater than preferred lifetime. Select the Default option to use the default value of 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. Select the Default option to use the default value of 604800 seconds (7 days).
DNS Server	Enter the DNS server IPv6 address to be assigned to requesting DHCPv6 clients here.
Domain Name	Enter the domain name to be assigned to requesting DHCPv6 clients here.

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

The following parameters can be configured in the **Static Bindings** section:

Parameter	Description
Static Bindings Address	Enter the static binding IPv6 address assign to the specific client here.
Static Bindings Prefix	Enter the static binding IPv6 network address and prefix length here.
Client DUID	Enter the client DHCP Unique Identifier (DUID) here. This string can be up to 28 characters long.
IAID	Enter the Identity Association Identifier (IAID) here. The IAID here uniquely identifies a collection of non-temporary addresses (IANA) assigned on the client.
Valid Lifetime	Enter the valid lifetime value here. The valid lifetime should be greater than the preferred lifetime. The range is from 60 to 4294967295 seconds. Select the Default option to use the default value of 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. Select the Default option to use the default value of 604800 seconds (7 days).

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

4.9.5.2 DHCPv6 Server Local Pool Settings

This window is used to configure and display the DHCPv6 server local pool settings.

Click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Local Pool Settings** to view the following window:

Figure 4-40 DHCPv6 Server Local Pool Settings

The following parameters can be configured in the **DHCPv6 Server Local Pool** section:

Parameter	Description
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.
IPv6 Address / Prefix Length	Enter the IPv6 prefix address and prefix length of the local pool here.
Assigned Length	Enter the prefix length to be delegated to the user from the pool here. The value of the assigned length cannot be less than the value of the prefix length.

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

Click the **Find** button to find and display entries in the table based on the search criteria specified.

Click the **User Detail** button to display user information associated with the specified entry in the second table.

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.

4.9.5.3 DHCPv6 Server Exclude Address

This window is used to configure and display IPv6 addresses that will be excluded from the DHCPv6 pool. Multiple IPv6 address can be excluded from the DHCPv6 pool.

Click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Exclude Address** to view the following window:

Figure 4-41 DHCPv6 Server Exclude Address

The following parameters can be configured in the **DHCPv6 Server Exclude Address** section:

Parameter	Description
Low IPv6 Address	Enter the excluded IPv6 address or first IPv6 address in the excluded address range here.
High IPv6 Address	Enter the last IPv6 address in the excluded address range 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.

4.9.5.4 DHCPv6 Server Binding

This window is used to display and clear DHCPv6 server binding entries.

Click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Binding** to view the following window:

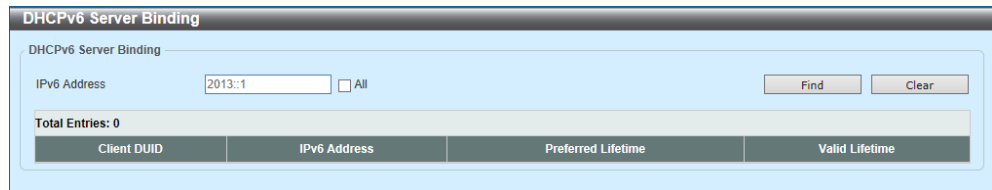


Figure 4-42 DHCPv6 Server Binding

The following parameters can be configured in the **DHCPv6 Server Binding** section:

Parameter	Description
IPv6 Address	Enter the binding entry IPv6 address to be displayed or cleared here. Select the All option to display or clear all DHCPv6 client prefix bindings in or from the binding table.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

Click the **Clear** button to clear the entries from the table based on the criteria specified.

4.9.5.5 DHCPv6 Server Interface Settings

This window is used to configure and display the interface settings associated with the DHCPv6 server.

Click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Interface Settings** to view the following window:

Figure 4-43 DHCPv6 Server Interface Settings

The following parameters can be configured in the **DHCPv6 Server Interface Settings** section:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. The range is from 1 to 4094.
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.
Rapid Commit	Select to enable or disable two-message exchange here. By default, two-message exchange is not allowed.
Preference	Enter the preference value here. Select the Default option to use the default value. Select the Allow Hint option to allow hints.
Interface Name	Enter the interface name here.

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

Click the **Find** button to find and display entries in the table based on the search criteria 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.

4.9.5.6 DHCPv6 Server Operational Information

This window is used to display operational DHCPv6 server information.

Click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Operational Information** to view the following window:

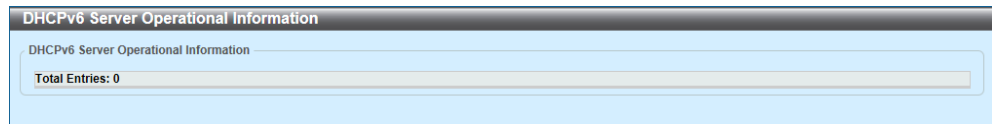


Figure 4-44 DHCPv6 Server Operational Information

4.9.6 DHCP Relay

4.9.6.1 DHCP Relay Global Settings

This window is used to configure and display the global DHCP relay settings.

Click **Management > DHCP > DHCP Relay > DHCP Relay Global Settings** to view the following window:

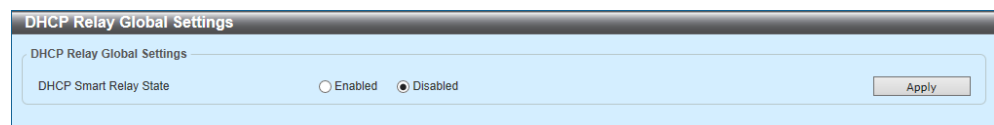


Figure 4-45 DHCP Relay Global Settings

The following parameters can be configured in the **DHCP Relay Global Settings** section:

Parameter	Description
DHCP Smart Relay State	Select to enable or disable the DHCP smart relay feature here.

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

4.9.6.2 DHCP Relay Pool Settings

This window is used to configure and display the DHCP relay pool on a DHCP relay agent.

Click **Management > DHCP > DHCP Relay > DHCP Relay Pool Settings** to view the following window:

Figure 4-46 DHCP Relay Pool Settings

The following parameters can be configured in the **DCHP Relay Pool Settings** section:

Parameter	Description
DHCP Pool Name	Enter the DHCP pool name here. This can be up to 32 characters long.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

Click the **Edit** button under **Source** to edit the DHCP relay source settings associated with the entry.

Click the **Edit** button under **Destination** to edit the DHCP relay destination settings associated with the entry.

Click the **Edit** button under **Class** to edit the DHCP relay class settings associated with the entry.

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

Click the **Edit** button under **Source** to view the following window:

Figure 4-47

The following parameters can be configured in the **DCHP Relay Pool Source Settings** section:

Parameter	Description
Source IP Address	Enter the source subnet of client packets.
Subnet Mask	Enter the network mask of the source subnet.

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

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

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

Click the **Edit** button under **Destination** to view the following window:

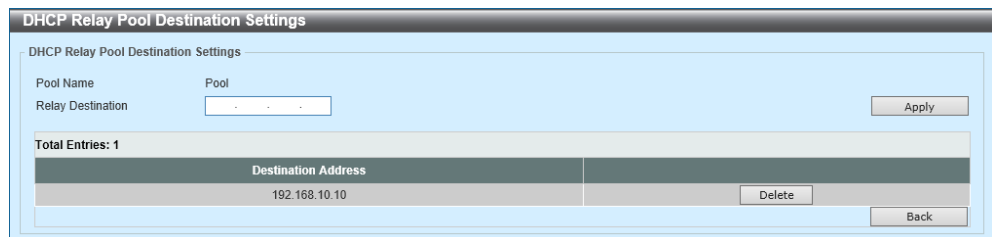


Figure 4-48

The following parameters can be configured in the **DCHP Relay Pool Destination Settings** section:

Parameter	Description
Relay Destination	Enter the IP address of the destination server used by DHCP relay here.

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

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

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

Click the **Edit** button under **Class** to view the following window:

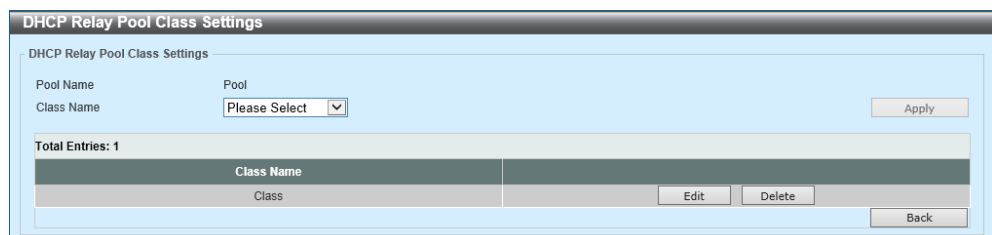


Figure 4-49

The following parameters can be configured in the **DCHP Relay Pool Class Settings** section:

Parameter	Description
Class Name	Select the DHCP class name.

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

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

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

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

Click the **Edit** button in the **DHCP Relay Pool Class Settings** to view the following window:

The screenshot shows a window titled "DHCP Relay Pool Class Edit Settings". Inside, there's a form with labels "Pool Name", "Class Name", "Relay Target", "Pool", and "Class". Below the form is a table with "Total Entries: 1" and one entry with "Target Address" "192.168.22.22". There are "Apply", "Delete", and "Back" buttons.

Figure 4-50

The following parameters can be configured in the **DCHP Relay Pool Class Edit Settings** section:

Parameter	Description
Relay Target	Enter the DHCP relay target for relaying packets that matches the value pattern of the option defined in the DHCP class.

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

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

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

4.9.6.3 DHCP Relay Information Settings

This window is used to configure and display the DHCP relay information settings.

Click **Management > DHCP > DHCP Relay > DHCP Relay Information Settings** to view the following window:

Figure 4-51 DHCP Relay Information Settings

The following parameters can be configured in the **DHCP Relay Information Global** section:

Parameter	Description
Information Trust All	Select this option to enable or disable the DHCP relay agent to trust the IP DHCP relay information for all interfaces.
Information Check	Select this option to enable or disable the DHCP relay agent to validate and remove the relay agent information option in the received DHCP reply packet.
Information Policy	Select the Option 82 re-forwarding policy for the DHCP relay agent. Options to choose from are: <ul style="list-style-type: none"> • Keep - Select to keep the packet that already has the relay option. The packet is left unchanged and directly relayed to the DHCP server. • Drop - Select to discard the packet that already has the relay option. • Replace - Select to replace the packet that already has the relay option. The packet will be replaced with a new option.
Information Option	Select this option to enable or disable the insertion of relay agent information (Option 82) during the relay of DHCP request packets.

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

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

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

4.9.6.4 DHCP Relay Information Option Format Settings

This window is used to configure and display the DHCP information format.

Click **Management > DHCP > DHCP Relay > DHCP Relay Information Option Format Settings** to view the following window:

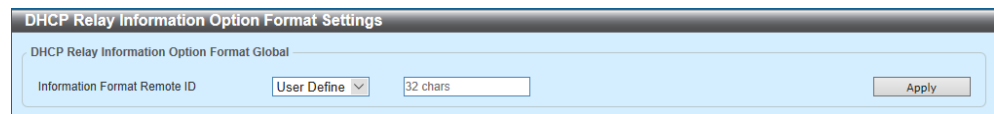


Figure 4-52 DHCP Relay Information Option Format Settings

The following parameters can be configured in the **DHCP Relay Information Option Format Global** section:

Parameter	Description
Information Format Remote ID	Select the DHCP information remote ID sub-option. Options to choose from are: <ul style="list-style-type: none">• Default - Select to use the Switch's system MAC address as the remote ID.• User Define - Select to use a user-defined remote ID. Enter the user-defined string with the maximum of 32 characters in the text box.

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

4.9.6.5 DHCP Local Relay VLAN

This window is used to configure and display the local relay on a VLAN or a group of VLANs.

Click **Management > DHCP > DHCP Relay > DHCP Local Relay VLAN** to view the following window:

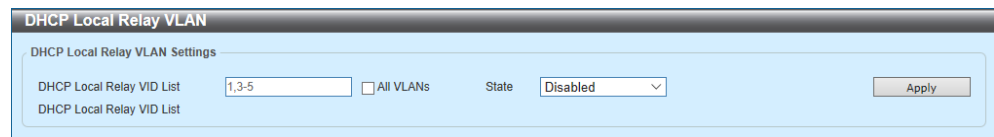


Figure 4-53 DHCP Local Relay VLAN

The following parameters can be configured in the **DHCP Local Relay VLAN Settings** section:

Parameter	Description
DHCP Local Relay VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094. Tick the All VLANs check box to select all VLANs.
State	Select this option to enable or disable the DHCP local relay on the specific VLAN(s).

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

4.9.7 DHCPv6 Relay

4.9.7.1 DHCPv6 Relay Global Settings

This window is used to configure and display the global DHCPv6 relay settings. This includes the Remote ID and Interface ID settings.

Click **Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings** to view the following window:

Figure 4-54 DHCPv6 Relay Global Settings

The following parameters can be configured in the **DHCPv6 Relay Remote ID Settings** section:

Parameter	Description
IPv6 DHCP Relay Remote ID Format	Select the IPv6 DHCP Relay remote ID format that will be used here. Options to choose from are Default , CID with User Define , and User Define .
IPv6 DHCP Relay Remote ID UDF	Select to choose the User Define Field (UDF) for remote ID. Options to choose from are: <ul style="list-style-type: none"> ASCII - Select to enter the ASCII string with a maximum of 128 characters in the text box. Hex - Select to enter the hexadecimal string with a maximum of 256 characters in the text box.
IPv6 DHCP Relay Remote ID Policy	Select to choose Option 37 forwarding policy for the DHCPv6 relay agent. Options to choose from are: <ul style="list-style-type: none"> Keep - Select that the DHCPv6 request packet that already has the relay agent Remote-ID option is left unchanged and directly relayed to the DHCPv6 server. Drop - Select to discard the packet that already has the relay agent Remote-ID Option 37.
IPv6 DHCP Relay Remote ID Option	Select this option to enable or disable the insertion of the relay agent remote ID Option 37 during the relay of DHCP for IPv6 request packets.

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

The following parameters can be configured in the **DHCPv6 Relay Interface ID Settings** section:

Parameter	Description
IPv6 DHCP Relay Interface ID Format	Select the IPv6 DHCP relay interface ID format that will be used here. Options to choose from are Default , CID , and Vendor1 .
IPv6 DHCP Relay Interface ID Policy	Select the Option 18 re-forwarding policy for the DHCPv6 relay agent here. Options to choose from are: <ul style="list-style-type: none">• Keep - Specifies that the DHCPv6 request packets that already contain the relay agent interface ID option are left unchanged and directly relay to the DHCPv6 server.• Drop - Specifies to discard the packets that already contain the relay agent interface ID Option 18.
IPv6 DHCP Relay Interface ID Option	Select to enable or disable the insertion of the relay agent interface ID Option 18 during the relay of DHCP for IPv6 request packets.

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

4.9.7.2 DHCPv6 Relay Interface Settings

This window is used to configure and display the DHCPv6 relay interface settings.

Click **Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Interface Settings** to view the following window:

The screenshot shows the 'DHCPv6 Relay Interface Settings' window. It contains three input fields: 'Interface VLAN (1-4094)', 'Destination IPv6 Address' (with the value '2012::100' entered), and 'Output Interface VLAN (1-4094)'. To the right of these fields are 'Apply' and 'Find' buttons. Below the input fields is a section 'Total Entries: 0' and a table with three columns: 'Interface', 'Destination IPv6 Address', and 'Output Interface'.

Figure 4-55 DHCPv6 Relay Interface Settings

The following parameters can be configured in the **DHCPv6 Relay Interface Settings** section:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID used in the DHCPv6 relay here. The range is from 1 to 4094.
Destination IPv6 Address	Enter the DHCPv6 relay destination address.
Output Interface VLAN	Enter the output interface VLAN ID for the relay destination here. The range is from 1 to 4094.

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

Click the **Find** button to find and display entries in the table based on the search criteria specified.

4.10 DHCP Auto Configuration

This window is used to enable or disable the DHCP auto-configuration feature.

Click **Management > DHCP Auto Configuration** to view the following window:

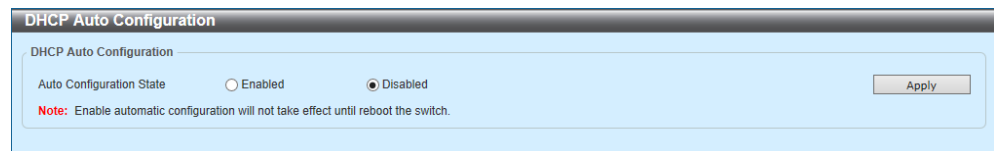


Figure 4-56 DHCP Auto Configuration

The following parameters can be configured in the **DHCP Auto Configuration** section:

Parameter	Description
Auto Configuration State	Select this option to enable or disable the DHCP auto-configuration function.

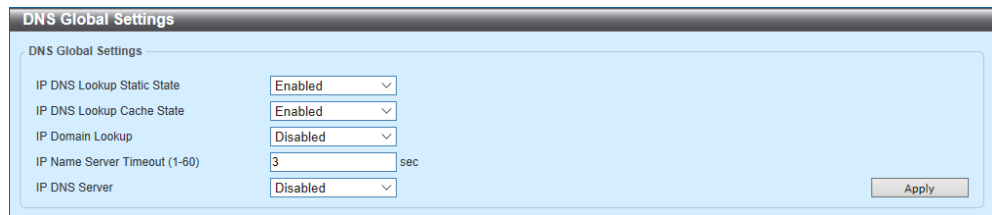
Click the **Apply** button to accept the changes made.

4.11 DNS (Domain Name System)

4.11.1 DNS Global Settings

This window is used to configure and display the global DNS settings.

Click **Management > DNS > DNS Global Settings** to view the following window:



The screenshot shows a window titled "DNS Global Settings". Inside, there are five configuration items, each with a label and a dropdown menu:

- 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

An "Apply" button is located at the bottom right of the settings area.

Figure 4-57 DNS Global Settings

The following parameters can be configured in the **DNS Global Settings** section:

Parameter	Description
IP DNS Lookup Static State	Select to enable or disable the IP DNS lookup static state here.
IP DNS Lookup Cache State	Select to enable or disable the IP DNS lookup cache state here.
IP Domain Lookup	Select to enable or disable the IP domain lookup state here.
IP Name Server Timeout	Enter the maximum time to wait for a response from a specified name server. This value is between 1 and 60 seconds.
IP DNS Server	Select to globally enable or disable the DNS server feature here.

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

4.11.2 DNS Name Server Settings

This window is used to configure and display DNS name server settings.

Click **Management > DNS > DNS Name Server Settings** to view the following window:

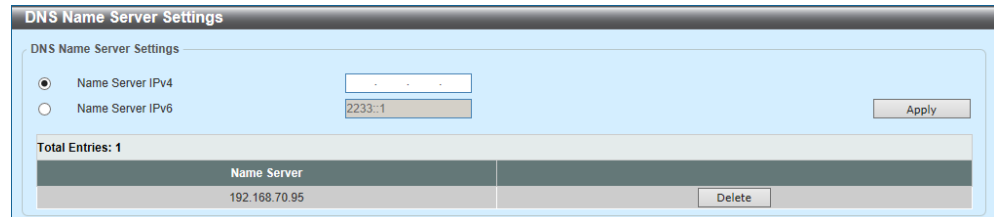


Figure 4-58 DNS Name Server Settings

The following parameters can be configured in the **DNS Name Server Settings** section:

Parameter	Description
Name Server IPv4	Select and enter the IPv4 address of the DNS server.
Name Server IPv6	Select and enter the IPv6 address of the DNS server.

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

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

4.11.3 DNS Host Settings

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

Click **Management > DNS > DNS Host Settings** to view the following window:

Figure 4-59 DNS Host Settings

The following parameters can be configured in the **Static Host Settings** section:

Parameter	Description
Host Name	Enter the name of the DNS host here.
IP Address	Select and enter the IPv4 address of the DNS host here.
IPv6 Address	Select and enter the IPv6 address of the DNS host here.

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

Click the **Clear All** button to remove all the dynamic entries from the table.

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.

4.12 File System

This window is used to configure and display the file system of the switch.

Click **Management > File System** to view the following window:

Drive	Media Type	Size (MB)	File System Type	Label
C:	Flash	119	FFS	

Figure 4-60 File System

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Path	Enter the path string here.

Click the **Go** button to navigate to the path entered.

Click the **Copy** button to copy a specific file to the file system.

Click the Drive Link (c:) to navigate the C: drive

Click the Drive Link (c:) to view the following window:

Index	Info	Attr	Size (byte)	Update Time	Name	Boot Up	Rename	Delete
1	CFG(*)	-rw	2417	Apr 24 2017 20:01:22	config.cfg			
2	RUN(*)	-rw	11861856	Apr 18 2017 18:31:37	V1.0.0.07.had			
3	RUN	-rw	11853180	Apr 12 2017 23:38:15	V1.0.0.06.had			
4		d--	0	Apr 24 2017 11:01:45	system			

125304832 bytes total (101013504 bytes free)
(*) -with boot up info

Figure 4-61 File System (c:)

Click the **Previous** button to return to the previous window.

Click the **Create Directory** button to create a new directory in the file system.

Click the **Boot Up** button to use the file(s) in the boot-up sequence. Only one configuration file and one firmware file can be used in the boot-up sequence.

Click the **Rename** button to rename a specific file name.

Click the **Delete** button to remove the file or folder from the file system.

Click the **Copy** button to view the following window:

Figure 4-62 File System (Copy)

The following parameters can be configured:

Parameter	Description
Source	Select the source Switch Unit ID and type of source file that will be copied here. Options to choose from are startup-config and Source File . Only after selecting the Source File option can the source file path and filename be entered in the space provided.
Destination	Select the destination Switch Unit ID and type of destination file that will be copied here. Options to choose from are startup-config , running-config , and Destination File . Only after selecting the Destination File option can the destination file path and filename be entered in the space provided. Select the Replace check box to replace the current running configuration with the indicated configuration file.

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

Click the **Cancel** button to cancel the copy.

4.13 Stacking

4.13.1 Physical Stacking

This window is used to configure and display the settings related to the physical stacking feature on the switch. Switches can be physically stacked using optical fiber cables connected to Quad Small Form-factor Pluggable (QSFP) transceivers or Direct Attached Cables (DAC) with QSFP connectors.

When stacking is enabled, the last two QSFP ports are dedicated for stacking and cannot be used for any other purpose. These ports are only able to perform stacking when the stacking mode is enabled.

Click **Management > Stacking > Physical Stacking** to view the following window:

Physical Stacking

Physical Stacking

Stacking Mode: ☒ Enabled ☐ Disabled Apply

Stack Preempt: ☒ Enabled ☐ Disabled Apply

Trap State: ☐ Enabled ☒ Disabled

Stack ID

Current Unit ID: New Box ID: Priority (1-63): Apply

Topology: Duplex_Chain My Box ID: 1
Master ID: 1 Backup Master ID: -
Box Count: 1

Box ID	User Set	Module Name	Exist	Priority	MAC	PROM Version	Runtime Version	H/W Version
1	Auto	ZEQUO6600RE	Exist	32	00-50-40-3C-77-81	V1.0.0.04	V1.0.0.15	A1
2	-	ZEQUO6600RE	No	-	-	-	-	-
3	-	ZEQUO6600RE	No	-	-	-	-	-
4	-	ZEQUO6600RE	No	-	-	-	-	-

Figure 4-63 Physical Stacking

The following parameters can be configured in the **Physical Stacking** section:

Parameter	Description
Stacking Mode	Select this option to enable or disable the stacking mode.
Stack Preempt	Select this option to enable or disable preemption of the master role when a unit with a higher priority is added to the Switch.
Trap State	Select to enable or disable the stacking trap state here.
Current Unit ID	Select the unit ID of the Switch in the stack.
New Box ID	Select the new box ID for the Switch that is selected in the Current Unit ID field. The user may choose any number between 1 and 9 to identify the Switch in the switch stack. Auto will automatically assign a box number to the Switch in the Switch stack.
Priority	Enter the priority of the Switch stacking unit. The range is from 1 to 63.

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

4.14 SMTP Settings

This window is used to configure and display the Simple Mail Transfer Protocol (SMTP) settings.

Click **Management > SMTP Settings** to view the following window:

The screenshot shows the 'SMTP Settings' window. It is divided into three main sections. The first section, 'SMTP Global Settings', contains five configuration fields: 'SMTP IP' (a dropdown menu currently showing 'IPv4'), 'SMTP IPv4 Server Address' (a text box containing '0.0.0.0'), 'SMTP IPv4 Server Port (1-65535)' (a text box containing '25'), 'Self Mail Address' (a text box with a '254 chars' limit), and 'Send Interval (0-65535)' (a text box containing '30' with a 'min' unit indicator). An 'Apply' button is located to the right of these fields. The second section, 'SMTP Mail Receiver Address', features an 'Add A Mail Receiver' button and a text box with a '254 chars' limit, followed by an 'Add' button. The third section, 'Send a Test Mail to All', includes a 'Subject' text box with a '128 chars' limit and a 'Content' text area with a '512 chars' limit, with an 'Apply' button to the right. At the bottom of the window, there is a table header showing 'Total Entries: 0' and a 'Delete All' button. Below this is a table with three columns: 'Index', 'Mail Receiver Address', and 'Delete'. The table contains eight rows, each with an index from 1 to 8, an empty 'Mail Receiver Address' field, and a 'Delete' button.

Figure 4-64 SMTP Settings

The following parameters can be configured in the **SMTP Global Settings** section:

Parameter	Description
SMTP IP	Select the SMTP server IP address type here. Options to choose from are IPv4 and IPv6 .
SMTP IPv4 Server Address	After selecting IPv4 as the SMTP IP type enter the SMTP server IPv4 address here.
SMTP IPv6 Server Address	After selecting IPv6 as the SMTP IP type enter the SMTP server IPv6 address here.
SMTP IPv4 Server Port	After selecting IPv4 as the SMTP IP type enter the SMTP server port number here. The range is from 1 to 65535. By default, this value is 25.
SMTP IPv6 Server Port	After selecting IPv6 as the SMTP IP type enter the SMTP server port number here. The range is from 1 to 65535. By default, this value is 25.
Self Mail Address	Enter the email address that represents the Switch here. This string can be up to 254 characters long.

Parameter	Description
Send Interval	Enter the sending interval value here. The range is from 0 to 65535 minutes. By default, this value is 30 minutes.

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

The following parameters can be configured in the **SMTP Mail Receiver Address** section:

Parameter	Description
Add A Mail Receiver	Enter the email address of the receiver here. This string can be up to 254 characters long.

The following parameters can be configured in the **Send a Test Mail to All** section:

Parameter	Description
Subject	Enter the subject of the email here. This string can be up to 128 characters long.
Content	Enter the content of the email here. This string can be up to 512 characters long.

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

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

Click the **Delete All** button to remove all the receiver mail addresses from all the entries.

Click the **Delete** button to remove the receiver mail address from the specified entry.

4.15 NLB FDB Settings

This window is used to configure and display the Network Load Balancing (NLB) File Database (FDB) settings on the specified port(s).

Click **Management > NLB FDB Settings** to view the following window:

Figure 4-65 NLB FDB Settings

The following parameters can be configured in the **NLB FDB Settings** section:

Parameter	Description
NLB Type	Select the NLB type here. Options to choose from are Unicast and Multicast .
VID	After selecting Multicast as the NLB Type , enter the VLAN ID that will be used here. The range is from 1 to 4094.
MAC Address	Enter the unicast or multicast MAC address of the entry here. If a received packet contains a destination MAC address that matches the specified MAC address, it will be forwarded to the specified interface.
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.

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

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

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.

4.16 IP Setup

4.16.1 IP Setup Settings

This window is used to enable or disable the IP setup interface feature.

Click **Management > IP Setup > IP Setup Settings** to view the following window:

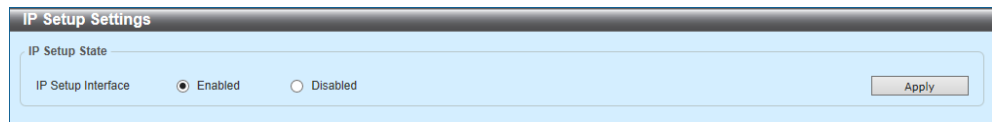


Figure 4-66 IP Setup Settings

The following parameters can be configured in the **IP Setup State** section:

Parameter	Description
IP Setup Interface	Select to enable or disable the IP setup interface feature here.

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

4.16.2 IP Setup Forwarding Settings

This window is used to configure and display the IP setup forwarding settings.

Click **Management > IP Setup > IP Setup Forwarding Settings** to view the following window:

Figure 4-67 IP Setup Forwarding Settings

The following parameters can be configured in the **IP Setup Forward Global State** section:

Parameter	Description
IP Setup Protocol Forward Status	Select to enable or disable the IP setup protocol forward status here.

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

The following parameters can be configured in the **Sender IP Settings** section:

Parameter	Description
Sender IP Address	Enter the IP address of the sender here.
Destination Interface Name	Enter the name of the destination interface here.

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

Click the **Delete** button to delete an entry based on the information specified.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

The following parameters can be configured in the **Interface Settings** section:

Parameter	Description
Received Interface	Enter the ID of the receiving interface here. The range is from 1 to 4094.
Destination Interface Name	Select and enter the name of the destination interface here.
Source IP Address	Select and enter the IP address of the source here.
Destination IP Address	Select and enter the IP address of the destination here.

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

Click the **Delete** button to delete an entry based on the information specified.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

5 L2 Features

5.1 FDB (File Database)

5.1.1 Static FDB

5.1.1.1 Unicast Static FDB

This window is used to configure and display the static unicast forwarding settings.

Click **L2 Features > FDB > Static FDB > Unicast Static FDB** to view the following window:

Figure 5-1 Unicast Static FDB

The following parameters can be configured in the **Unicast Static FDB** section:

Parameter	Description
Port/Drop	Select the Port option to use the port on which the MAC address entered resides. Select the Drop option to drop the MAC address from the unicast static FDB.
Unit	Select the unit ID of the switch in the physical stack here.
Port Number	After selecting the Port option, select the port that will be used here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
MAC Address	Enter the MAC address to which packets will be statically forwarded. This must be a unicast MAC address.

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

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

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.

5.1.1.2 Multicast Static FDB

This window is used to configure and display the multicast static FDB settings.

Click **L2 Features > FDB > Static FDB > Multicast Static FDB** to view the following window:

Figure 5-2 Multicast Static FDB

The following parameters can be configured in the **Multicast Static FDB** 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.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
MAC Address	Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address.

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

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

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.

5.1.2 MAC Address Table Settings

This window is used to configure and display the MAC address table settings.

Click **L2 Features > FDB > MAC Address Table Settings** to view the following window:

The screenshot shows the 'MAC Address Table Settings' window with the 'Global Settings' tab selected. It contains two main configuration fields: 'Aging Time (0, 10-1000000)' set to '300' seconds, and 'Aging Destination Hit' with radio buttons for 'Enabled' and 'Disabled' (the latter is selected). An 'Apply' button is located at the bottom right.

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

The following parameters can be configured in the **Global Settings** section:

Parameter	Description
Aging Time	Enter the MAC address table aging time here. The range is from 10 to 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.
Aging Destination Hit	Select to enable or disable the aging destination hit function.

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

Click the **MAC Address Port Learning Settings** tab to view the following window:

The screenshot shows the 'MAC Address Table Settings' window with the 'MAC Address Port Learning Settings' tab selected. It features a configuration area for 'Unit 1' with dropdowns for 'Unit' (set to 1), 'From Port' (set to Gi1/0/1), 'To Port' (set to Gi1/0/1), and 'Status' (set to Enabled). Below this is a table titled 'Unit 1 Settings' showing a list of ports from Gi1/0/1 to Gi1/0/10, all with a status of 'Enabled'. An 'Apply' button is at the top right.

Port	Status
Gi1/0/1	Enabled
Gi1/0/2	Enabled
Gi1/0/3	Enabled
Gi1/0/4	Enabled
Gi1/0/5	Enabled
Gi1/0/6	Enabled
Gi1/0/7	Enabled
Gi1/0/8	Enabled
Gi1/0/9	Enabled
Gi1/0/10	Enabled

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

The following parameters can be configured in the **MAC Address Port Learning 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.
Status	Select to enable or disable the MAC address learning function on the ports specified here.

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

Click the **MAC Address VLAN Learning Settings** tab to view the following window:

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

The following parameters can be configured in the **MAC Address VLAN Learning Settings** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
Status	Select to enable or disable the MAC address learning function on the VLAN(s) specified here.

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

The following parameters can be configured in the **Find MAC Address VLAN Learning** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

5.1.3 MAC Address Table

This window is used to display and clear MAC address table entries.

Click **L2 Features > FDB > MAC Address Table** to view the following window:

VID	MAC Address	Type	Port
1	00-22-33-44-55-66	Static	Gi1/0/10
1	00-23-7D-BC-08-44	Dynamic	Gi1/0/1
1	00-23-7D-BC-2E-18	Dynamic	Gi1/0/1
1	00-50-40-3C-77-81	Static	CPU
1	00-FF-47-77-70-B8	Dynamic	Gi1/0/1
1	10-BF-48-D6-E2-E2	Dynamic	Gi1/0/1
1	24-24-0E-E5-96-DE	Dynamic	Gi1/0/1
1	D0-AE-EC-C4-E3-80	Dynamic	Gi1/0/1
1	01-00-00-00-00-02	Static	Gi1/0/10

Figure 5-6 MAC Address Table

The following parameters can be configured in the **MAC Address Table** section:

Parameter	Description
Port	Select the stacking unit ID and the port number of the Switch that will be configured here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
MAC Address	Enter the MAC address that will be used for this configuration here.

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 specified dynamic MAC address from the table.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

Click the **Clear All** button to remove all the entries from the table.

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

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

5.1.4 MAC Notification

This window is used to configure and display the global MAC notification settings and the MAC notification settings on the specified port(s).

Click **L2 Features > FDB > MAC Notification** to view the following window:

Figure 5-7 MAC Notification (MAC Notification Settings)

The following parameters can be configured in the **MAC Notification Global Settings** section:

Parameter	Description
MAC Address Notification	Select to enable or disable MAC notification globally on the Switch.
Interval	Enter the time value between notifications. The range is from 1 to 2147483647 seconds. By default, this value is 1 second.
History Size	Enter the maximum number of entries listed in the history log used for notification. The range is from 0 to 500. By default, this value is 1.
MAC Notification Trap State	Select to enable or disable the MAC notification trap state.
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.
Added Trap	Select to enable or disable the added trap for the port(s) selected.

Parameter	Description
Removed Trap	Select to enable or disable the removed trap for the port(s) selected.

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

Click the **MAC Notification History** tab to view the following window:

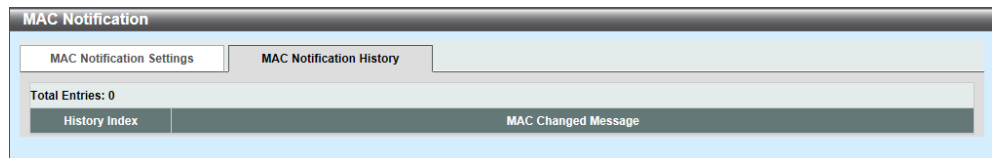


Figure 5-8 MAC Notification (MAC Notification History)

5.2 Link Aggregation

This window is used to configure and display the link aggregation settings.

Click **L2 Features > Link Aggregation** to view the following window:

Figure 5-9 Link Aggregation

The following parameters can be configured in the first section:

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

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

The following parameters can be configured in the **Channel Group Information** 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.

Parameter	Description
Group ID	Enter the channel group number here. The range is from 1 to 32. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are Static , Active , and Passive . If the mode Static is specified, the channel group type is static. If the mode Active or Passive is specified, the channel group type is the Link Aggregation Control Protocol (LACP). A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

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

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

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

Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:

Port Channel

Port Channel Information
Port Channel 1
Protocol Static

Port Channel Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
Gi1/0/20	None	None	down	None	None	Edit
Gi1/0/21	None	None	down	None	None	Edit
Gi1/0/22	None	None	down	None	None	Edit
Gi1/0/23	None	None	down	None	None	Edit
Gi1/0/24	None	None	down	None	None	Edit

Port Channel Neighbor Information

Port	Partner System ID	Partner Port No.	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
Gi1/0/20	None	None	None	None	None
Gi1/0/21	None	None	None	None	None
Gi1/0/22	None	None	None	None	None
Gi1/0/23	None	None	None	None	None
Gi1/0/24	None	None	None	None	None

Note:
LACP State:
bnd: Port is attached to an aggregator and bundled with other ports.
indep: Port is in an independent state(not bundled but able to switch data traffic).
hot-sby: Port is in a hot-standby state.
down: Port is down.

Back

Figure 5-10 Link Aggregation (Show Detail)

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

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

5.3 VLAN (Virtual Local Area Network)

5.3.1 802.1Q VLAN

This window is used to configure and display the IEEE 802.1Q VLAN settings.

Click **L2 Features > VLAN > 802.1Q VLAN** to view the following window:

Figure 5-11 802.1Q VLAN

The following parameters can be configured in the **802.1Q VLAN** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be created or deleted here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

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

Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Find VLAN** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

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.

5.3.2 802.1v Protocol VLAN

5.3.2.1 Protocol VLAN Profile

This window is used to configure and display IEEE 802.1v protocol VLAN settings. Multiple VLANs are supported for each protocol. Untagged ports can be configured for different protocols on the same physical port.

Click **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile** to view the following window:

Figure 5-12 Protocol VLAN Profile

The following parameters can be configured in the **Add Protocol VLAN Profile** section:

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

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

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

5.3.2.2 Protocol VLAN Profile Interface

This window is used to configure and display the protocol-VLAN profile interface settings.

Click **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface** to view the following window:

Figure 5-13 Protocol VLAN Profile Interface

The following parameters can be configured in the **Add New Protocol VLAN Interface** section:

Parameter	Description
Port	Select the stacking unit ID and the port number of the Switch that will be configured here.
Profile ID	Select the 802.1v protocol VLAN profile ID here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Priority	Select the priority value used here. This value is between 0 and 7. This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the Class of Service (CoS) queue that packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously.

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

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

5.3.3 GVRP

5.3.3.1 GVRP Global

This window is used to configure and display the global GARP VLAN Registration Protocol (GVRP) settings. GARP stands for Generic Attribute Registration Protocol.

Click **L2 Features > VLAN > GVRP > GVRP Global** to view the following window:

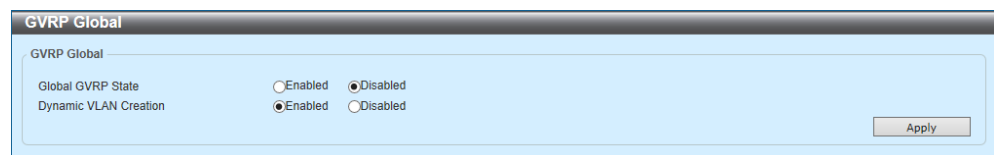


Figure 5-14 GVRP Global

The following parameters can be configured in the **GVRP Global** section:

Parameter	Description
Global GVRP State	Select to enable or disable the global GVRP state here.
Dynamic VLAN Creation	Select to enable or disable the dynamic VLAN creation function here.

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

5.3.3.2 GVRP Port

This window is used to configure and display the GVRP port settings.

Click **L2 Features > VLAN > GVRP > GVRP Port** to view the following window:

GVRP Port

GVRP Port

Unit: 1 From Port: Gi1/0/1 To Port: Gi1/0/1 GVRP Status: Disabled Join Time (10-10000): 20 centiseconds Leave Time (10-10000): 60 centiseconds Leave All Time (10-10000): 1000 centiseconds

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

Unit 1 Settings

Port	GVRP Status	Join Time	Leave Time	Leave All Time
Gi1/0/1	Disabled	20	60	1000
Gi1/0/2	Disabled	20	60	1000
Gi1/0/3	Disabled	20	60	1000
Gi1/0/4	Disabled	20	60	1000
Gi1/0/5	Disabled	20	60	1000
Gi1/0/6	Disabled	20	60	1000
Gi1/0/7	Disabled	20	60	1000
Gi1/0/8	Disabled	20	60	1000
Gi1/0/9	Disabled	20	60	1000
Gi1/0/10	Disabled	20	60	1000

Figure 5-15 GVRP Port

The following parameters can be configured in the **GVRP Port** 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.
GVRP Status	Select the enable or disable the GVRP port status. This enables the port to become a member of a VLAN dynamically. By default, this option is disabled.
Join Time	Enter the Join Time value here. The range is from 10 to 10000 centiseconds. By default, this value is 20 centiseconds.
Leave Time	Enter the Leave Time value here. The range is from 10 to 10000 centiseconds. By default, this value is 60 centiseconds.
Leave All Time	Enter the Leave All Time value here. The range is from 10 to 10000 centiseconds. By default, this value is 1000 centiseconds.

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

5.3.3.3 GVRP Advertise VLAN

This window is used to configure and display the GVRP advertise VLAN settings.

Click **L2 Features > VLAN > GVRP > GVRP Advertise VLAN** to view the following window:

Figure 5-16 GVRP Advertise VLAN

The following parameters can be configured in the **GVRP Advertise VLAN** 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.
Action	Select the advertised VLAN to port mapping action here. Options to choose from are All , Add , Remove , and Replace . When selecting All , all the advertised VLANs will be used.
Advertise VID List	Enter the VLAN ID(s) that will be advertised used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

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

5.3.3.4 GVRP Forbidden VLAN

This window is used to configure and display the GVRP forbidden VLAN settings.

Click **L2 Features > VLAN > GVRP > GVRP Forbidden VLAN** to view the following window:

Figure 5-17 GVRP Forbidden VLAN

The following parameters can be configured in the **GVRP Forbidden VLAN** 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.
Action	Select the forbidden VLAN to port mapping action that will be taken here. Options to choose from are All , Add , Remove , and Replace . When selecting All , all the forbidden VLANs will be used.
Forbidden VID List	Enter the VLAN ID(s) that will be forbidden used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

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

5.3.3.5 GVRP Statistics Table

This window is used to display and clear the GVRP statistics.

Click **L2 Features > VLAN > GVRP > GVRP Statistics Table** to view the following window:

GVRP Statistics Table							
GVRP Statistics Table							
Unit	1		Port	Gi1/0/1			
					Find	Clear	
					Show All	Clear All	
Unit 1 Settings							
Port		JoinEmpty	JoinIn	LeaveEmpty	LeaveIn	LeaveAll	Empty
Gi1/0/1	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
Gi1/0/2	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
Gi1/0/3	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
Gi1/0/4	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
Gi1/0/5	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
Gi1/0/6	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0

Figure 5-18 GVRP Statistics Table

The following parameters can be configured in the **GVRP Statistics Table** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

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

5.3.4 Asymmetric VLAN

This window is used to configure and display the asymmetric VLAN settings.

Click **L2 Features > VLAN > Asymmetric VLAN** to view the following window:



Figure 5-19 Asymmetric VLAN

The following parameters can be configured in the **Asymmetric VLAN** section:

Parameter	Description
Asymmetric VLAN State	Select to enable or disable the asymmetric VLAN feature here.

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

5.3.5 MAC VLAN

This window is used to configure and display the MAC-based VLAN settings. VLAN operating on a port will change when a static MAC-based VLAN entry is configured and associated to that port.

Click **L2 Features > VLAN > MAC VLAN** to view the following window:

Figure 5-20 MAC VLAN

The following parameters can be configured in the **MAC VLAN** section:

Parameter	Description
MAC Address	Enter the unicast MAC address.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Priority	Select the priority that is assigned to untagged packets. This value is between 0 and 7.

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.

5.3.6 VLAN Interface

This window is used to configure and display the VLAN interface settings.

Click **L2 Features > VLAN > VLAN Interface** to view the following window:

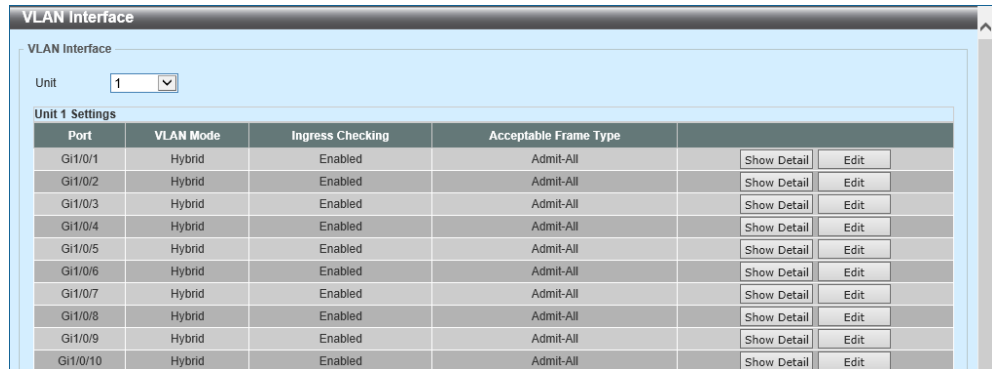


Figure 5-21 VLAN Interface

The following parameters can be configured in the **VLAN Interface** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to view the following window:

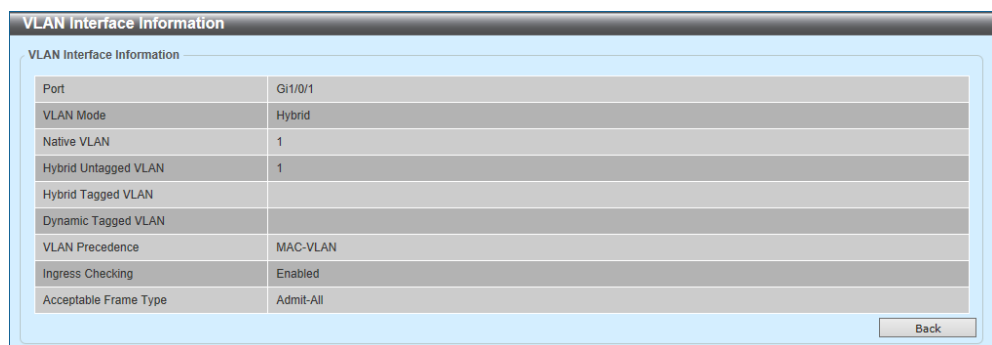


Figure 5-22 VLAN Interface (Show Detail)

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

Click the **Edit** button to view the following window:

The screenshot shows the 'Configure VLAN Interface' window. The 'VLAN Mode' is set to 'ACCESS'. The 'Acceptable Frame' is set to 'Admit All'. 'Ingress Checking' is set to 'Enabled'. The 'VID (1-4094)' is set to '1'. The 'Port' is 'Gi1/0/1'. There are 'Clone', 'From Port', and 'To Port' options, all set to 'Gi1/0/1'. 'Back' and 'Apply' buttons are at the bottom right.

Figure 5-23 VLAN Interface (Edit, Access)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , Promiscuous , and Host .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VLAN ID	Enter the VLAN ID used for this configuration here. The range is from 1 to 4094.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the port(s) that will be used here.

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

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

Select **Hybrid** as the **VLAN Mode** to view the following window:

The screenshot shows the 'Configure VLAN Interface' window for Hybrid mode. 'VLAN Mode' is 'Hybrid'. 'Acceptable Frame' is 'Admit All'. 'Ingress Checking' is 'Enabled'. 'VLAN Precedence' is 'MAC-based VLAN'. 'Native VLAN' is checked. 'VID (1-4094)' is '1'. 'Action' is 'Add'. 'Add Mode' is 'Untagged'. 'Allowed VLAN Range', 'Current Hybrid untagged VLAN Range', and 'Current Hybrid tagged VLAN Range' are all set to '1'. 'Port' is 'Gi1/0/1'. 'Clone', 'From Port', and 'To Port' are also 'Gi1/0/1'. 'Back' and 'Apply' buttons are at the bottom right.

Figure 5-24 VLAN Interface (Edit, Hybrid)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , Promiscuous , and Host .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VLAN Precedence	Select the VLAN precedence option here. Options to choose from are MAC-based VLAN and Subnet-based VLAN .
Native VLAN	Tick this option to enable the native VLAN function.
VID	After ticking the Native VLAN option, this parameter will be available. Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Action	Select the action that will be taken here. Options to choose from are None , Add , Remove , Tagged , and Untagged .
Add Mode	Select whether to add an Untagged or Tagged parameters.
Allowed VLAN Range	Enter the allowed VLAN range here.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

Select **Trunk** as the **VLAN Mode** to view the following window:

The screenshot shows the 'Configure VLAN Interface' window. The 'Port' is 'Gi1/0/1'. The 'VLAN Mode' is 'Trunk'. The 'Acceptable Frame' is 'Admit All'. The 'Ingress Checking' is 'Enabled'. The 'Native VLAN' is 'Untagged'. The 'VID' is '1'. The 'Action' is 'Add'. The 'Allowed VLAN Range' is empty. The 'Current Allowed VLAN Range' is empty. The 'Clone' checkbox is unchecked. The 'From Port' and 'To Port' are both 'Gi1/0/1'. The 'Back' and 'Apply' buttons are at the bottom right.

Figure 5-25 VLAN Interface (Edit, Trunk)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , Promiscuous , and Host .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	After selecting Trunk as the VLAN Mode , the following parameter will be available. Select to enable or disable the ingress checking function.
Native VLAN	Tick this option to enable the native VLAN function. Also select if this VLAN supports Untagged or Tagged frames.
VID	After ticking the Native VLAN option, this parameter will be available. Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Action	Select the action that will be taken here. Options to choose from are None , All , Add , Remove , Except , and Replace .
Allowed VLAN Range	Enter the allowed VLAN range here.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the port(s) that will be used here.

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

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

Select **Promiscuous** as the **VLAN Mode** to view the following window:

The screenshot shows the 'Configure VLAN Interface' window. The 'Port' is set to 'Gi1/0/1'. The 'VLAN Mode' is set to 'Promiscuous'. The 'Acceptable Frame' is set to 'Admit All'. The 'Ingress Checking' is set to 'Enabled'. The 'Clone' checkbox is unchecked. The 'From Port' and 'To Port' are both set to 'Gi1/0/1'. There are 'Back' and 'Apply' buttons at the bottom right.

Figure 5-26 VLAN Interface (Edit, Promiscuous)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , Promiscuous , and Host .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

Select **Host** as the **VLAN Mode** to view the following window:

Figure 5-27 VLAN Interface (Edit, Host)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , Promiscuous , and Host .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

5.3.7 Subnet VLAN

This window is used to configure and display the subnet VLAN settings. If an untagged or priority-tagged IP packet is received on a port, its source IP address will be used to match the subnet VLAN entries. If the source IP is in the subnet of an entry, the packet will be classified to the VLAN defined for this subnet.

Click **L2 Features > VLAN > Subnet VLAN** to view the following window:

Figure 5-28 Subnet VLAN

The following parameters can be configured in the **Subnet VLAN** section:

Parameter	Description
IPv4 Network Prefix / Prefix Length	Select and enter the IPv4 address and prefix length value for the subnet VLAN here.
IPv6 Network Prefix / Prefix Length	Select and enter the IPv6 address and prefix length value for the subnet VLAN here.
VID	Enter the subnet VLAN ID that will be used here. The range is from 1 to 4094.
Priority	Select the priority value used here. This value is between 0 and 7. A lower value takes higher priority.

Click the **Apply** button to 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.

5.3.8 Voice VLAN

5.3.8.1 Voice VLAN Global

This window is used to configure and display the global voice VLAN settings. This is used to globally enable or disable the voice VLAN feature and to specify the voice VLAN on the switch. Only one voice VLAN can be specified on the switch.

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN Global** to view the following window:

Figure 5-29 Voice VLAN Global

The following parameters can be configured in the **Voice VLAN Global** section:

Parameter	Description
Voice VLAN State	Select to globally enable or disable the voice VLAN feature here.
Voice VLAN ID	Enter the VLAN ID of the voice VLAN here. The VLAN to be specified as the voice VLAN needs to pre-exist before configuration. The range is from 2 to 4094.
Voice VLAN CoS	Select the CoS of the voice VLAN here. The range is from 0 to 7. The voice packets arriving at the voice VLAN enabled port are marked as the CoS specified here. The remarking of CoS packets allow the voice VLAN traffic to be distinguished from data traffic in Quality of Service.
Aging Time	Enter the aging time value here. This is used to configure the aging time for aging out the automatically learned voice device and voice VLAN information. When the last voice device connected to the port stops sending traffic and the MAC address of this voice device is aged out from FDB, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. If voice traffic resumes during the aging time, the aging timer will be cancelled. The range is from 1 to 65535 minutes.

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

5.3.8.2 Voice VLAN Port

This window is used to configure and display the voice VLAN interface settings.

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN Port** to view the following window:

Port	State	Mode
Gi1/0/1	Disabled	Auto/Untag
Gi1/0/2	Disabled	Auto/Untag
Gi1/0/3	Disabled	Auto/Untag
Gi1/0/4	Disabled	Auto/Untag
Gi1/0/5	Disabled	Auto/Untag
Gi1/0/6	Disabled	Auto/Untag
Gi1/0/7	Disabled	Auto/Untag
Gi1/0/8	Disabled	Auto/Untag
Gi1/0/9	Disabled	Auto/Untag
Gi1/0/10	Disabled	Auto/Untag

Figure 5-30 Voice VLAN Port

The following parameters can be configured in the **Voice VLAN Port** 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 voice VLAN feature on the specified port(s) here. When the voice VLAN is enabled for a port, the received voice packets will be forwarded in the voice VLAN. The received packets are determined as voice packets if the source MAC address of the packet complies with the OUI addresses.

Parameter	Description
Mode	<p>Select the mode here. Options to choose from are:</p> <ul style="list-style-type: none">• Auto Untagged - Specifies that voice VLAN untagged membership will be automatically learned.• Auto Tagged - Specifies that voice VLAN tagged membership will be automatically learned.• Manual - Specifies that voice VLAN membership will be manually configured. <p>If auto-learning is enabled, the port will automatically be learned as a voice VLAN member. This membership will automatically be aged out. When the port is working in the auto-tagged mode and the port captures a voice</p>

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

5.3.8.3 Voice VLAN OUI

This window is used to configure and display the voice VLAN OUI settings. A user-defined OUI can be associated with a voice VLAN. If the source MAC address of the received packet matches any of the OUI patterns, the received packet is determined as a voice packet. Default OUIs cannot be deleted or duplicated.

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI** to view the following window:

Voice VLAN OUI

Voice VLAN OUI

OUI Address: 00-01-E3-00-00-00 Mask: FF-FF-FF-00-00-00 Description: 32 chars Apply

Total Entries: 8

OUI Address	Mask	Description	
00-01-E3-00-00-00	FF-FF-FF-00-00-00	Siemens	Delete
00-03-6B-00-00-00	FF-FF-FF-00-00-00	Cisco	Delete
00-09-8E-00-00-00	FF-FF-FF-00-00-00	Avaya	Delete
00-0F-E2-00-00-00	FF-FF-FF-00-00-00	Huawei&3COM	Delete
00-60-B9-00-00-00	FF-FF-FF-00-00-00	NEC&Philips	Delete
00-D0-1E-00-00-00	FF-FF-FF-00-00-00	Pingtel	Delete
00-E0-75-00-00-00	FF-FF-FF-00-00-00	Veritel	Delete
00-E0-BB-00-00-00	FF-FF-FF-00-00-00	3COM	Delete

Figure 5-31 Voice VLAN OUI

The following parameters can be configured in the **Voice VLAN OUI** section:

Parameter	Description
OUI Address	Enter the voice VLAN OUI MAC address here.
Mask	Enter the matching bitmask for the voice VLAN OUI MAC address here.
Description	Enter the description for the user-defined OUI MAC address here. This string can be up to 32 characters long.

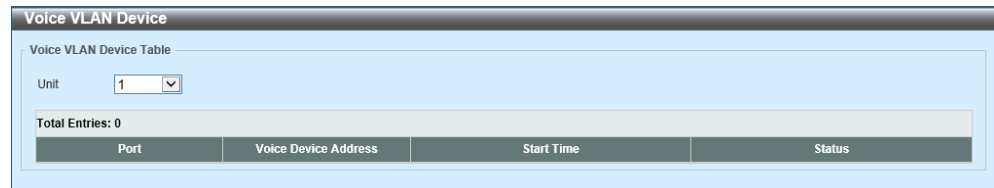
Click the **Apply** button to add a new entry based on the information specified.

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

5.3.8.4 Voice VLAN Device

This window is used to display the voice VLAN device table and information.

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN Device** to view the following window:



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

Figure 5-32 Voice VLAN Device

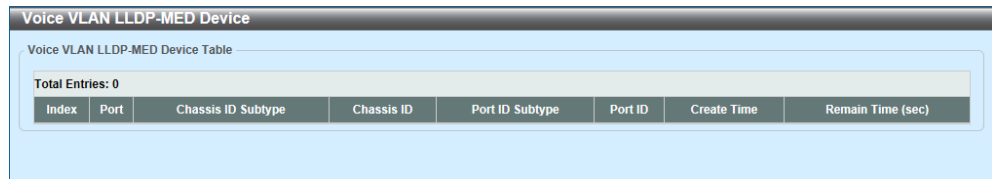
The following parameters can be configured in the **Voice VLAN Device Table** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.

5.3.8.5 Voice VLAN LLDP-MED Device

This window is used to display the voice VLAN LLDP-MED device table and information.

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device** to view the following window:



The screenshot shows a web interface window titled "Voice VLAN LLDP-MED Device". Inside, there is a section labeled "Voice VLAN LLDP-MED Device Table". Below this label, it says "Total Entries: 0". A table with 8 columns is displayed: Index, Port, Chassis ID Subtype, Chassis ID, Port ID Subtype, Port ID, Create Time, and Remain Time (sec). The table is currently empty.

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

Figure 5-33 Voice VLAN LLDP-MED Device

5.3.9 Private VLAN

This window is used to configure and display the private VLAN settings.

Click **L2 Features > VLAN > Private VLAN** to view the following window:

Figure 5-34 Private VLAN

The following parameters can be configured in the **Private VLAN** section:

Parameter	Description
VID List	Enter the private VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
State	Select to enable or disable the private VLAN state here.
Type	Select the type of private VLAN that will be created here. Options to choose from are Community , Isolated , and Primary .

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

The following parameters can be configured in the **Private VLAN Association** section:

Parameter	Description
VID List	Enter the private VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
Action	Select the action that will be taken for the private VLAN here. Options to choose from are Add , Remove , and Disabled .

Parameter	Description
Secondary VID List	Enter the secondary private VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

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

The following parameters can be configured in the **Private VLAN Host Association** 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.
Primary VID	Enter the primary VLAN ID that will be used here. The range is from 1 to 4094.
Secondary VID	Enter the secondary VLAN ID that will be used here. The range is from 1 to 4094. When ticking the Remove Association option, specifies that this configuration will not be enabled.

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

The following parameters can be configured in the **Private VLAN Mapping** 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.
Primary VID	Enter the primary VLAN ID that will be used here. The range is from 1 to 4094.
Action	Select Add to add a new entry based in the information entered. Select Remove to remove an entry based in the information entered.
Secondary VID List	Enter the secondary VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094. When ticking the Remove Mapping option, this specifies that this configuration will not be enabled.

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

5.4 STP (Spanning Tree Protocol)

5.4.1 STP Global Settings

This window is used to configure and display the global STP settings.

Click **L2 Features > STP > STP Global Settings** to view the following window:

Figure 5-35 STP Global Settings

The following parameters can be configured in the **STP State** section:

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

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

The following parameters can be configured in the **STP Mode** section:

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

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

The following parameters can be configured in the **STP Priority** section:

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

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

The following parameters can be configured in the **STP Configuration** section:

Parameter	Description
Bridge Max Age	Enter the bridge maximum age value here. The range is from 6 to 40 seconds. By default, this value is 20 seconds. The Maximum Age value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN.
Bridge Hello Time	After selecting RSTP/STP as the Spanning Tree Mode , this parameter will be available. Enter the bridge Hello Time value here. The range is from 1 to 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of Bridge Protocol Data Unit (BPDU) packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or Rapid Spanning Tree Protocol (RSTP) is selected for the STP version. For MSTP, the Hello Time must be set on a port per-port basis.
Bridge Forward Time	Enter the bridge Forwarding Time value here. The range is from 4 to 30 seconds. By default, this value is 15 seconds. Every port on the Switch spends this time in the Listening state while moving from the Blocking state to the Forwarding state.
TX Hold Count	Enter the Transmit Hold Count value here. The range is from 1 to 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.
Max Hops	Enter the maximum number of hops that are allowed. The range is from 6 to 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the Bridge Protocol Data Unit (BPDU) packet sent by the Switch will be discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out.

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

5.4.2 STP Port Settings

This window is used to configure and display the STP port settings.

Click **L2 Features > STP > STP Port Settings** to view the following window:

Port	State	Cost	Guard Root	Link Type	Port Fast	TCN Filter	BPDU Forward	Priority
Gi1/0/1	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
Gi1/0/2	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
Gi1/0/3	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
Gi1/0/4	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
Gi1/0/5	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
Gi1/0/6	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
Gi1/0/7	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
Gi1/0/8	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
Gi1/0/9	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
Gi1/0/10	Enabled	0/2000000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128

Figure 5-36 STP Port Settings

The following parameters can be configured in the **STP 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.
Cost	Enter the cost value here. The range is from 1 to 200000000. This value defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is 200000, a Gigabit port is 20000, and a 10 Gigabit port is 2000. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.
Guard Root	Select to enable or disable the Guard Root function.

Parameter	Description
Link Type	Select the Link Type option here. Options to choose from are Auto , P2P , and Shared . A full-duplex port is considered to have a Point-to-Point (P2P) connection. Alternatively, a half-duplex port is considered to have a Shared connection. The port cannot transit into the forwarding state rapidly by setting the link type to Shared . By default, this option is Auto .
Port Fast	Select the Port Fast option here. Options to choose from are: <ul style="list-style-type: none"> • Network - The port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. • Disabled - The port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. • Edge - The port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. By default, this option is Network .
TCN Filter	Select to enable or disable the Topology Change Notification (TCN) filter option. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is Disabled .
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is Disabled .
Priority	Select the priority value here. Options to choose from are 0 to 240 . By default, this option is 128. A lower value has higher priority.
Hello Time	Enter the hello time value here. The range is from 1 to 2 seconds. This value specifies the interval that a designated port will wait between the periodic transmissions of each configuration message.

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

5.4.3 MST Configuration Identification

This window is used to configure and display the MST configuration identification settings. These settings are used to identify Multiple Spanning Tree Instances (MSTIs) configured on the switch. The default Common Internal Spanning Tree (CIST) can be modified but cannot be deleted and the MSTI ID cannot be changed.

Click **L2 Features > STP > MST Configuration Identification** to view the following window:

MST Configuration Identification

MST Configuration Identification

Configuration Name: 00:50:40:3C:77:81

Revision Level (0-65535): 0

Digest: AC36177F50283CD4B83821D8AB26DE62

Apply

Private VLAN Synchronize

Private VLAN Synchronize

Apply

Instance ID Settings

Instance ID (1-64):

Action: Add VID

VID List: 1 or 3-5

Apply

Total Entries: 2

Instance ID	VID List	Edit	Delete
CIST	1,3-4094	Edit	Delete
1	2	Edit	Delete

1/1 1 Go

Figure 5-37 MST Configuration Identification

The following parameters can be configured in the **MST Configuration Identification** section:

Parameter	Description
Configuration Name	Enter the MST. This name uniquely identifies the MSTI. If the configuration name is not set, this field will show the MAC address to the device running MSTP.
Revision Level	Enter the revision level value here. The range is from 0 to 65535. By default, this value is 0. This value, along with the configuration name, identifies the MSTP region configured on the Switch.

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

The following parameters can be configured in the **Instance ID Settings** section:

Parameter	Description
Instance ID	Enter the instance ID here. The range is from 1 to 64.
Action	Select the action that will be taken here. Options to choose from are Add VID and Remove VID .
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

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

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

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.

5.4.4 STP Instance

This window is used to configure and display the STP instance settings.

Click **L2 Features > STP > STP Instance** to view the following window:

Instance	Instance State	Instance Priority	
CIST	Disabled	32768(32768 sysid 0)	Edit
1	Disabled	32769(32769 sysid 1)	Edit

1/1 1 Go

Instance CIST	
	CIST Global Info[Mode RSTP]
Bridge Address	00-50-40-3C-77-81
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 5-38 STP Instance

The following parameters can be configured in the **STP Instance** section:

Parameter	Description
Instance Priority	After clicking the Edit button, enter the Instance Priority value here. The range is from 0 to 61440.

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

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

5.4.5 MSTP Port Information

This window is used to configure and display the MSTP port information settings.

Click **L2 Features > STP > MSTP Port Information** to view the following window:

Figure 5-39 MSTP Port Information

The following parameters can be configured in the **MSTP Port Information** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Cost	After clicking the Edit button, enter the cost value here. The range is from 1 to 2000000000.
Priority	After clicking the Edit button, select the priority value here. Options to choose from are 0 to 240 . By default, this option is 128. A lower value has higher priority.

Click the **Clear Detected Protocol** button to remove the detected protocol association from the port specified.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

5.5 Line Loopback

5.5.1 Line Loopback Settings

This window is used to configure and display the line loopback settings.

Click **L2 Features > Line Loopback > Line Loopback Settings** to view the following window:

Port	Link	State	Loop Detect	Mode	Recovery	Recovery Time
Gi1/0/1	Up	Forwarding	Enabled	Block	Enabled	60
Gi1/0/2	Down	Forwarding	Enabled	Block	Enabled	60
Gi1/0/3	Down	Forwarding	Enabled	Block	Enabled	60
Gi1/0/4	Down	Forwarding	Enabled	Block	Enabled	60
Gi1/0/5	Down	Forwarding	Enabled	Block	Enabled	60
Gi1/0/6	Down	Forwarding	Enabled	Block	Enabled	60
Gi1/0/7	Down	Forwarding	Enabled	Block	Enabled	60
Gi1/0/8	Down	Forwarding	Enabled	Block	Enabled	60
Gi1/0/9	Down	Forwarding	Enabled	Block	Enabled	60
Gi1/0/10	Down	Forwarding	Enabled	Block	Enabled	60

Figure 5-40 Line Loopback Settings

The following parameters can be configured in the **Line Loopback Settings** section:

Parameter	Description
Global State	Select to globally enable or disable the line loopback feature.
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 line loopback feature on the specified port(s).
Mode	Select the line loopback mode that will be used on the specified port(s). Options to choose from are: <ul style="list-style-type: none"> Shutdown - Specifies to first set the port(s) to the shutdown state and then to the blocking state when a loop occurs. Block - Specifies to set the port(s) to the blocking state directly when a loop occurs.

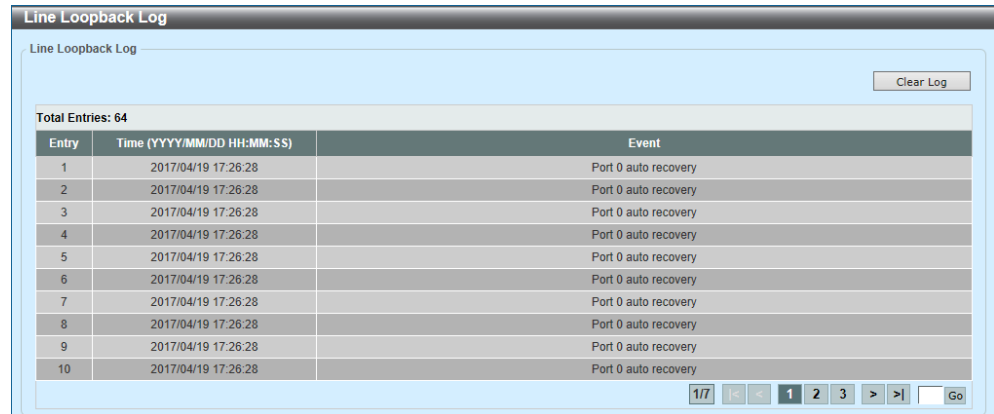
Parameter	Description
Loop Recovery	Select to enable or disable the loop recovery feature here. When enabled, the port(s) will be recovered to the normal state after the timeout value has expired. Enter the timeout value in the space provided. The range is from 60 to 86400 seconds.

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

5.5.2 Line Loopback Log

This window is used to display and clear the line loopback log.

Click **L2 Features > Line Loopback > Line Loopback Log** to view the following window:



Entry	Time (YYYY/MM/DD HH:MM:SS)	Event
1	2017/04/19 17:26:28	Port 0 auto recovery
2	2017/04/19 17:26:28	Port 0 auto recovery
3	2017/04/19 17:26:28	Port 0 auto recovery
4	2017/04/19 17:26:28	Port 0 auto recovery
5	2017/04/19 17:26:28	Port 0 auto recovery
6	2017/04/19 17:26:28	Port 0 auto recovery
7	2017/04/19 17:26:28	Port 0 auto recovery
8	2017/04/19 17:26:28	Port 0 auto recovery
9	2017/04/19 17:26:28	Port 0 auto recovery
10	2017/04/19 17:26:28	Port 0 auto recovery

Figure 5-41 Line Loopback Log

Click the **Clear Log** button to clear the log entries from the table.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.6 L2 Protocol Tunnel

This window is used to configure and display the Layer 2 protocol tunnel settings.

Click **L2 Features > L2 Protocol Tunnel** to view the following window:

The screenshot shows the 'L2 Protocol Tunnel' configuration window. It has two tabs: 'L2 Protocol Tunnel Global Settings' (selected) and 'L2 Protocol Tunnel Port Settings'. Under Global Settings, there are two rows of configuration: 'CoS for Encapsulated Packets' with a dropdown set to '5' and a 'Default' checkbox, and 'Drop Threshold (100-20000)' with a text box set to '0' and a 'Default' checkbox. An 'Apply' button is to the right. Below this is a section for adding new tunnels with fields for 'Action' (dropdown set to 'Add'), 'Tunneled Protocol' (dropdown set to 'GVRP'), 'Protocol MAC' (dropdown set to '01-00-0C-CC-CC-CC'), and 'MAC Address' (text box). An 'Apply' button is also here. At the bottom is a table with three columns: 'Protocol', 'Drop Counter', and 'Tunneling Address'.

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)

The following parameters can be configured in the **L2 Protocol Tunnel Global Settings** section:

Parameter	Description
CoS for Encapsulated Packets	Select the CoS value for encapsulated packets here. This value is between 0 and 7. Select the Default option to use the default value.
Drop Threshold	Enter the drop threshold value here. The range is from 100 to 20000. By default, this value is 0. The tunneling of the Layer 2 protocol packets will consume CPU processing power in encapsulating, decapsulating, and forwarding of the packet. Use this option to restrict the CPU processing bandwidth consumed by specifying a threshold on the number of all Layer 2 protocol packets that can be processed by the system. When the maximum number of packets is exceeded, the excessive protocol packets are dropped. Select the Default option to use the default value.
Action	Select the action that will be taken here. Options to choose from are Add and Delete . This is used to add or delete a Layer 2 Protocol Tunneling (L2PT) tunneling multicast address to or from the specified protocol.

Parameter	Description
Tunneled Protocol	Select the tunneled protocol here. Options to choose from are: <ul style="list-style-type: none"> • GVRP - Specifies that GVRP packets will be tunneled to the configured address. • STP - Specifies that STP packets will be tunneled to the configured address. • MAC - Specifies that protocol packets with the specified destination address will be tunneled to the configured address. • All - Specifies that all packets will be tunneled to the configured address.
Protocol MAC	After selecting the MAC option as the Tunneled Protocol , select the destination address that will be tunneled to the configured address here. Options to choose from are 01-00-0C-CC-CC-CC and 01-00-0C-CC-CC-CD .
MAC Address	Enter the MAC address of which the specified protocol will be tunneled to here. This MAC address should not be an address reserved or used by other protocols.

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

Click the **L2 Protocol Tunnel Port Settings** tab to view the following window:

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

The following parameters can be configured in the **L2 Protocol Tunnel 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.
Action	Select Add to add a new entry based in the information entered. Select Delete to delete an entry based in the information entered.

Parameter	Description
Type	Select the type option here. Options to choose from are None , Shutdown , and Drop .
Tunneled Protocol	Select the tunneled protocol option here. Options to choose from are GVRP , STP , Protocol MAC , and All .
Protocol MAC	After selecting the Protocol MAC option as the Tunneled Protocol , the following option will be available. Select the protocol MAC option here. Options to choose from are 01-00-0C-CC-CC-CC and 01-00-0C-CC-CC-CD .
Threshold	After selecting the Shutdown or Drop option in the Type field, the following parameter will be available. Enter the threshold value here. The range is from 1 to 4096.

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

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

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

5.7 L2 Multicast Control

5.7.1 IGMP Snooping

5.7.1.1 IGMP Snooping Settings

This window is used to configure and display the Internet Group Management Protocol (IGMP) snooping settings.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings** to view the following window:

Figure 5-44 IGMP Snooping Settings

The following parameters can be configured in the **Global Settings** section:

Parameter	Description
Global State	Select this option to globally enable or disable IGMP snooping.

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

The following parameters can be configured in the **VLAN Status Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

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

The following parameters can be configured in the **IGMP Snooping Table** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

Click the **Show Detail** button to display detailed information related to the entry.

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

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

Click the **Show Detail** button to view the following window:

IGMP Snooping VLAN Parameters	
VID	1
Status	Disabled
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

[Modify](#)

Figure 5-45 IGMP Snooping Settings (Show Detail)

Click the **Modify** button to edit the settings.

Click the **Edit** or **Modify** button to view the following window:

IGMP Snooping VLAN Settings	
VID (1-4094)	<input type="text" value="1"/>
Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Fast Leave	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Querier State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Query Version	<input type="text" value="3"/>
Query Interval (1-31744)	<input type="text" value="125"/> sec
Max Response Time (1-25)	<input type="text" value="10"/> sec
Robustness Value (1-7)	<input type="text" value="2"/>
Last Member Query Interval (1-25)	<input type="text" value="1"/> sec
Proxy Reporting	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Source Address <input type="text" value="0.0.0.0"/>
Rate Limit (1-1000)	<input type="text" value="0"/> <input checked="" type="checkbox"/> No Limit

[Apply](#)

Figure 5-46 IGMP Snooping Settings (Edit, Modify)

The following parameters can be configured in the **IGMP Snooping VLAN Settings** section:

Parameter	Description
Fast Leave	Select this option to enable or disable the IGMP snooping fast-leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message.
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the IGMP snooping querier. Options to choose from are 1, 2, and 3.
Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically. The range is from 1 to 31744.
Max Response Time	Enter the maximum response time, in seconds, advertised in IGMP snooping queries. The range is from 1 to 25.
Robustness Value	Enter the robustness variable used in IGMP snooping. The range is from 1 to 7.
Last Member Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages. The range is from 1 to 25.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Source Address	Enter the source IP of proxy reporting. This is available when Enabled is selected in Proxy Reporting .
Rate Limit	Enter the rate limit value here. The range is from 1 to 1000. Tick the No Limit option to apply no rate limit on this profile.

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

5.7.1.2 IGMP Snooping Groups Settings

This window is used to configure and display the IGMP snooping group settings.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings** to view the following window:

Figure 5-47 IGMP Snooping Groups Settings

The following parameters can be configured in the **IGMP Snooping Static Groups Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Enter an IP multicast group address.
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.

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

Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **IGMP Snooping Static Groups Table** section:

Parameter	Description
VID	Select and enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

The following parameters can be configured in the **IGMP Snooping Groups Table** section:

Parameter	Description
VID	Select and enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.
Detail	Select this option to display the IGMP group detail information.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

5.7.1.3 IGMP Snooping Filter Settings

This window is used to configure and display the IGMP snooping filter settings.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Filter Settings** to view the following window:

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

- IGMP Snooping Rate Limit Settings:** Fields for Unit (1), From Port (Gi1/0/1), To Port (Gi1/0/1), and Limit Number (1-1000). There is a 'No Limit' checkbox and an 'Apply' button.
- IGMP Snooping Limit Settings:** Fields for Unit (1), From Port (Gi1/0/1), To Port (Gi1/0/1), Limit Number (1-4096), Exceed Action (Default), Except ACL Name (32 chars), and VID (1-4094). There is a 'Please Select' button and an 'Apply' button.
- Access Group Settings:** Fields for Unit (1), From Port (Gi1/0/1), To Port (Gi1/0/1), Action (Add), ACL Name (32 chars), and VID (1-4094). There is a 'Please Select' button and an 'Apply' button.
- IGMP Snooping Filter Table:** Fields for Unit (1), From Port (Gi1/0/1), and To Port (Gi1/0/1). It includes 'Find' and 'Show All' buttons. Below is a table with 1 entry:

Port	Rate Limit
Gi1/0/10	1000pps

 There is a 'Show Detail' button and a 'Go' button at the bottom right.

Figure 5-48 IGMP Snooping Filter Settings

The following parameters can be configured in the **IGMP Snooping Rate Limit 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. This is only available if the Port option was selected as the action below.
Limit Number	Enter the limit number here. This is to configure the rate of IGMP control packets that the Switch can process on a specific interface. The range is from 1 to 1000 packets per second. Select the No Limit option to remove the limitation.

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

The following parameters can be configured in the **IGMP Snooping Limit 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.
Limit Number	Enter the limit number here. This is used to set the limitation on the number of IGMP cache entries that can be created. The range is from 1 to 4096.
Exceed Action	Select the exceed action here. This parameter specifies the action for handling newly learned groups when the limitation is exceeded. Options to choose from are: <ul style="list-style-type: none"> • Default - Specifies that the default action will be taken. • Drop - Specifies that the new group will be dropped. • Replace - Specifies that the new group will replace the oldest group.
Except ACL Name	Enter the standard IP access list name here. The group (*,G), or channel (S,G) permitted by the access list will be excluded from the limit. To permit a channel (S,G), specify S in the source address field and G in the destination address field of the access list entry. To permit a group (*,G), specify "any" in the source address field and G in the destination address field of the access list entry. This name can be up to 32 characters long. Alternatively, click the Please Select button to find and select any of the exiting access lists configured on this Switch to be used in this configuration.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

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

Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Access Group 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.
Action	Select Add to add a new entry based in the information entered. Select Delete to delete an entry based in the information entered.
ACL Name	Enter the standard IP access list name here. This is used to permit users to join a group (*, G), specify "any" in source address field and G in destination address field of the access list entry. This name can be up to 32 characters long. Alternatively, click the Please Select button to find and select any of the exiting access lists configured on this Switch to be used in this configuration.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

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

The following parameters can be configured in the **IGMP Snooping Filter Table** 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.

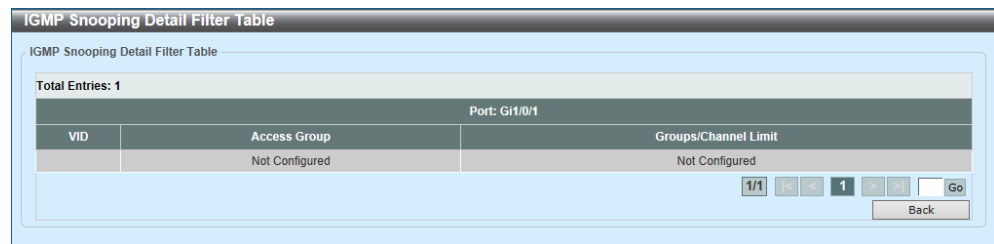
Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to view the following window:



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

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

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

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

5.7.1.4 IGMP Snooping Multicast Router Information

This window is used to configure and display the IGMP Snooping multicast router settings.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Multicast Router Information** to view the following window:

Figure 5-50 IGMP Snooping Multicast Router Information

The following parameters can be configured in the **IGMP Snooping Multicast Router Port Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Configuration	Select the port configuration. Options to choose from are: <ul style="list-style-type: none"> Port - Select to have the configured ports to be static multicast router ports. Forbidden Port - Select to have the configured ports not to be multicast router ports.
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.

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

Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **IGMP Snooping Multicast Router Port Table** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

5.7.1.5 IGMP Snooping Statistics Settings

This window is used to display and clear IGMP snooping statistics.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings** to view the following window:

Figure 5-51 IGMP Snooping Statistics Settings

The following parameters can be configured in the **IGMP Snooping Statistics Settings** section:

Parameter	Description
Statistics	Select the interface here. Options to choose from are All , VLAN , and Port .
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. This is available when VLAN is selected in the Statistics drop-down list.
Unit	Select the unit ID of the switch in the physical stack here. This is available when Port is selected in the Statistics drop-down list.
From Port - To Port	Select the port(s) that will be used here. This is available when Port is selected in the Statistics drop-down list.

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

The following parameters can be configured in the **IGMP Snooping Statistics Table** section:

Parameter	Description
Find Type	Select the interface type. Options to choose from are VLAN , and Port .
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. This is available when VLAN is selected in the Find Type drop-down list.
Unit	Select the unit ID of the switch in the physical stack here. This is available when Port is selected in the Find Type drop-down list.
From Port - To Port	Select the port(s) that will be used here. This is available when Port is selected in the Find Type drop-down list.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

5.7.2 MLD Snooping

5.7.2.1 MLD Snooping Settings

This window is used to configure and display the Multicast Listener Discovery (MLD) snooping settings.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings** to view the following window:

Figure 5-52 MLD Snooping Settings

The following parameters can be configured in the **Global Settings** section:

Parameter	Description
Global State	Select this option to enable or disable the global MLD snooping state.

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

The following parameters can be configured in the **VLAN Status Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

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

The following parameters can be configured in the **MLD Snooping Table** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

Click the **Show Detail** button to display detailed information related to the entry.

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

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

Click the **Show Detail** button to view the following window:

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

[Modify](#)

Figure 5-53 MLD Snooping Settings (Show Detail)

Click the **Modify** button to edit the settings.

Click the **Edit** or **Modify** button to view the following window:

MLD Snooping VLAN Settings	
VID (1-4094)	<input type="text" value="1"/>
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Fast Leave	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Proxy Reporting	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Source Address: <input type="text"/>
Querier State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Query Version	<input type="text" value="2"/>
Query Interval (1-31744)	<input type="text" value="125"/> sec
Max Response Time (1-25)	<input type="text" value="10"/> sec
Robustness Value (1-7)	<input type="text" value="2"/>
Last Listener Query Interval (1-25)	<input type="text" value="1"/> sec
Rate Limit (1-1000)	<input type="text"/> <input checked="" type="checkbox"/> No Limit

[Apply](#)

Figure 5-54 MLD Snooping Settings (Edit, Modify)

The following parameters can be configured in the **IGMP Snooping VLAN Settings** section:

Parameter	Description
Fast Leave	Select this option to enable or disable the MLD snooping fast-leave function. If enabled, the membership is immediately removed when the system receives the MLD leave message.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Source Address	Enter the source IP of proxy reporting. This is available when Enabled is selected in Proxy Reporting .
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the MLD snooping querier. Options to choose from are 1, and 2.
Query Interval	Enter the interval at which the MLD snooping querier sends MLD general query messages periodically. The range is from 1 to 31744.
Max 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 used in MLD snooping. The range is from 1 to 7.
Last Listener Query Interval	Enter the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages. The range is from 1 to 25.
Rate Limit	Enter the rate limit value here. The range is from 1 to 1000. Tick the No Limit option to apply no rate limit on this profile.

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

5.7.2.2 MLD Snooping Groups Settings

This window is used to configure and display the MLD snooping group settings.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings** to view the following window:

Figure 5-55 MLD Snooping Groups Settings

The following parameters can be configured in the **MLD Snooping Static Groups Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Enter the IPv6 multicast group address here.
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.

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

Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **MLD Snooping Static Groups Table** section:

Parameter	Description
VID	Select and enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IPv6 multicast group address.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

The following parameters can be configured in the **MLD Snooping Groups Table** section:

Parameter	Description
VID	Select and enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IPv6 multicast group address.
Detail	Select this option to display the MLD group detail information.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

5.7.2.3 MLD Snooping Filter Settings

This window is used to configure and display the MLD snooping filter settings.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Filter Settings** to view the following window:

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

- MLD Snooping Rate Limit Settings:** Includes fields for Unit (1), From Port (Gi1/0/1), To Port (Gi1/0/1), and Limit Number (1-1000). There is a 'No Limit' checkbox and an 'Apply' button.
- MLD Snooping Limit Settings:** Includes fields for Unit (1), From Port (Gi1/0/1), To Port (Gi1/0/1), Limit Number (1-2048), Exceed Action (Default), Except ACL Name (32 chars), and VID (1-4094). There is a 'Please Select' button and an 'Apply' button.
- Access Group Settings:** Includes fields for Unit (1), From Port (Gi1/0/1), To Port (Gi1/0/1), Action (Add), ACL Name (32 chars), and VID (1-4094). There is a 'Please Select' button and an 'Apply' button.
- MLD Snooping Filter Table:** Includes fields for Unit (1), From Port (Gi1/0/1), To Port (Gi1/0/1), and buttons for Find, Show All, and Go. Below these fields is a table with the following data:

Port	Rate Limit
Gi1/0/10	1000pps

Figure 5-56 MLD Snooping Filter Settings

The following parameters can be configured in the **MLD Snooping Rate Limit 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. This is only available if the Port option was selected as the action below.
Limit Number	Enter the limit number here. This number is used to configure the rate of MLD control packets that the Switch can process on a specific interface. The range is from 1 to 1000 packets per second. Select the No Limit option to remove the limitation.

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

The following parameters can be configured in the **MLD Snooping Limit 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.
Limit Number	Enter the limit number here. This is used to set the limitation on the number of MLD cache entries that can be created. The range is from 1 to 2048.
Exceed Action	Select the exceed action here. This parameter specifies the action for handling newly learned groups when the limitation is exceeded. Options to choose from are: <ul style="list-style-type: none"> • Default - Specifies that the default action will be taken. • Drop - Specifies that the new group will be dropped. • Replace - Specifies that the new group will replace the oldest group.
Except ACL Name	Enter the standard IP access list name here. The group (*,G), or channel (S,G) permitted by the access list will be excluded from the limit. To permit a channel (S,G), specify S in the source address field and G in the destination address field of the access list entry. To permit a group (*,G), specify "any" in the source address field and G in the destination address field of the access list entry. This name can be up to 32 characters long. Alternatively, click the Please Select button to find and select any of the exiting access lists configured on this Switch to be used in this configuration.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

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

Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Access Group 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.

Parameter	Description
Action	Select Add to add a new entry based in the information entered. Select Delete to delete an entry based in the information entered.
ACL Name	Enter the standard IP access list name here. This is used to permit users to join a group (*, G), specify "any" in source address field and G in destination address field of the access list entry. This name can be up to 32 characters long. Alternatively, click the Please Select button to find and select any of the exiting access lists configured on this Switch to be used in this configuration.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

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

The following parameters can be configured in the **MLD Snooping Filter Table** 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.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to view the following window:

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

1/1 [Go] [Back]

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

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

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

5.7.2.4 MLD Snooping Multicast Router Information

This window is used to configure and display the MLD snooping multicast router settings.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Multicast Router Information** to view the following window:

Figure 5-58 MLD Snooping Multicast Router Information

The following parameters can be configured in the **MLD Snooping Multicast Router Port Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Configuration	Select the port configuration. Options to choose from are: <ul style="list-style-type: none"> • Port - Select to have the configured ports as being connected to multicast-enabled routers. • Forbidden Port - Select to have the configured ports as being not connected to multicast-enabled routers.
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.

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

Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **MLD Snooping Multicast Router Port Table** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

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

5.7.2.5 MLD Snooping Statistics Settings

This window is used to display and clear MLD snooping statistics.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings** to view the following window:

Figure 5-59 MLD Snooping Statistics Settings

The following parameters can be configured in the **MLD Snooping Statistics Settings** section:

Parameter	Description
Statistics	Select the interface here. Options to choose from are All , VLAN , and Port .
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. This is available when VLAN is selected in the Statistics drop-down list.
Unit	Select the unit ID of the switch in the physical stack here. This is available when Port is selected in the Statistics drop-down list.
From Port - To Port	Select the port(s) that will be used here. This is available when Port is selected in the Statistics drop-down list.

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

The following parameters can be configured in the **MLD Snooping Statistics Table** section:

Parameter	Description
Find Type	Select the interface type. Options to choose from are VLAN and Port .
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. This is available when VLAN is selected in the Find Type drop-down list.
Unit	Select the unit ID of the switch in the physical stack here. This is available when Port is selected in the Find Type drop-down list.
From Port - To Port	Select the port(s) that will be used here. This is available when Port is selected in the Find Type drop-down list.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

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

5.7.3 Multicast Filtering Mode

This window is used to configure and display the multicast filtering mode.

Click **L2 Features > L2 Multicast Control > Multicast Filtering Mode** to view the following window:

Figure 5-60 Multicast Filtering Mode

The following parameters can be configured in the **Multicast Filtering Mode** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are: <ul style="list-style-type: none"> • Forward Unregistered - Registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. • Forward All - All multicast packets will be flooded based on the VLAN domain. • Filter Unregistered - Registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

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

5.8 LLDP (Link Layer Discovery Protocol)

5.8.1 LLDP Global Settings

This window is used to configure and display the global LLDP settings.

Click **L2 Features > LLDP > LLDP Global Settings** to view the following window:

LLDP Global Settings

LLDP Global Settings

LLDP State ☐ Enabled ☒ Disabled

LLDP Forward State ☐ Enabled ☒ Disabled

LLDP Trap State ☐ Enabled ☒ Disabled

LLDP-MED Trap State ☐ Enabled ☒ Disabled Apply

LLDP-MED Configuration

Fast Start Repeat Count (1-10) times ☐ Default Apply

LLDP Configurations

Message TX Interval (5-32768) sec ☐ Default

Message TX Hold Multiplier (2-10) sec ☐ Default

Retmit Delay (1-10) sec ☐ Default

TX Delay (1-8192) sec ☐ Default Apply

LLDP System Information

Chassis ID Subtype MAC Address

Chassis ID 00-50-40-3C-77-81

System Name Switch

System Description Gigabit Ethernet Switch

System Capabilities Supported Repeater, Bridge

System Capabilities Enabled Repeater, Bridge

LLDP-MED System Information

Device Class Network Connectivity Device

Hardware Revision A1

Firmware Revision V1.0.0.03

Software Revision V1.0.0.07

Serial Number 73S53010056

Manufacturer Name Panasonic

Model Name ZEQUO6600RE

Asset ID

Figure 5-61 LLDP Global Settings

The following parameters can be configured in the **LLDP Global Settings** section:

Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature
LLDP Forward State	Select this option to enable or disable LLDP forward state. When the LLDP State is disabled and LLDP Forward State is enabled, the received LLDP Data Unit (LLDPDU) packet will be forwarded.
LLDP Trap State	Select this option to enable or disable the LLDP trap state.
LLDP-MED Trap State	Select this option to enable or disable the LLDP Media Endpoint Discovery (LLDP-MED) trap state.

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

The following parameters can be configured in the **LLDP-MED Configuration** section:

Parameter	Description
Fast Start Repeat Count	Enter the LLDP-MED fast start repeat count value. The range is from 1 to 10. Select the Default option to use the default value.

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

The following parameters can be configured in the **LLDP Configurations** section:

Parameter	Description
Message TX Interval	Enter the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds. Select the Default option to use the default value.
Message TX Hold Multiplier	Enter the multiplier on the LLDPDU's transmission interval that used to calculate the Time-To-Live (TTL) value of an LLDPDU. The range is from 2 to 10. Select the Default option to use the default value.
ReInit Delay	Enter the delay value for LLDP initialization on an interface. The range is from 1 to 10 seconds. Select the Default option to use the default value.
TX Delay	Enter the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer. Select the Default option to use the default value.

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

5.8.2 LLDP Port Settings

This window is used to configure and display the LLDP port settings.

Click **L2 Features > LLDP > LLDP Port Settings** to view the following window:

Port	Notification	Subtype	Admin State	IPv4/IPv6 Address
Gi1/0/1	Disabled	Local	TX and RX	
Gi1/0/2	Disabled	Local	TX and RX	
Gi1/0/3	Disabled	Local	TX and RX	
Gi1/0/4	Disabled	Local	TX and RX	
Gi1/0/5	Disabled	Local	TX and RX	
Gi1/0/6	Disabled	Local	TX and RX	
Gi1/0/7	Disabled	Local	TX and RX	
Gi1/0/8	Disabled	Local	TX and RX	
Gi1/0/9	Disabled	Local	TX and RX	
Gi1/0/10	Disabled	Local	TX and RX	

Figure 5-62 LLDP Port Settings

The following parameters can be configured in the **LLDP 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.
Notification	Select to enable or disable the notification feature here.
Subtype	Select the subtype of LLDP Type-Length-Value (TLV) here. Options to choose from are MAC Address and Local .
Admin State	<p>Select the local LLDP agent and allow it to send and receive LLDP frames on the port. Options to choose from are:</p> <ul style="list-style-type: none"> TX - The local LLDP agent can only transmit LLDP frames. RX - The local LLDP agent can only receive LLDP frames. TX and RX - The local LLDP agent can both transmit and receive LLDP frames. Disabled - The local LLDP agent can neither transmit nor receive LLDP frames. <p>The default option is TX and RX.</p>
IP Subtype	Select the type of the IP address information to be sent. Options to choose from are Default , IPv4 and IPv6 .

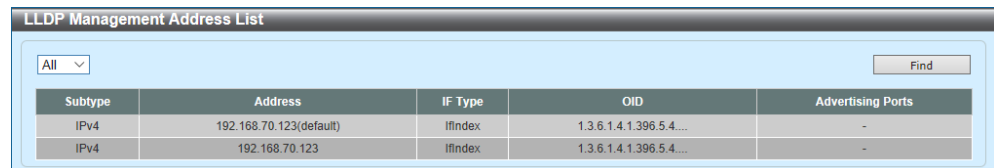
Parameter	Description
Action	Select the action that will be taken here. Options to choose from are Remove and Add .
Address	Enter the IP address that will be sent.

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

5.8.3 LLDP Management Address List

This window is used to display the LLDP management address list and information.

Click **L2 Features > LLDP > LLDP Management Address List** to view the following window:



Subtype	Address	IF Type	OID	Advertising Ports
IPv4	192.168.70.123(default)	IfIndex	1.3.6.1.4.1.396.5.4...	-
IPv4	192.168.70.123	IfIndex	1.3.6.1.4.1.396.5.4...	-

Figure 5-63 LLDP Management Address List

The following parameters can be configured:

Parameter	Description
Subtype	<p>Select the subtype. Options to choose from are All, IPv4 and IPv6.</p> <ul style="list-style-type: none">After selecting the IPv4 option, enter the IPv4 address in the space provided.After selecting the IPv6 option, enter the IPv6 address in the space provided.

Click the **Find** button to find and display entries in the table based on the search criteria specified.

5.8.4 LLDP Basic TLVs Settings

This window is used to configure and display the basic LLDP TLV settings.

Click **L2 Features > LLDP > LLDP Basic TLVs Settings** to view the following window:

Port	Port Description	System Name	System Description	System Capabilities
Gi1/0/1	Disabled	Disabled	Disabled	Disabled
Gi1/0/2	Disabled	Disabled	Disabled	Disabled
Gi1/0/3	Disabled	Disabled	Disabled	Disabled
Gi1/0/4	Disabled	Disabled	Disabled	Disabled
Gi1/0/5	Disabled	Disabled	Disabled	Disabled
Gi1/0/6	Disabled	Disabled	Disabled	Disabled
Gi1/0/7	Disabled	Disabled	Disabled	Disabled
Gi1/0/8	Disabled	Disabled	Disabled	Disabled
Gi1/0/9	Disabled	Disabled	Disabled	Disabled
Gi1/0/10	Disabled	Disabled	Disabled	Disabled

Figure 5-64 LLDP Basic TLVs Settings

The following parameters can be configured in the **LLDP Basic TLVs 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.
Port Description	Select to enable or disable the sending of the port description TLV.
System Name	Select to enable or disable the sending of the system name TLV.
System Description	Select to enable or disable the sending of the system description TLV.
System Capabilities	Select to enable or disable the sending of the system capabilities TLV.

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

5.8.5 LLDP Dot1 TLVs Settings

This window is used to configure and display the IEEE 802.1 LLDP TLV settings.

Click **L2 Features > LLDP > LLDP Dot1 TLVs Settings** to view the following window:

Port	Port VLAN ID	Enabled Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity
Gi1/0/1	Disabled			
Gi1/0/2	Disabled			
Gi1/0/3	Disabled			
Gi1/0/4	Disabled			
Gi1/0/5	Disabled			
Gi1/0/6	Disabled			
Gi1/0/7	Disabled			
Gi1/0/8	Disabled			
Gi1/0/9	Disabled			
Gi1/0/10	Disabled			

Figure 5-65 LLDP Dot1 TLVs Settings

The following parameters can be configured in the **LLDP Dot1 TLVs 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.
Port VLAN	Select to enable or disable the sending of the port VLAN ID TLV.
Protocol VLAN	Select to enable or disable the sending of the port and protocol VLAN ID (PPVID) TLV. Enter the ID of the protocol VLAN in the space provided.
VLAN Name	Select to enable or disable the sending of the VLAN name TLV. Enter the ID of the VLAN in the space provided.
Protocol Identity	Select to enable or disable the sending of the protocol identity TLV. Options for protocol name to choose from are None , EAPOL , LACP , GVRP , STP , and All .

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

5.8.6 LLDP Dot3 TLVs Settings

This window is used to configure and display the IEEE 802.3 LLDP TLV settings.

Click **L2 Features > LLDP > LLDP Dot3 TLVs Settings** to view the following window:

Unit	From Port	To Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size
1	Gi1/0/1	Gi1/0/1	Disabled	Disabled	Disabled

Unit 1 Settings			
Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size
Gi1/0/1	Disabled	Disabled	Disabled
Gi1/0/2	Disabled	Disabled	Disabled
Gi1/0/3	Disabled	Disabled	Disabled
Gi1/0/4	Disabled	Disabled	Disabled
Gi1/0/5	Disabled	Disabled	Disabled
Gi1/0/6	Disabled	Disabled	Disabled
Gi1/0/7	Disabled	Disabled	Disabled
Gi1/0/8	Disabled	Disabled	Disabled
Gi1/0/9	Disabled	Disabled	Disabled
Gi1/0/10	Disabled	Disabled	Disabled

Figure 5-66 LLDP Dot3 TLVs Settings

The following parameters can be configured in the **LLDP Dot3 TLVs 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.
MAC/PHY Configuration/Status	Select to enable or disable the sending of the MAC/PHY configuration/status TLV.
Link Aggregation	Select to enable or disable the sending of the link aggregation TLV.
Maximum Frame Size	Select to enable or disable the sending of the maximum frame size TLV.

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

5.8.7 LLDP-MED Port Settings

This window is used to configure and display the LLDP-MED port settings.

Click **L2 Features > LLDP > LLDP-MED Port Settings** to view the following window:

Port	Notification	Capabilities	Inventory	Network Policy
Gi1/0/1	Disabled	Disabled	Disabled	Disabled
Gi1/0/2	Disabled	Disabled	Disabled	Disabled
Gi1/0/3	Disabled	Disabled	Disabled	Disabled
Gi1/0/4	Disabled	Disabled	Disabled	Disabled
Gi1/0/5	Disabled	Disabled	Disabled	Disabled
Gi1/0/6	Disabled	Disabled	Disabled	Disabled
Gi1/0/7	Disabled	Disabled	Disabled	Disabled
Gi1/0/8	Disabled	Disabled	Disabled	Disabled
Gi1/0/9	Disabled	Disabled	Disabled	Disabled
Gi1/0/10	Disabled	Disabled	Disabled	Disabled

Figure 5-67 LLDP-MED Port Settings

The following parameters can be configured in the **LLDP-MED 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.
Notification	Select to enable or disable the sending of the LLDP-MED notification TLV.
Capabilities	Select to enable or disable the sending of the LLDP-MED capabilities TLV.
Inventory	Select to enable or disable the sending of the LLDP-MED inventory management TLV.
Network Policy	Select to enable or disable the sending of the LLDP-MED network policy TLV.

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

5.8.8 LLDP Statistics Information

This window is used to display and clear the LLDP statistics.

Click **L2 Features > LLDP > LLDP Statistics Information** to view the following window:

LLDP Statistics Information

LLDP Statistics Information

Last Change Time 0
Total Inserts 0
Total Deletes 0
Total Drops 0
Total Ageouts 0

Clear Counter

LLDP Statistics Ports

Unit 1 Port Gi1/0/1

Clear Counter Clear All

Unit 1 Settings

Port	Total Transmits	Total Discards	Total Errors	Total Receives	Total TLV Discards	Total TLV Unknowns	Total Ageouts
Gi1/0/1	0	0	0	0	0	0	0
Gi1/0/2	0	0	0	0	0	0	0
Gi1/0/3	0	0	0	0	0	0	0
Gi1/0/4	0	0	0	0	0	0	0
Gi1/0/5	0	0	0	0	0	0	0
Gi1/0/6	0	0	0	0	0	0	0
Gi1/0/7	0	0	0	0	0	0	0
Gi1/0/8	0	0	0	0	0	0	0
Gi1/0/9	0	0	0	0	0	0	0
Gi1/0/10	0	0	0	0	0	0	0

Figure 5-68 LLDP Statistics Information

The following parameters can be configured in the **LLDP Statistics Ports** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.

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

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

5.8.9 LLDP Local Port Information

This window is used to display local LLDP port information.

Click **L2 Features > LLDP > LLDP Local Port Information** to view the following window:

Port	Port ID Subtype	Port ID	Port Description
Gi1/0/1	Local	Gi1/0/1	Panasonic ZEQUO6600RE HW A1 fl...
Gi1/0/2	Local	Gi1/0/2	Panasonic ZEQUO6600RE HW A1 fl...
Gi1/0/3	Local	Gi1/0/3	Panasonic ZEQUO6600RE HW A1 fl...
Gi1/0/4	Local	Gi1/0/4	Panasonic ZEQUO6600RE HW A1 fl...
Gi1/0/5	Local	Gi1/0/5	Panasonic ZEQUO6600RE HW A1 fl...
Gi1/0/6	Local	Gi1/0/6	Panasonic ZEQUO6600RE HW A1 fl...
Gi1/0/7	Local	Gi1/0/7	Panasonic ZEQUO6600RE HW A1 fl...
Gi1/0/8	Local	Gi1/0/8	Panasonic ZEQUO6600RE HW A1 fl...
Gi1/0/9	Local	Gi1/0/9	Panasonic ZEQUO6600RE HW A1 fl...
Gi1/0/10	Local	Gi1/0/10	Panasonic ZEQUO6600RE HW A1 fl...

Figure 5-69 LLDP Local Port Information

The following parameters can be configured in the **LLDP Local Port Brief Table** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.

Click the **Find** button to find and LLDP local port information associated with the specified port

Click the **Show Detail** button to display detailed LLDP local port information associated with the specified port

Click the **Show Detail** button to view the following window:

The screenshot displays the 'LLDP Local Port Information' window. It contains two main sections: 'LLDP Local Information Table' and 'LLDP Local Management Address Detail Table'.

LLDP Local Information Table

Port	Gi1/0/1
Port ID Subtype	Local
Port ID	Gi1/0/1
Port Description	Panasonic ZEQUO6600RE HW A1 firmware V1.0.0.07 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
Link Aggregation	Show Detail
Maximum Frame Size	1518
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail

[Back](#)

LLDP Local Management Address Detail Table

Port	Subtype	Address	IF Type	OID
Gi1/0/1	IPv4	System(192.168.70.123)	IfIndex	1.3.6.1.4.1.396.5.4....
Gi1/0/1	IPv4	192.168.70.123	IfIndex	1.3.6.1.4.1.396.5.4....

Figure 5-70 LLDP Local Port Information (Show Detail)

Click each individual link to display detailed information related to the specified feature in the table.

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

5.8.10 LLDP Neighbor Port Information

This window is used to display neighboring LLDP port information.

Click **L2 Features > LLDP > LLDP Neighbor Port Information** to view the following window:

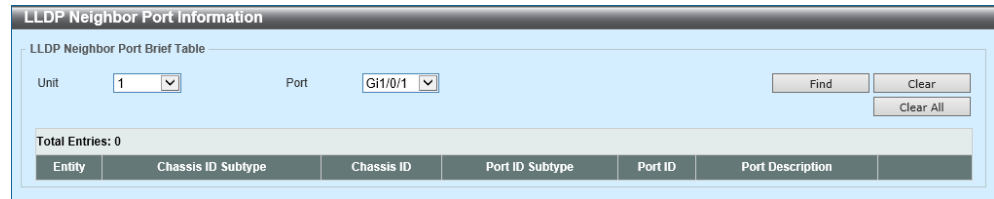


Figure 5-71 LLDP Neighbor Port Information

The following parameters can be configured in the **LLDP Neighbor Port Brief Table** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.

Click the **Find** button to find and LLDP neighbor port information associated with the specified port

Click the **Clear** button to clear LLDP neighbor port information associated with the specified port.

Click the **Clear All** button to clear all LLDP neighbor port information.

5.9 UDLD (Unidirectional Link Detection)

Use the following window, and then implement the UDLD settings to display the settings and condition.

Choose **L2 Features > UDLD** to display the following window.

Port	Admin State	Mode	Link State	Neighbor MAC	Neighbor Port	Neighbor State
Gi1/0/1	Disabled	Normal	Unknown	-	-	-
Gi1/0/2	Disabled	Normal	Unknown	-	-	-
Gi1/0/3	Disabled	Normal	Unknown	-	-	-
Gi1/0/4	Disabled	Normal	Unknown	-	-	-
Gi1/0/5	Disabled	Normal	Unknown	-	-	-
Gi1/0/6	Disabled	Normal	Unknown	-	-	-
Gi1/0/7	Disabled	Normal	Unknown	-	-	-
Gi1/0/8	Disabled	Normal	Unknown	-	-	-
Gi1/0/9	Disabled	Normal	Unknown	-	-	-
Gi1/0/10	Disabled	Normal	Unknown	-	-	-
Gi1/0/11	Disabled	Normal	Unknown	-	-	-
Gi1/0/12	Disabled	Normal	Unknown	-	-	-

图 5-72 UDLD

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

Parameter	Description
UDLD Detection Time	Configure the unidirectional connection detection time (seconds). The range of the configuration is from 5 to 65,535 seconds. The factory default settings is five (5) seconds.
From Port - To Port	Choose the port you use.
Administration State	Enable or disable the UDLD function of the port specified. The factory default settings is Enabled.
Mode	Choose the UDLD mode to be used on the port specified. The factory default settings is Normal. The options (or values) available are as follows: <ul style="list-style-type: none"> [Normal] - If you detect the unidirectional connection, relay the link of the corresponding port to record an event on the system log. [Shutdown] - If you detect the unidirectional connection, execute to shutdown the corresponding ports to record an event on the system log.

Click **Apply** to reflect the change.

NOTE

You can use this function among our products.

5.10 RRP (Ring Redundant Protocol)

This window is used to configure and display the RRP settings.

Click **L2 Features > RRP** to view the following window:

RRP Settings					
RRP Global Status					
RRP Status		<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		<button>Apply</button>	
RRP Domain Status					
Domain Name		<input type="text" value="25 chars"/>		<button>Create</button>	
Total Entries: 1					
Domain Name	Control VLAN	Data VLAN(s)	Ring Status		
Domain	0		IDLE	<button>Show Detail</button>	<button>Delete</button>

Figure 5-73 RRP

The following parameters can be configured in the **RRP Global Status** section:

Parameter	Description
RRP Status	Select to enable or disable the RRP feature here.

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

The following parameters can be configured in the **RRP Domain Status** section:

Parameter	Description
Domain Name	Enter the RRP domain name here. This can be up to 25 characters long. The domain represents the physical ring.

Click the **Create** button to create a new RRP domain.

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to view the following window:

The 'RRP Domain Status' window displays the following configuration details:

Parameter	Value
RRP Domain Name	Domain
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 the **Edit** button to edit the settings.

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

Click the **Edit** button to view the following window:

The 'RRP Domain Settings' window displays the following configuration options:

Parameter	Value
RRP Domain Name	Domain
RRP Domain Status	Disabled
RRP Node Type	Master
Primary Port	Gi1/0/1 <input checked="" type="checkbox"/> Default
Secondary Port	Gi1/0/1 <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 (Edit)

The following parameters can be configured in the **RRP Domain Settings** section:

Parameter	Description
RRP Domain Status	Select the enable or disable the RRP domain here.
RRP Node Type	<p>Select the RRP node type here. Options to choose from are:</p> <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 an RRP domain. Responsibilities 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 an RRP domain. Responsibilities of a transit node include link down alerts.

Parameter	Description
Primary Port	Select the primary switch unit and port here. This port will be the first port in the RRP domain. Select the Default option to clear current settings.
Secondary Port	Select the secondary switch unit and port here. This port will be the second port in the RRP domain. Select the Default option to clear current settings.
Polling Interval	Enter the hello-packet polling interval here. The range is from 1 to 2 seconds. The polling interval should be shorter than the fail period.
Fail Period	Enter the fail period here. The range is from 2 to 5 seconds. The fail period should be longer than the polling interval.
Ring Guard Port	Select to status of the guard port in the RRP ring here. Options to choose from are: <ul style="list-style-type: none">• Primary - Specifies use the primary port as the ring guard-enabled port.• Secondary - Specifies the secondary port as the ring guard-enabled port.• Both - Specifies both the primary and secondary ports as ring guard-enabled ports.• Disable - Specifies to disable this feature.
Control VLAN	Enter the ID of the control VLAN here. The range is from 2 to 4094.
Data VLAN	Enter the ID(s) of the data VLAN(s) here. The range is from 1 to 4094.

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

Click the **Cancel** button to discard the changes made.

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

6 L3 Features

6.1 ARP (Address Resolution Protocol)

6.1.1 ARP Control Settings

This window is used to enable or disable the ARP refresh before timeout feature.

Click **L3 Features > ARP > ARP Control Settings** to view the following window:

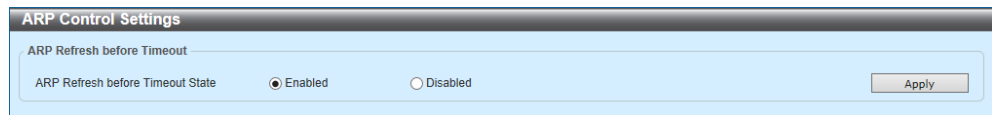


Figure 6-1 ARP Control Settings

The following parameters can be configured in the **ARP Refresh before Timeout** section:

Parameter	Description
ARP Refresh before Timeout State	Select to enable or disable the ARP refresh before timeout feature here.

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

6.1.2 ARP Aging Time

This window is used to configure and display the ARP aging time settings.

Click **L3 Features > ARP > ARP Aging Time** to view the following window:

Figure 6-2 ARP Aging Time

The following parameters can be configured in the **ARP Aging Time Search** section:

Parameter	Description
Interface VLAN	Enter the VLAN ID here. The range is from 1 to 4094.
Timeout	After clicking the Edit button, enter the timeout value here. The range is from 0 to 65535 minutes.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

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

6.1.3 Static ARP

This window is used to configure and display the static ARP settings.

Click **L3 Features > ARP > Static ARP** to view the following window:

Interface Name	IP Address	Hardware Address	Aging Time	Type	Edit	Delete
vlan1	192.168.70.123	00-50-40-3C-77-81	Forever			

Figure 6-3 Static ARP

The following parameters can be configured in the **Static ARP Setting** section:

Parameter	Description
IP Address	Enter the IP address that will be associated with the MAC address here.
Hardware Address	Enter the MAC address that will be associated with the IP address here.

Click the **Apply** button to add a new Static ARP entry.

The following parameters can be configured in the **Static ARP Search** section:

Parameter	Description
IP Address	Select and enter the IP address of the entry here.
IP Network Mask	Select and enter the subnet mask for the IP address here.
Hardware Address	Select and enter the MAC address of the entry here.
Interface VLAN	Select and enter the VLAN ID here. The range is from 1 to 4094.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

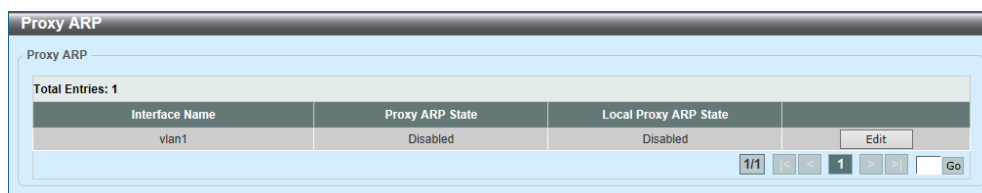
Click the **Delete** button to delete the entry.

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

6.1.4 Proxy ARP

This window is used to configure and display the proxy ARP settings. Proxy ARP will allow the switch to respond to ARP requests destined for another device by mimicking its IP and MAC Address as the original ARP responder. The switch can route packets to the intended destination without adding static routes or default gateways. Hosts will respond to packets destined to other devices.

Click **L3 Features > ARP > Proxy ARP** to view the following window:



Interface Name	Proxy ARP State	Local Proxy ARP State
vian1	Disabled	Disabled

Figure 6-4 Proxy ARP

The following parameters can be configured in the **Static ARP Search** section:

Parameter	Description
Proxy ARP State	After clicking the Edit button, select to enable or disable the Proxy ARP state here.
Local Proxy ARP State	After clicking the Edit button, select to enable or disable the local Proxy ARP state here. This local Proxy ARP function allows the Switch to respond to the Proxy ARP, if the source IP and destination IP are in the same interface.

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

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

6.1.5 ARP Table

This window is used to display and clear the ARP entries in the table.

Click **L3 Features > ARP > ARP Table** to view the following window:

ARP Table

ARP Search

☒ Interface VLAN (1-4094) ☐ IP Address Mask ☐ Hardware Address ☐ Type

Total Entries: 6

Interface Name	IP Address	Hardware Address	Aging Time (min)	Type	
vlan1	192.168.70.14	10-BF-48-D6-E2-E2	240		<input type="button" value="Clear"/>
vlan1	192.168.70.15	00-23-7D-BC-2E-18	240		<input type="button" value="Clear"/>
vlan1	192.168.70.101	24-24-0E-E5-96-DE	240		<input type="button" value="Clear"/>
vlan1	192.168.70.104	30-F7-C5-20-83-B6	240		<input type="button" value="Clear"/>
vlan1	192.168.70.123	00-50-40-3C-77-81	Forever		<input type="button" value="Clear"/>
vlan1	192.168.70.212	00-22-33-88-99-44	Forever	Static	<input type="button" value="Clear"/>

1/1

Figure 6-5 ARP Table

The following parameters can be configured in the **ARP Search** section:

Parameter	Description
Interface VLAN	Select and enter the VLAN ID of the interface here. This range is from 1 to 4094.
IP Address	Select and enter the IP address to display here.
Mask	Select and enter the subnet mask for the IP address here.
Hardware Address	Select and enter the MAC address to display here.
Type	Select the Type option here. Options to choose from are All and Dynamic .

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Clear All** button to remove all the entries from the table.

Click the **Clear** button to remove the specified entry.

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

6.2 Gratuitous ARP

This window is used to configure and display the gratuitous ARP settings. A gratuitous ARP request packet is an ARP request packet where the source and the destination IP address are both set to the IP address of the sending device and the destination MAC address is the broadcast address. A device uses a gratuitous ARP request packet to discover whether the IP address is duplicated by other hosts or to preload or reconfigure the ARP cache entry of hosts connected to the interface.

Click **L3 Features > Gratuitous ARP** to view the following window:

Figure 6-6 Gratuitous ARP

The following parameters can be configured in the **Gratuitous ARP Global Settings** section:

Parameter	Description
IP Gratuitous ARP State	Select to enable or disable the transmission of gratuitous ARP request packets.
Gratuitous ARP Trap State	Select to enable or disable the gratuitous ARP feature trap state here.
IP Gratuitous ARP Dad-Reply State	Select to enable or disable the IP gratuitous ARP Dad-reply state.
Gratuitous ARP Learning State	Select to enable or disable the gratuitous ARP learning state. Normally, the system will only learn ARP entries from ARP reply packets or a normal ARP request packet that asks for the MAC address of the Switch IP address. This option used to enable or disable the learning of ARP entries based on received gratuitous ARP packets. The gratuitous ARP packet is sent by a source IP address and is identical to the IP that the packet is querying.

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

The following parameters can be configured in the **Gratuitous ARP Send Interval** section:

Parameter	Description
Interval Time	After clicking the Edit button, enter the gratuitous ARP sending interval time, in seconds, here.

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

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

6.3 IPv6 Neighbor

This window is used to configure and display the IPv6 neighbor settings.

Click **L3 Features > IPv6 Neighbor** to view the following window:

The screenshot shows the 'IPv6 Neighbor' configuration window. It includes a settings section with input fields for Interface VLAN, IPv6 Address, and MAC Address. Below this is a search section with 'Find' and 'Clear' buttons. A table displays the current neighbor entries, showing one entry with IPv6 Address 2017::1, Link-Layer Address 11-22-33-44-55-66, Interface vlan1, and Type Static. The table also has a 'Delete' button. At the bottom, there are pagination controls indicating 1/1 entries and a 'Go' button.

Figure 6-7 IPv6 Neighbor

The following parameters can be configured in the **IPv6 Neighbor Settings** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here.
IPv6 Address	Enter the IPv6 address.
MAC Address	Enter the MAC address.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Clear** button to clear the information based on the criteria specified.

Click the **Clear All** button to remove all the dynamic entries.

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.

6.4 Interface

6.4.1 IPv4 Interface

This window is used to configure and display the IPv4 interface settings.

Click **L3 Features > Interface > IPv4 Interface** to view the following window:

Figure 6-8 IPv4 Interface

The following parameters can be configured in the **IPv4 Interface** section:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. The range is from 1 to 4094.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Edit** button to edit the settings of the specified 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.

Click the **Edit** button to view the following window:

The screenshot shows the 'IPv4 Interface Configure' window. It has two tabs: 'IPv4 Interface Settings' (selected) and 'DHCP Client'. The 'Interface' is 'vian1'. In the 'Settings' section, 'State' is 'Enabled', 'IP MTU (512-16383)' is '1500' bytes, and 'IP Directed Broadcast' is 'Disabled'. In the 'IP Settings' section, 'Get IP From' is 'Static', 'IP Address' is '192.168.80.123', 'Mask' is '255.255.255.0', and 'Secondary' is unchecked. At the bottom, there is a 'Secondary IP Entry' table with one entry: IP Address 192.168.80.123, Mask 255.255.255.0, Boot Mode Manual, and Secondary Yes. Buttons for 'Back', 'Apply', and 'Delete' are visible.

Figure 6-9 IPv4 Interface (Edit, IPv4 Interface Settings)

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

Parameter	Description
State	Select to enable or disable the IPv4 interface global state.
IP MTU	Enter the Maximum Transmission Unit (MTU) value here. The range is from 512 to 16383 bytes. By default, this value is 1500 bytes.
IP Directed Broadcast	Select to enable or disable the IP directed broadcast feature here. This parameter is used to enable or disable the conversion of IP directed broadcasts received by the interface to physical broadcasts when the destination network is directly connected to the Switch.

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

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

The following parameters can be configured in the **IP Settings** section:

Parameter	Description
Get IP From	Select the get IP from option here. Options to choose from are: <ul style="list-style-type: none"> Static - Enter the IPv4 address settings of this interface manually in the fields provided. DHCP - This interface will obtain IPv4 settings automatically from the DHCP server located on the local network.
IP Address	Enter the IPv4 address for this interface here.

Parameter	Description
Mask	Enter the IPv4 subnet mask for this interface here.
Secondary	Tick this option to use the IPv4 address and mask as the secondary interface configuration.

Click the **Apply** button to 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.

Click the **DHCP Client** tab to view the following window:

The screenshot shows the 'IPv4 Interface Configure' window with the 'DHCP Client' tab selected. It contains the following fields and controls:

- DHCP Client Client-ID (1-4094)**: A text input field.
- Class ID String**: A text input field with a '32 chars' label and a 'Hex' checkbox.
- Host Name**: A text input field with a '64 chars' label.
- Lease**: A text input field for days (0-10000), and dropdown menus for hours (00) and minutes (00).
- Apply**: A button in the bottom right corner.

Figure 6-10 IPv4 Interface (Edit, DHCP Client)

The following parameters can be configured in the **DHCP Client** section:

Parameter	Description
DHCP Client Client-ID	Enter the DHCP Client ID here. The range is from 1 to 4094. This parameter is used to specify the VLAN interface whose hexadecimal MAC address will be used as the client ID sent with the discover message.
Class ID String	Enter the class ID string here. This string can be up to 32 characters long. Select the Hex option to enter the Class ID string in the hexadecimal format. This string can be up to 64 characters long. This parameter is used to specify the vendor class identifier used as the value of Option 60 in the DHCP discover message.
Host Name	Enter the host name here. This string can be up to 64 characters long. This parameter is used to specify the value of the host name option to be sent with the DHCP discover message.
Lease	Enter and optionally select the DHCP client lease time here. In the textbox, the lease time, in days, can be entered. The range is from 0 to 10000 days. Hours and Minutes can also be selected optionally.

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

6.4.2 IPv6 Interface

This window is used to configure and display the IPv6 interface settings.

Click **L3 Features > Interface > IPv6 Interface** to view the following window:

Figure 6-11 IPv6 Interface

The following parameters can be configured in the **IPv6 Interface** section:

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

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to view the following window:

Figure 6-12 IPv6 Interface (Show Detail, IPv6 Interface Settings)

The following parameters can be configured in the **IPv6 Interface Settings** section:

Parameter	Description
IPv6 MTU	Enter the IPv6 MTU value here. The range is from 1280 to 65534 bytes. By default, this value is 1500 bytes. This parameter is used to configure the MTU to be advertised in Router Advertisement (RA) messages.
IPv6 State	Select to enable or disable the IPv6 interface global state here.

Click the **Back** button to return to the previous window.
Click the **Apply** button to accept the changes made.

The following parameters can be configured in the **Static IPv6 Address Settings** section:

Parameter	Description
IPv6 Address	Enter the IPv6 address for this IPv6 interface here. <ul style="list-style-type: none"> Select the Extended Unique Identifier 64-bit (EUI-64) option to configure an IPv6 address on the interface using the EUI-64 interface ID. Select the Link Local option to configure a link-local address for the IPv6 interface.

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

Click the **Interface IPv6 Address** tab to view the following window:

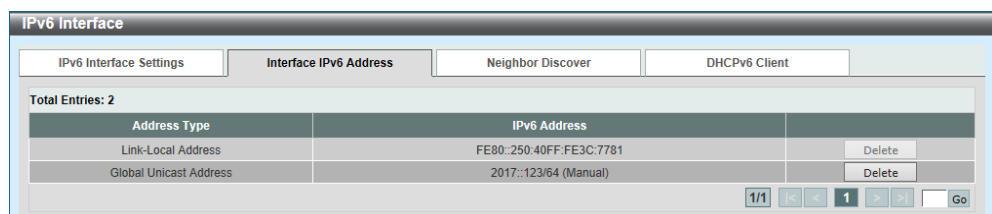


Figure 6-13 IPv6 Interface (Show Detail, Interface IPv6 Address)

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.

Click the **Neighbor Discover** tab to view the following window:

The screenshot shows the 'IPv6 Interface' configuration window with the 'Neighbor Discover' tab selected. The 'ND Settings' section includes the following parameters:

- Managed Config Flag: Off
- RA Min Interval (3-1350): 66 sec
- RA Lifetime (0-9000): 1800 sec
- Reachable Time (0-3600000): 1200000 millisecond
- Hop Limit (0-255): 64
- Other Config Flag: Off
- RA Max Interval (4-1800): 200 sec
- RA Suppress: Enabled
- NS Interval (0-3600000): 0 millisecond

An 'Apply' button is located at the bottom right of the settings section. Below the settings is a table titled 'Total Entries: 1'.

IPv6 Prefix/Prefix Length	Preferred Life Time (sec)	Valid Life Time (sec)	Link Flag	Autoconfig Flag	
2017::/64	604800	2592000	Enabled	Enabled	Edit

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

Figure 6-14 IPv6 Interface (Show Detail, Neighbor Discover)

The following parameters can be configured in the **ND Settings** section:

Parameter	Description
Managed Config Flag	Turn the Managed Config Flag option On or Off here. When the neighbor host receives the RA which has flag turned on, the host should use a stateful configuration protocol to obtain IPv6 addresses.
Other Config Flag	Turn the Other Config Flag option On or Off here. By setting the other configuration flag on, the router instructs the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than the IPv6 address.
RA Min Interval	Enter the minimum RA interval time value here. The range is from 3 to 1350 seconds. This value must be smaller than 0.75 times the maximum value.
RA Max Interval	Enter the maximum RA interval time value here. The range is from 4 to 1800 seconds.
RA Lifetime	Enter the RA lifetime value here. The range is from 0 to 9000 seconds. The lifetime value in RA instructs the received host the lifetime value for taking the router as the default router.
RA Suppress	Select to enable or disable the RA suppress feature here.
Reachable Time	Enter the Reachable Time here. The range is from 0 to 3600000 milliseconds. If the specified time is 0, the router will use 1200 seconds on the interface and advertise 1200 (unspecified) in the RA message. The Reachable Time is used by the IPv6 node in determining the reachability of the neighbor nodes.
NS Interval	Enter the Neighbor Solicitation (NS) interval value here. The range is from 0 to 3600000 milliseconds, in multiples of 1000. If the specified time is 0, the router will use 1 second.

Parameter	Description
Hop Limit	Enter the hop limit value here. The range is from 0 to 255. The IPv6 packet originated by the system will also use this value as the initial hop limit.

Click the **Apply** button to add a new entry.

Click the **Edit** button to edit the settings of the specified entry.

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

Click the **DHCPv6 Client** tab to view the following window:

Figure 6-15 IPv6 Interface (Show Detail, DHCPv6 Client)

Click the **Restart** button to restart the DHCPv6 client feature.

The following parameters can be configured in the **DHCPv6 Client Settings** section:

Parameter	Description
Client State	Select to enable or disable the DHCPv6 client service here. Select the Rapid Commit option to proceed with two-message exchange for address delegation. The rapid-commit option will be included in the Solicit message to request a two-message handshake.

The following parameters can be configured in the **DHCPv6 Client PD Settings** section:

Parameter	Description
Client PD State	Select to enable or disable the DHCPv6 client process that requests a Prefix Delegation (PD) through a specified interface. Select the Rapid Commit option to proceed with two-message exchange for prefix delegation. The rapid-commit option will be included in the Solicit message to request a two-message handshake.

Parameter	Description
General Prefix Name	Enter the IPv6 general prefix name here. This name can be up to 12 characters long.
IPv6 DHCP Client PD Hint	Enter the IPv6 prefix to be sent in the message as a hint here.

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

6.4.3 Loopback Interface

This window is used to configure and display the loopback interface settings.

Click **L3 Features > Interface > Loopback Interface** to view the following window:

Interface	State	Link Status	
loopback1	Disabled	Down	<button>Edit</button> <button>Delete</button>

Figure 6-16 Loopback Interface

The following parameters can be configured in the **Loopback Interface** section:

Parameter	Description
Interface Loopback	Enter the loopback interface ID here. The range is from 1 to 8.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Edit** button to edit the settings of the specified 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.

Click the **Edit** button to view the following window:

Interface	loopback1	<button>Back</button>
State	Disabled	<button>Apply</button>
IPv4		
IP Address		<button>Apply</button>

Figure 6-17 Loopback Interface (Edit)

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

The following parameters can be configured in the first section:

Parameter	Description
State	Select to enable or disable the loopback interface here.

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

The following parameters can be configured in the **IPv4** section:

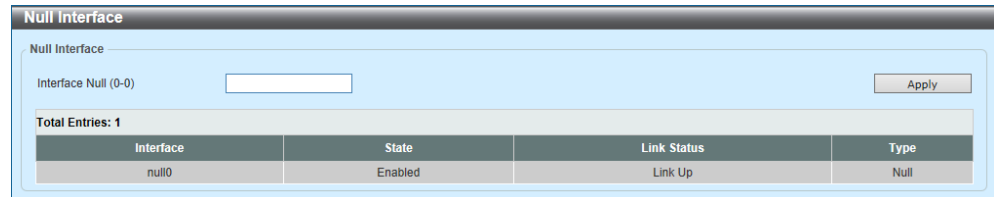
Parameter	Description
IP Address	Enter the IPv4 address associated with this loopback interface here.
Mask	Enter the IPv4 subnet mask associated with this loopback interface here.

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

6.4.4 Null Interface

This window is used to configure and display the Null interface settings.

Click **L3 Features > Interface > Null Interface** to view the following window:



Interface	State	Link Status	Type
null0	Enabled	Link Up	Null

Figure 6-18 Null Interface

The following parameters can be configured in the **Null Interface** section:

Parameter	Description
Interface Null	Enter the Null interface ID here. This value can only be 0.

Click the **Apply** button to add a new entry.

6.5 IPv4 Static/Default Route

This window is used to configure and display IPv4 static and default routes.

Click **L3 Features > IPv4 Static/Default Route** to view the following window:

Figure 6-19 IPv4 Static/Default Route

The following parameters can be configured in the **IPv4 Static/Default Route** section:

Parameter	Description
IP Address	Enter the IPv4 address for this route here. Tick the Default Route option to use the default route as the IPv4 address.
Mask	Enter the IPv4 network mask for this route here.
Gateway	Enter the gateway address for this route here.
Null Interface	Select to enable or disable the NULL interface here.
Backup State	<p>Select the backup state option here. Options to choose from are:</p> <ul style="list-style-type: none"> • Primary - Specifies the route as the primary route to the destination. • Backup - Specifies the route as the backup route to the destination. • Weight - Specifies a weight number greater than zero, but less than the maximum paths number. This number is used to replicate identical route paths (multiple copies) in the routing table, so the paths get more chance of being hit for traffic routing. If the weight number is not specified for the static route, the default for the path exists in the hashing table. Enter the weight value in the space provided. The range is from 1 to 64.

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.

6.6 IPv4 Route Table

This window is used to display the IPv4 route table and information.

Click **L3 Features > IPv4 Route Table** to view the following window:

IPv4 Route Table

☒ IP Address
☐ Network Address
☐ RIP ☐ OSPF ☐ Connected ☐ Hardware ☐ Summary

Find Show All

Total Entries: 3

IP Address	Mask	Gateway	Interface	Distance/Metric	Protocol	Candidate Default
0.0.0.0	0.0.0.0	192.168.70.1	vlan1	1/1	Static	Yes
192.168.70.0	255.255.255.0	Directly Connected	vlan1	-	Connected	-
192.168.80.0	255.255.255.0	Directly Connected	vlan1_1	-	Connected	-

1/1 1 2 3 4 5 6 7 8 9 10 Go

Figure 6-20 IPv4 Route Table

The following parameters can be configured in the **IPv4 Route Table** section:

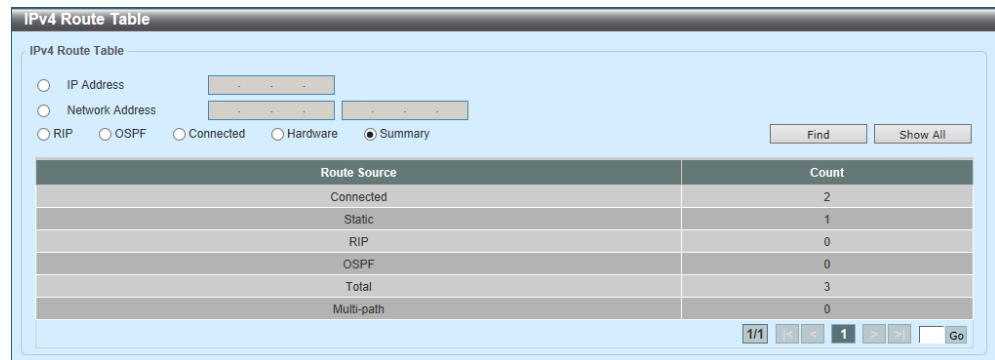
Parameter	Description
IP Address	Select and enter the single IPv4 address here.
Network Address	Select and enter the IPv4 network address here. In the first space enter the network prefix and in the second space enter the network mask.
RIP	Select this option to display only RIP routes.
OSPF	Select this option to display only OSPF routes.
Connected	Select this option to display only connected routes.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

Click the **Summary** option to view the following window:



The screenshot shows a window titled "IPv4 Route Table". At the top, there are search filters: "IP Address" and "Network Address" (both with empty text boxes), and radio buttons for "RIP", "OSPF", "Connected", "Hardware", and "Summary" (which is selected). To the right of these are "Find" and "Show All" buttons. Below the filters is a table with two columns: "Route Source" and "Count". The table lists the following sources and counts: Connected (2), Static (1), RIP (0), OSPF (0), Total (3), and Multi-path (0). At the bottom right of the table area, there is a pagination control showing "1/1", navigation arrows, a page number "1", and a "Go" button.

Route Source	Count
Connected	2
Static	1
RIP	0
OSPF	0
Total	3
Multi-path	0

Figure 6-21 IPv4 Route Table (Summary)

6.7 IPv6 Static/Default Route

This window is used to configure and display IPv6 static or default routes.

Click **L3 Features > IPv6 Static/Default Route** to view the following window:

Figure 6-22 IPv6 Static/Default Route

The following parameters can be configured in the **IPv6 Static/Default Route** section:

Parameter	Description
IPv6 Address/Prefix Length	Enter the IPv6 address and prefix length for this route here. Tick the Default Route option to use this route as the default route.
Interface Name	Enter the name of the interface that will be associated with this route here.
Next Hop IPv6 Address	Enter the next hop IPv6 address here.
Distance	Enter the administrative distance of the static route here. The range is from 1 to 254. A lower value represents a better route. If not specified, the default administrative distance for a static route is 1.
Backup State	Select the backup state option here. Options to choose from are: <ul style="list-style-type: none"> • Primary - The route is specified as the primary route to the destination. • Backup - The route is specified as the backup route to the destination.

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.

6.8 IPv6 Route Table

This window is used to display IPv6 route table and information.

Click **L3 Features > IPv6 Route Table** to view the following window:

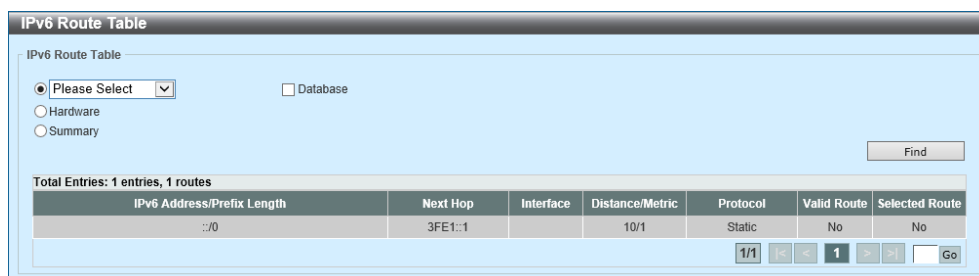


Figure 6-23 IPv6 Route Table

The following parameters can be configured in the **IPv6 Route Table** section:

Parameter	Description
IPv6 Address	Select and enter the IPv6 address to display here.
IPv6 Address/Prefix Length	Select and enter the IPv6 address and prefix length to display here. Select the Longer Prefixes option to display the route and all of the more specific routes.
Interface Name	Select and enter the name of the interface to display here.
Connected	Select this option to display only connected routes.
OSPFv3	Select this option to display only OSPFv3 routes.
Database	Select this option to display all the related entries in the routing database instead of just the best route.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

Click the **Find** button to find and display entries based on the search criteria specified.

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

Click the **Summary** option to view the following window:

IPv6 Route Table

☐ Connected ☐ Database

☐ Hardware

☒ Summary

Find

Route Source	Count
Connected	0
Static	0
OSPF	0
Total	0

1/1 < > 1 Go

Figure 6-24 IPv6 Route Table (Summary)

6.9 Route Preference

This window is used to configure and display the route preference settings.

Click **L3 Features > Route Preference** to view the following window:

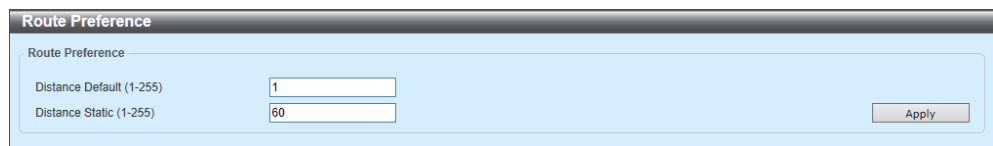


Figure 6-25 Route Preference

The following parameters can be configured in the **Route Preference** section:

Parameter	Description
Distance Default	Enter the administrative distance of default routes here. The range is from 1 to 255. By default, this value is 1.
Distance Static	Enter the administrative distance of static default routes here. The range is from 1 to 255. By default, this value is 60.

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

6.10 ECMP Settings[ZEQUO6700RE/6600RE]

This window is used to configure and display the Equal-Cost Multi-Path (ECMP) routing settings.

Click **L3 Features > ECMP Settings** to view the following window:

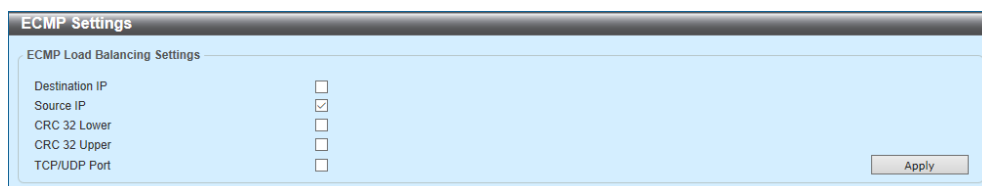


Figure 6-26 ECMP Settings

The following parameters can be configured in the **ECMP Load Balancing Settings** section:

Parameter	Description
Destination IP	Select this option to use the destination IP address as the ECMP hash key.
Source IP	Select this option to use the least significant bits of the source IP address as the ECMP hashing algorithm.
CRC 32 Lower	Select this option to use the lower bits of CRC-32 as the ECMP hashing algorithm.
CRC 32 Upper	Select this option to use the upper bits of CRC-32 as the ECMP hashing algorithm.
TCP/UDP Port	Select this option to use TCP/UDP port number as ECMP hash key.

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

6.11 IPv6 General Prefix

This window is used to configure and display the general IPv6 prefixes.

Click **L3 Features > IPv6 General Prefix** to view the following window:

Figure 6-27 IPv6 General Prefix

The following parameters can be configured in the **IPv6 General Prefix** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
Prefix Name	Enter the IPv6 general prefix entry name here. This name can be up to 12 characters long.
IPv6 Address	Enter the IPv6 address and prefix length here. The prefix length of the IPv6 address is also the local subnet on the VLAN interface.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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.

6.12 RIP (Routing Information Protocol)

6.12.1 RIP Settings

This window is used to configure and display the RIP settings.

Click **L3 Features > RIP > RIP Settings** to view the following window:

Figure 6-28 RIP Settings

The following parameters can be configured in the **RIP Global Settings** section:

Parameter	Description
RIP State	Select to globally enable or disable the RIP feature here.

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

The following parameters can be configured in the **Redistribution Configuration** section:

Parameter	Description
Redistribution	<p>Select to enable or disable the RIP redistribution feature here.</p> <p>Select the routing protocol (domain) that will be redistributed into RIP. Options to choose from are Connected, OSPF, and Static.</p> <ul style="list-style-type: none"> The Connected option refers to routes that are established automatically through configuring an IP address on an interface. The Static option means redistribute IP static routes. Enter the metric value for the redistributed route in the space provided. The range is from 0 to 16.

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

The following parameters can be configured in the **RIP Configuration** section:

Parameter	Description
Update Time	Enter the update interval in seconds at which the update message is sent. The range is from 1 to 65535 seconds. Select the Default option to use the default value here which is 30 seconds.
Invalid Time	Enter the invalid time value in seconds here. The range is from 1 to 65535 seconds. Select the Default option to use the default value here which is 180 seconds.
Flush Time	Enter the flush time value in seconds here. The range is from 1 to 65535 seconds. Select the Default option to use the default value here which is 120 seconds.
Default Metric	Enter the default metric value here. The range is from 0 to 16. The default metric is used in redistributing routes from other routing protocols. The routes being redistributed are learned by other protocols and may have an incompatible metric to RIP. The specifying of the metric allows the metric to be synced. Select the Default option to use the default metric value, which is 0.
Version	Select the global RIP version that will be used as the default version for all interfaces here. Options to choose from are v1 (RIPv1) and v2 (RIPv2). Select the Default option to specify that this feature should use the default configuration. By default, RIPv1 and RIPv2 packets are received, but only RIPv1 packets are sent.

Parameter	Description
Distance	Enter the Administrative Distance for RIP here. The range is from 1 to 255. A lower value represents a better route. Select the Default option to use the default Administrative Distance for RIP, which is 100.
Global Passive Interface State	Select to globally enable or disable the passive interface state here. The sending of RIP routing updates will globally be disabled when this feature is enabled.

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

6.12.2 RIP Interface Settings

This window is used to configure and display the RIP interface settings.

Click **L3 Features > RIP > RIP Interface Settings** to view the following window:

Interface	Send	Receive	Send v2-broadcast	Authentication Mode	Passive Interface	IP Interface Address
vlan1	v1	v1	Disabled	None	Disabled	192.168.70.123/24

Figure 6-29 RIP Interface Settings

The following parameters can be configured in the **RIP Interface Settings** section:

Parameter	Description
Network	Enter the IPv4 network address used by RIP here. Interfaces that have a subnet belonging to the network specified here will be activated for RIP.

Click the **Add** button to add a new entry.

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

Click the **Edit** button to edit the settings of the specified entry.

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

Click the **Edit** button to view the following window:

Figure 6-30 RIP Interface Settings (Edit)

The following parameters can be configured in the **Configure RIP Interface** section:

Parameter	Description
Send Version	Select the RIP version that will be used in the sending of RIP packets on the interface. Options to choose from are RIP version 1 (v1) and RIP version 2 (v2).
Received Version	Select the RIP version that will be used in the receiving of RIP packets on the interface. Options to choose from are RIP version 1 (v1), RIP version 2 (v2), and RIP version 1 or 2 (v1/v2).
Send v2-broadcast	Select to enable or disable the sending of RIP version 2 update packets as broadcast packets instead of multicast packets.
Authentication Mode	Select the authentication mode here. Options to choose from are Disabled and Text .
Authentication Text Password	Select and enter the authentication text password here. This can be up to 16 characters long and can only be entered when Text was selected as the Authentication Mode .
Passive Interface	Select to enable or disable the passive interface option here. The sending of RIP routing updates in this interface will be disabled when this feature is enabled.

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

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

6.12.3 RIP Database

This window is used to display the RIP routing database.

Click **L3 Features > RIP > RIP Database** to view the following window:

The screenshot shows the 'RIP Database' window. At the top, there's a 'Network Address' search field with two input boxes and buttons for 'Find' and 'Show All'. Below this, it says 'Total Entries: 1 entries, 1 routes'. A table displays the following data:

Network	Next Hop	Metric	From	Interface	Time
Rc 192.168.70.0/24		1		vlan1	

Below the table, there are pagination controls showing '1/1' and a 'Go' button. A 'Note' section at the bottom explains the codes: R - RIP, Rc - RIP connected, K - Kernel, C - Connected, S - Static, O - OSPF, A - Aggregate.

Figure 6-31 RIP Database

The following parameters can be configured in the **RIP Database** section:

Parameter	Description
Network Address	Enter the subnet prefix and the prefix length of the network(s) to be displayed here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

6.13 OSPF (Open Shortest Path First) [ZEQUO6700RE/6600RE]

6.13.1 OSPFv2

6.13.1.1 OSPFv2 Process Settings

This window is used to configure and display the OSPFv2 process settings.

Click **L3 Features > OSPF > OSPFv2 > OSPFv2 Process Settings** to view the following window:

The screenshot shows the 'OSPFv2 Process Settings' window. It features a 'Clear Process' button and an 'Apply' button. Below them, it states 'Total Entries: 1'. A table displays the OSPF process configuration:

OSPF State	Router ID	Default Metric	Distance Settings		Default Originate Info			ECMP	
			Type	Distance	State	Originate	Metric		
Enabled	192.168.70.0	10	Intra-area	20	Enabled	Always	20	30	

Below the table, there are 'Edit' and 'Show Detail' buttons. At the bottom, a pagination control shows '1/1' and a 'Go' button. A note at the bottom states: 'Note: Changing router ID or distance of one running OSPF process will cause it restart.'

Figure 6-32 OSPFv2 Process Settings

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

Click the **Edit** button to edit the settings of the specified entry.

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Edit** button to view the following window:

The screenshot shows the 'STP Global Settings' window. It contains several sections with configuration options and 'Apply' buttons:

- STP State:** Radio buttons for 'Disabled' (selected) and 'Enabled'.
- STP Mode:** A dropdown menu set to 'RSTP'.
- STP Priority:** A dropdown menu set to '32768'.
- STP Configuration:**
 - Bridge Max Age (6-40): 20 sec
 - Bridge Hello Time (1-2): 2 sec
 - Bridge Forward Time (4-30): 15 sec
 - TX Hold Count (1-10): 6 times
 - Max Hops (6-40): 20 times

Figure 6-33 OSPFv2 Process Settings (Edit)

The following parameters can be configured in the **OSPF Process Table** section:

Parameter	Description
OSPF State	Select to enable or disable the OSPFv2 state on the specified VRF instance.
Router ID	Enter the router ID in the IPv4 address format here. The router ID is a 32-bit number assigned to each router running the OSPF protocol. This number uniquely identifies the router within an AS. Each router has a unique router ID. If the router is already active when this command is configured, the new router ID will not take effect immediately. It is applied on the next reload or manual restart of the OSPF process.
Default Metric	Enter the default metric value used here. The range is from 1 to 16777214.
Type	Select the distance setting type here. Options to choose from are: <ul style="list-style-type: none"> • Inter-Area - Specifies the distance for OSPF inter-area routes. • Intra-Area - Specifies the distance for OSPF intra-area routes. • External-1 - Specifies the distance for OSPF external type-5 and type-7 routes with a type-1 metric. • External-2 - Specifies the distance for OSPF external type-5 and type-7 routes with a type-2 metric.
Distance	Enter the administrative distance value here. The range is from 1 to 255.
State	Select to enable or disable the Default Originate Information state here. This feature is used to generate a default external route (type-5 LA) network 0.0.0.0 to the AS.
Originate	Select the Originate option here. Options to choose from are Always and None . Selecting the Always option specifies to always generate the default route regardless of existence of a default route in the redistributed routes.
Metric	Enter the cost value associated with the generated default route here. If not specified, the default metric cost is 1. The range is from 1 to 65535.
ECMP	Enter the ECMP value for this process here. The range is from 1 to 32.

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

Click the **Show Detail** button to view the following window:

OSPF Global Settings Information	
OSPF Global Settings Information	
Detail Information	
OSPF State	Enabled
Router ID	192.168.70.0
Default Metric	10
Default Originate Information State	Enabled
Default Originate Information Always	Always
Default Originate Information Metric	20
Intra-Area Distance	20
Inter-Area Distance	90
External-1 Distance	110
External-2 Distance	115
Conforms to RFC2328, and RFC1583 Compatibility flag is disabled	
Process Uptime	00Day00:00:33
This Router is an ABR	No
This Router is an ASBR	Yes
SPF Schedule Hold Time Between Two SPF's (sec)	3
Number of External LSA	1
External LSA Checksum Sum	0xb35b
Number of LSA Originated	1
Number of LSA Received	0
Number of Current LSA	1
LSDB Database Overflow Limit	49152
Number of Areas Attached to This Router	1
Equal Cost Multi-Path (ECMP)	30

OK

Figure 6-34 OSPFv2 Process Settings (Show Detail)

Click the **OK** button to return to the previous window.

6.13.1.2 OSPFv2 Passive Interface Settings

This window is used to configure and display the OSPFv2 passive interface settings.

Click **L3 Features > OSPF > OSPFv2 > OSPFv2 Passive Interface Settings** to view the following window:

OSPFv2 Passive Interface Settings

OSPF Passive Interface Settings

Interface Name ☒ Default

Total Entries: 2

Passive Interface	Delete
vlan1	<input type="button" value="Delete"/>
loopback1	<input type="button" value="Delete"/>

1/1

Figure 6-35 OSPFv2 Passive Interface Settings

The following parameters can be configured in the **OSPF Passive Interface Settings** section:

Parameter	Description
Interface Name	Enter the interface name that will be used here. This name can be up to 12 characters long. Select the Default option to use the default interface here.

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.

6.13.1.3 OSPFv2 Area Settings

This window is used to configure and display the OSPFv2 area settings.

Click **L3 Features > OSPF > OSPFv2 > OSPFv2 Area Settings** to view the following window:

OSPFv2 Area Settings

OSPF Area Settings

OSPF Area ID: ☐ ☐ 0-4294967295

☒ Range ☐ NSSA ☐ Stub

Area Range IP: Area Range Mask:

Advertise:

Apply Delete

OSPF Area Table

Total Entries: 3

Area ID	Area Type	Metric	Area Range	Summary	Advertise	
0.0.0.0	Normal	-	-	-	-	Delete
10.1.1.2	NSSA	1	-	Yes	-	Delete
10.1.1.3	Normal	-	192.168.20.0/255.255.255.0	-	Advertise	Delete

1/1 < < 1 > > Go

Figure 6-36 OSPFv2 Area Settings (Range)

Select the **NSSA** or **Stub** options to view the following window:

OSPFv2 Area Settings

OSPF Area Settings

OSPF Area ID: ☐ ☐ 0-4294967295

☐ Range ☒ NSSA ☐ Stub

Default Cost (0-65535): ☒ Default ☐ No-Summary

Apply Delete

OSPF Area Table

Total Entries: 3

Area ID	Area Type	Metric	Area Range	Summary	Advertise	
0.0.0.0	Normal	-	-	-	-	Delete
10.1.1.2	NSSA	1	-	Yes	-	Delete
10.1.1.3	Normal	-	192.168.20.0/255.255.255.0	-	Advertise	Delete

1/1 < < 1 > > Go

Figure 6-37 OSPFv2 Area Settings (NSSA/Stub)

The following parameters can be configured in the **OSPF Area Settings** section:

Parameter	Description
OSPF Area ID	Enter the OSPFv2 area ID here. The area will be created on an interface if the subnet configured on the interface falls within the network range specified here.
Range	Select this option to summarize OSPF routes at an Area Border Router (ABR).
NSSA	Select this option to assign the OSPF area as a Not-So-Stubby Area (NSSA) area.

Parameter	Description
Stub	Select this option to specify an OSPF area as a Stub Area.
Area Range IP	After selecting the Range option, enter the OSPF area range IP address here.
Area Range Mask	After selecting the Range option, enter the OSPF area range subnet mask here.
Advertise	After selecting the Range option, select the advertise option here. Options to choose from are: <ul style="list-style-type: none">• Advertise - Specifies to advertise a Type-3 summary Link-State Advertisement (LSA) for the specified range of addresses.• No-Advertise - Specifies to suppress the advertising of Type-3 summary LSAs. Component routes are still hidden behind it.
Default Cost	After selecting the NSSA or Stub option, enter the default cost value here. The cost reflects the overhead for sending packets across the interface. It is advertised as the link cost in the router link advertisement. The range is from 0 to 65535. Select the Default option to use the default value.
No Summary	Select this option to disable the injection of summary routes into this area.

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.

6.13.1.4 OSPFv2 Interface Settings

This window is used to configure and display the OSPFv2 interface settings.

Click **L3 Features > OSPF > OSPFv2 > OSPFv2 Interface Settings** to view the following window:

Figure 6-38 OSPFv2 Interface Settings

The following parameters can be configured in the **OSPF Interface Settings** section:

Parameter	Description
Area ID	Select and enter the OSPFv2 area ID here.
Network IP Address	Enter the network IPv4 address here.
Network Mask	Enter the network IPv4 subnet mask here.

Click the **Apply** button to add a new entry.

The following parameters can be configured in the **OSPF Interface Table** section:

Parameter	Description
Interface Name	Enter the name of the interface to be displayed here.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Show Detail** button to display detailed information related to the 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.

Click the **Show Detail** button to view the following window:

OSPF Interface Settings	
Interface	vian1
Cost (1-65535)	<input type="text"/> <input type="checkbox"/> Default
Hello Interval (1-65535)	<input type="text"/> sec <input type="checkbox"/> Default
Dead Interval (1-65535)	<input type="text"/> sec <input type="checkbox"/> Default
Priority (0-255)	<input type="text"/> <input type="checkbox"/> Default
Authentication	None <input type="checkbox"/> Default
<input type="button" value="Apply"/>	

OSPF Interface Information	
Interface	vian1
Link Status	Up
Network IP Address	192.168.70.123
Network Mask	255.255.255.0
Area ID	10.1.1.1
Router ID	192.168.70.0
Network Type	Broadcast
Cost	1
Transmit Delay (sec)	1
State	Wait
Priority	1
Designated Router (ID)	0.0.0.0
Designated Router Interface Address	0.0.0.0
Backup Designated Router (ID)	0.0.0.0
Backup Designated Router Interface Address	0.0.0.0
Hello Interval Configured (sec)	10
Dead Interval Configured (sec)	40
Retransmit Interval (sec)	5
Current Authentication Type	None

Figure 6-39 OSPFv2 Interface Settings (Show Detail)

The following parameters can be configured in the **OSPF Interface Settings** section:

Parameter	Description
Cost	Enter the cost value here. The range is from 1 to 65535. The interface cost reflects the overhead for sending the packet across the interface. This cost is advertised as the link cost in the router link advertisement. The cost is inversely proportional to the speed of an interface. The cost can be either manually assigned or be automatically determined. By default, the cost of an interface is calculated based on reference bandwidth. The cost corresponds to a reference bandwidth of 1. Select the Default option to use the default value which is 1.
Hello Interval	Enter the Hello Interval time value here. The range is from 1 to 65535 seconds. The Hello Interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter Hello Interval ensures faster detection of topological changes but generates more routing traffic and might cause routing instability. Select the Default option to use the default value which is 10 seconds.

Parameter	Description
Dead Interval	Enter the Dead Interval time value here. The range is from 1 to 65535 seconds. The Dead Interval is the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down. This value is advertised in the router's hello packets. It must be the same for all routers on a specific network. Specifying a smaller Dead Interval ensures faster detection of topology changes, but might cause routing instability. Select the Default option to use the default value which is 40 seconds.
Priority	Enter the priority value here. The range is from 0 to 255. The OSPF router will determine a Designated Router (DR) for the multi-access network. This sets the priority used to determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority will be elected the DR. If the routers have the same priority, the router with the higher router ID takes precedence. Only routers with non-zero router priority values are eligible to become the DR or Backup Designated Router (BDR). Select the Default option to use the default value which is 1.
Authentication	Select the authentication type that will be used here. Options to choose from are None , Simple Password , and MD5 .
Password	After selecting Simple Password as the Authentication , enter the simple password here. This password can be up to 8 characters long. The syntax is general string that does not allow spaces. This creates a password (key) that is inserted into the OSPF header when the router originates routing protocol packets. Assign a separate password to each network for different interfaces. Routers on the same network must use the same password to be able to exchange OSPF routing data. Configure the routers in the same routing domain with the same password.
MD5 Key ID	After selecting MD5 as the Authentication , enter the MD5 key ID for the password here. The range is from 1 to 255.

Parameter	Description
MD5	<p>After selecting MD5 as the Authentication, enter the MD5 key here. This key must be 16 characters long. The syntax is an alphanumeric string that does not allow spaces.</p> <p>In the MD5 mode, the OSPF message sender will compute a message digest based on the message digest key for the TX message. The message digest and the key ID will be encoded in the packet. The receiver of the packet will verify the digest in the message against the digest computed based on the locally defined message digest key corresponding to the same key ID. The same key ID on the neighboring router should be defined with the same key string.</p> <p>All the neighboring routers on the same interface must use the same key to exchange the OSPF packet with each other. Normally, all neighboring routers on the interface use the same key.</p> <p>With the MD5 digest mode, the user can roll over to a new key without disrupting the current message exchange using the new key. Supposing that a router is currently using an old key to exchange OSPF packets with the neighbor router, as the user configures a new key, the router will start the roll over process by sending duplicated packets for both of the old and the new key. The router will stop sending duplicated packets until it finds that all routers on the network have learned the new key. After the rollover process completed, the user should delete the old key to prevent the router from communicating with the router using the old key.</p>

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

6.13.1.5 OSPFv2 Redistribute Settings

This window is used to configure and display the OSPFv2 redistribution settings.

Click **L3 Features > OSPF > OSPFv2 > OSPFv2 Redistribute Settings** to view the following window:

Figure 6-40 OSPFv2 Redistribute Settings

The following parameters can be configured in the **OSPF Redistribute Settings** section:

Parameter	Description
Protocol	Select the source protocol that will be redistributed here. Options to choose from are Connected , Static , and RIP . For routing protocols like Open Shortest Path First (OSPF), these routes will be redistributed as external to the autonomous system.
Metric Type	Select the metric type here. Options to choose from are External Type-1 and External Type-2 . This specifies the external link type of the route being redistributed into the OSPF routing domain. If a metric type is not specified, the Switch will adopt a Type-2 external route.
Metric	Enter the metric value for the redistributed routes here. The range is from 1 to 16777214.

Click the **Apply** button to add a new entry.

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

6.13.1.6 OSPFv2 Virtual Link Settings

This window is used to configure and display the OSPFv2 virtual link settings.

Click **L3 Features > OSPF > OSPFv2 > OSPFv2 Virtual Link Settings** to view the following window:

Figure 6-41 OSPFv2 Virtual Link Settings

The following parameters can be configured in the **OSPF Virtual Link** section:

Parameter	Description
Area ID	Enter the OSPFv2 area ID here. This area will be used to establish the virtual link. It can be specified as either a decimal value or as an IPv4 address.
Router ID	Enter the router ID of the virtual link neighbor here.
Hello Interval	Enter the hello packet interval that the router sends on the virtual link here. The range is from 1 and 65535 seconds. Select the Default option to use the default value, which is 10 seconds.
Dead Interval	Enter the Dead Interval time after which a neighbor is regarded as offline if no hello packets are received within that time frame here. The range is from 1 and 65535 seconds. Select the Default option to use the default value, which is 40 seconds.
Authentication	Select the authentication type used here. Options to choose from are None , Simple Password , and MD5 . If the authentication type is not specified for the virtual link, the 'password' authentication type for the area will be used.
Password	After selecting Simple Password as the Authentication , enter the password to be used here. This password can be up to 8 characters long.

Parameter	Description
MD5 Key ID	After selecting MD5 as the Authentication , enter the MD5 authentication key ID here. The range is from 1 to 255.
MD5 Key	After selecting MD5 as the Authentication , enter the MD5 authentication key here. This key can be up to 16 characters long.

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.

6.13.1.7 OSPFv2 LSDB Table

This window is used to display the OSPFv2 LSDB table and information.

Click **L3 Features > OSPF > OSPFv2 > OSPFv2 LSDB Table** to view the following window:

Link ID	ADV Router	Age	Sequence Number	Checksum	Count	LS Type
192.168.70.0	192.168.70.0	60	0x80000006	0x2d0f	1	Router-LSA
0.0.0.0	192.168.70.0	59	0x80000001	0x83da	-	AS-External-LSA
192.168.80.0	192.168.70.0	59	0x80000001	0x2e57	-	AS-External-LSA

Figure 6-42 OSPFv2 LSDB Table

The following parameters can be configured in the **OSPF LSDB Table** section:

Parameter	Description
LS Type	Select the LS type of information that will be displayed here. Options to choose from are All , Router , Network , Summary , ASBR Summary , External , Stub , and NSSA External .
Link State	Select the link-state information that will be displayed here. Options to choose from are: <ul style="list-style-type: none"> All - Specifies to display all OSPFv2 link-state information. Link State ID - Specifies to display information associated with the link-state ID. Enter the link state ID in the space provided here. Self Originate - Specifies to display LSAs generated by the local router. Adv Router - Specifies to display all of the LSAs generated by the advertising router. Enter the advertising router ID in the space provided here.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to view the following window:

The image shows a software window titled "OSPF LSA Detail Information". It contains two sections: "OSPF LSA Detail Information" and "Detail Information".

OSPF LSA Detail Information	
Area ID	10.1.1.1
LS Age	76
Options	0x2 (* + + + E +)
Flags	0x2
This Router is an ABR	No
This Router is an ASBR	Yes
This Router is a Virtual Link Endpoint	No
LS Type	Router-LSA
Link State ID	192.168.70.0
Advertising Router	192.168.70.0
LS Seq. Number	0x80000006
Checksum	0x2d0f
Length	36

Back

Detail Information	
Number of Links	1
Link Connected to Stub Network	
(Link ID) Network/Subnet Number	192.168.70.0
(Link Data) Network Mask	255.255.255.0
Number of TOS Metrics	0
TOS 0 Metric	1

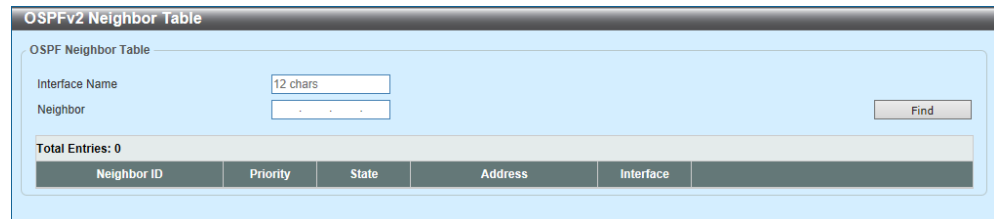
Figure 6-43 OSPFv2 LSDB Table (Show Detail)

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

6.13.1.8 OSPFv2 Neighbor Table

This window is used to display the OSPFv2 neighbor table.

Click **L3 Features > OSPF > OSPFv2 > OSPFv2 Neighbor Table** to view the following window:



Neighbor ID	Priority	State	Address	Interface
-------------	----------	-------	---------	-----------

Figure 6-44 OSPFv2 Neighbor Table

The following parameters can be configured in the **OSPF Neighbor Table** section:

Parameter	Description
Interface Name	Enter the name of the interface that will be used in the results here.
Neighbor	Enter the neighbor ID here.

Click the **Find** button to find and display entries based on the search criteria specified.

6.13.1.9 OSPFv2 Host Route Settings

This window is used to configure and display the OSPFv2 host route settings. The switch will advertise specific host routes as router LSAs for a stub link.

Click **L3 Features > OSPF > OSPFv2 > OSPFv2 Host Route Settings** to view the following window:

Figure 6-45 OSPFv2 Host Route Settings

The following parameters can be configured in the **OSPF v2 Host Route Settings** section:

Parameter	Description
Area ID	Enter the OSPF area ID here.
Host IP	Enter the host IPv4 address here.
Cost	Enter the cost value for the stub entry here. The range is from 0 to 65535. Select the Default option to use the default value, which is 1.

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.

6.13.2 OSPFv3

6.13.2.1 OSPFv3 Process Settings

This window is used to configure and display the OSPFv3 process settings.

Click **L3 Features > OSPF > OSPFv3 > OSPFv3 Process Settings** to view the following window:

OSPFv3 Process Settings

OSPFv3 Process Settings

Process ☒ Enabled ☐ Disabled Apply

OSPFv3 Process Table

Total Entries: 1

Router ID	Distance Settings		Auto Bandwidth	
	Type	Distance		
192.168.70.124	Intra-area	110	100	Edit Clear

1/1 < > 1 < > Go

Note: Changing router ID or distance of one running OSPF process will cause it restart.

Figure 6-46 OSPFv3 Process Settings

The following parameters can be configured in the **OSPFv3 Process Settings** section:

Parameter	Description
Process	Select to globally enable or disable OSPFv3 here.

Click the **Apply** button to add a new entry.

Click the **Edit** button to edit the settings of the specified entry.

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

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

Click the **Edit** button to view the following window:

OSPFv3 Process Settings

OSPFv3 Process Settings

Process ☒ Enabled ☐ Disabled Apply

OSPFv3 Process Table

Total Entries: 1

Router ID	Distance Settings		Auto Bandwidth	
	Type	Distance		
192.168.70.124	Intra-Area	110	100	Apply Clear

1/1 < > 1 < > Go

Note: Changing router ID or distance of one running OSPF process will cause it restart.

Figure 6-47 OSPFv3 Process Settings (Edit)

The following parameters can be configured in the **OSPF Process Table** section:

Parameter	Description
Router ID	Enter the router ID for the OSPF process here.
Type	Select the distance type here. Options to choose from are: <ul style="list-style-type: none"> • Intra-Area - Specifies the distance for OSPF intra-area routes. • Inter-Area - Specifies the distance for OSPF inter-area routes. • External - Specifies the distance for OSPF external routes.
Distance	Enter the distance value for the OSPF process here. The range is from 1 to 254. By default, this value is 110 for all OSPF routes.
Auto Bandwidth	Enter the auto-bandwidth value here. This feature is used to control the reference value IPv6 OSPF uses when calculating metrics for interfaces. The range is from 1 to 4294967.

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

Double-click on the entry in the table to view the following window:

OSPFv3 Global Settings Information	
OSPF State	Enabled
Router ID	192.168.70.124
Intra-Area Distance	110
Inter-Area Distance	110
External Distance	110
Auto Cost Reference Bandwidth	100
Process Uptime	00Day00:46:55
This Router is an ABR	No
This Router is an ASBR	No
SPF Schedule Hold Time Between Two SPF's (sec)	10
SPF Schedule Delay (sec)	5
Number of LSA Originated	0
Number of LSA Received	0
Number of Areas Attached to This Router	2

Figure 6-48 OSPFv3 Global Settings Information

Click the **OK** button to return to the previous window.

6.13.2.2 OSPFv3 Passive Interface Settings

This window is used to configure and display the OSPFv3 passive interface settings. If an interface is passive, the OSPF routing update packets are not sent or received through the specified interface.

Click **L3 Features > OSPF > OSPFv3 > OSPFv3 Passive Interface Settings** to view the following window:

Figure 6-49 OSPFv3 Passive Interface Settings

The following parameters can be configured in the **OSPFv3 Passive Interface Settings** section:

Parameter	Description
Interface Name	Enter the passive interface name here. This name can be up to 12 characters long. Select the Default option specify all the interfaces as passive interfaces.

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.

6.13.2.3 OSPFv3 Area Settings

This window is used to configure and display the OSPFv3 area settings.

Click **L3 Features > OSPF > OSPFv3 > OSPFv3 Area Settings** to view the following window:

OSPFv3 Area Settings

OSPF Area ID:

☒ Range ☐ Stub

Area Range IPv6 Prefix:

Advertise:

Apply

OSPFv3 Area Table

Total Entries: 2

Area ID	Area Type	Metric	Summary	
10.1.1.10	Normal	-	-	Delete
10.2.2.10	Stub	1	Yes	Delete

1/1 < > 1 Go

Figure 6-50 OSPFv3 Area Settings (Range)

Select the **Stub** option to view the following window:

OSPFv3 Area Settings

OSPF Area ID:

☐ Range ☒ Stub

Default Cost (0-65535): ☒ Default ☐ No-Summary

Apply

OSPFv3 Area Table

Total Entries: 2

Area ID	Area Type	Metric	Summary	
10.1.1.10	Normal	-	-	Delete
10.2.2.10	Stub	1	Yes	Delete

1/1 < > 1 Go

Figure 6-51 OSPFv3 Area Settings (Stub)

The following parameters can be configured in the **OSPFv3 Area Settings** section:

Parameter	Description
OSPF Area ID	Enter the OSPF area ID used here. It can be specified as an IPv4 address.
Range	Select this option to consolidate and summarize routes at an area boundary. This feature is used only with ABRs. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range.

Parameter	Description
Stub	Select this option to define an area as a Stub area.
Area Range IPv6 Prefix	After selecting the Range option, enter the OSPF area range IPv6 prefix and prefix length here.
Advertise	After selecting the Range option, select the advertise option here. Options to choose from are: <ul style="list-style-type: none"> • Advertise - Specifies to advertise and generate a Type-3 summary LSA for the specified address range. • No-Advertise - Specifies to set the status to Do-Not-Advertise for the specified address range. The Type-3 summary LSA is suppressed, and the component networks remain hidden from other networks.
Default Cost	After selecting the Stub option, enter the stub area metric value here. The range is from 0 to 65535. <ul style="list-style-type: none"> • Select the Default option use the default metric value for this area, which is 1. • Select the No-Summary option to prevent an ABR from sending summary LSAs into the stub area.

Click the **Apply** button to add a new entry.

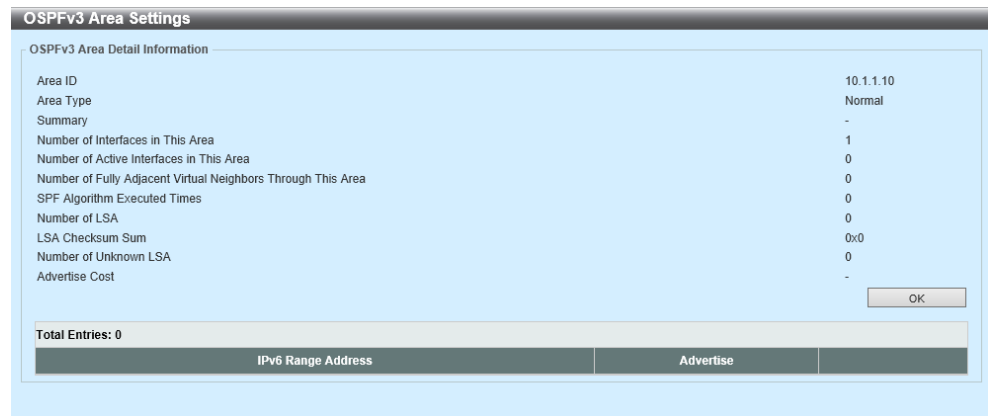
The following parameters can be configured in the **OSPFv3 Area Table** section:

Parameter	Description
Process ID	Enter the process ID of the OSPF area used here. The range is from 1 to 65535.

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.

Double-click on the **Normal** entry in the table to view the following window:



The screenshot shows the 'OSPFv3 Area Settings' window. It contains a table with the following data:

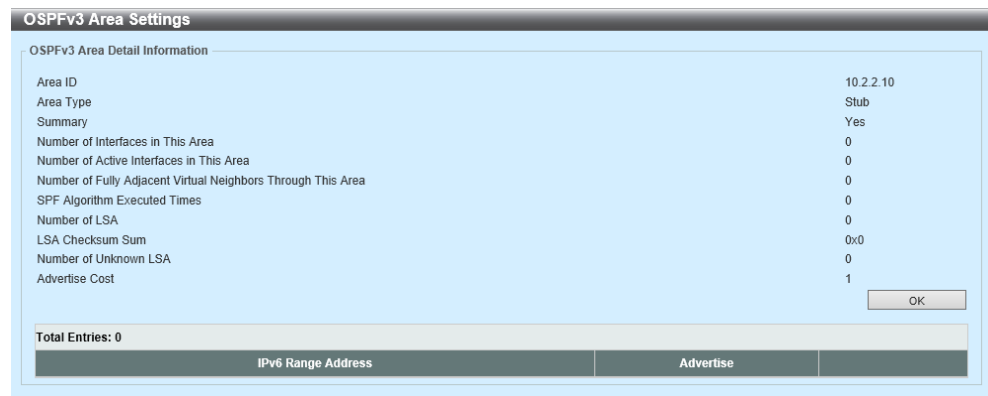
OSPFv3 Area Detail Information	
Area ID	10.1.1.10
Area Type	Normal
Summary	-
Number of Interfaces in This Area	1
Number of Active Interfaces in This Area	0
Number of Fully Adjacent Virtual Neighbors Through This Area	0
SPF Algorithm Executed Times	0
Number of LSA	0
LSA Checksum Sum	0x0
Number of Unknown LSA	0
Advertise Cost	-

At the bottom right of the table is an 'OK' button. Below the table, there is a section labeled 'Total Entries: 0' followed by a table with two columns: 'IPv6 Range Address' and 'Advertise'.

Figure 6-52 OSPFv3 Area Setting (Normal)

Click the **OK** button to return to the previous window.

Double-click on the **Stub** entry in the table to view the following window:



The screenshot shows the 'OSPFv3 Area Settings' window for a Stub area. It contains a table with the following data:

OSPFv3 Area Detail Information	
Area ID	10.2.2.10
Area Type	Stub
Summary	Yes
Number of Interfaces in This Area	0
Number of Active Interfaces in This Area	0
Number of Fully Adjacent Virtual Neighbors Through This Area	0
SPF Algorithm Executed Times	0
Number of LSA	0
LSA Checksum Sum	0x0
Number of Unknown LSA	0
Advertise Cost	1

At the bottom right of the table is an 'OK' button. Below the table, there is a section labeled 'Total Entries: 0' followed by a table with two columns: 'IPv6 Range Address' and 'Advertise'.

Figure 6-53 OSPFv3 Area Settings (Stub)

Click the **OK** button to return to the previous window.

6.13.2.4 OSPFv3 Interface Settings

This window is used to configure and display the OSPFv3 interface settings.

Click **L3 Features > OSPF > OSPFv3 > OSPFv3 Interface Settings** to view the following window:

Figure 6-54 OSPFv3 Interface Settings

The following parameters can be configured in the **OSPFv3 Interface Settings** section:

Parameter	Description
Instance ID	Enter the instance identifier here. The range is from 0 to 255. If not specified, the default is 0.
Area ID	Enter the identifier of the area here. It can be specified as an IPv4 address.
Interface Name	Enter the name of the VLAN interface here. This name can be up to 12 characters long.

Click the **Apply** button to add a new entry.

The following parameters can be configured in the **OSPFv3 Interface Table** section:

Parameter	Description
Process ID	Enter the ID for an IPv6 OSPF routing process here. The range is from 1 to 65535.
Interface Name	Enter the name of the interface here.

Click the **Find** button to find and display entries based on the search criteria specified.

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.

Double-click on the entry in the table to view the following window:

OSPFv3 Interface Information

OSPFv3 Interface Information

Interface: vian3

Cost (1-65535): ☐ Default

Hello Interval (1-65535): sec ☐ Default

Dead Interval (1-65535): sec ☐ Default

Priority (0-255): ☐ Default

Transmit Delay (1-65535): sec ☐ Default

Retransmit Interval (1-65535): sec ☐ Default

Apply

OSPFv3 Interface Information

Area ID	10.1.1.10
Instance ID	0
MTU	1500
Interface Name	vian3
Link State	down
Line Protocol State	down
Link Local Address	FE80::250:40FF:FE3C:7781/128
Interface ID	2
Router ID	192.168.70.124
Network Type	Broadcast
Cost	10
Transmit Delay (sec)	1
State	Down
Priority	1
This is Passive Interface	Yes
Designated Router (ID)	0.0.0.0
Designated Router Local Address	::
Backup Designated Router (ID)	0.0.0.0

Figure 6-55 OSPFv3 Interface Information

The following parameters can be configured in the **OSPFv3 Interface Information** section:

Parameter	Description
Cost	Enter cost value here. It is an integer value expressed as the link-state metric. The range is from 1 to 65535. Select the Default option to use the default value.
Hello Interval	Enter the Hello Interval value, between the hello packets that the router sends on an interface here. This value is advertised in the hello packets. The shorter the Hello Interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network. The range is from 1 to 65535 seconds. Select the Default option to use the default value, which is 10 seconds.
Dead Interval	Enter the Dead Interval value here, during which no packets are received and after which a neighbor is regarded as offline. The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network. The range is from 1 to 65535 seconds. Select the Default option to use the default value, which is 40 seconds.

Parameter	Description
Priority	<p>Enter the priority value of the router here. The range is from 0 to 255. Set the priority to help determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID takes precedence.</p> <p>Only routers with non-zero router priority values are eligible to become the designated or backup designated router. Configure router priority for multi-access networks (not point-to-point) only.</p> <p>Select the Default option to use the default value, which is 1.</p>
Transmit Delay	<p>Enter the Transmit Delay value here. The range is from 1 to 65535 seconds. Link-State Updates (LSUs) must have their ages incremented by the amount specified in the seconds argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.</p> <p>If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low speed links.</p> <p>Select the Default option to use the default value, which is 1 second.</p>
Retransmit Interval	<p>Enter the Retransmit Interval value here. The range is from 1 to 65535 seconds. After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. In case the router does not receive an acknowledgement during the set time (the Retransmit Interval value), it retransmits the LSA. Set the retransmission interval value conservatively to avoid unnecessary retransmission. The interval should be greater than the expected round-trip delay between two routers.</p> <p>Select the Default option to use the default value, which is 5 seconds.</p>

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

6.13.2.5 OSPFv3 Virtual link Settings

This window is used to configure and display the OSPFv3 virtual link settings.

Click **L3 Features > OSPF > OSPFv3 > OSPFv3 Virtual link Settings** to view the following window:

Figure 6-56 OSPFv3 Virtual link Settings

The following parameters can be configured in the **OSPFv3 Virtual Link** section:

Parameter	Description
Instance ID	Select and enter the instance ID here. The range is from 0 to 255.
Area ID	Enter the OSPF area ID here. It can be specified as an IPv4 address.
Router ID	Enter the router ID here associated with the virtual link neighbor.
Hello Interval	Enter the Hello Interval value between the hello packets that the router sends on an interface here. The range is from 1 to 65535 seconds. Select the Default option to use the default value, which is 10 seconds.
Dead Interval	Enter the Dead Interval value, during which no packets are received and after which a neighbor is regarded as offline, here. The range is from 1 to 65535 seconds. Select the Default option to use the default value, which is 40 seconds.
Transmit Delay	Enter the transmit delay value here that the router uses to wait before it transmits a packet. The range is from 1 to 65535 seconds. Select the Default option to use the default value, which is 1 second.

Parameter	Description
Retransmit Interval	Enter the retransmit interval value here that the router uses to wait before it retransmits a packet. The range is from 1 to 65535 seconds. Select the Default option to use the default value, which is 5 seconds.

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.

Double-click on the entry in the table to view the following window:

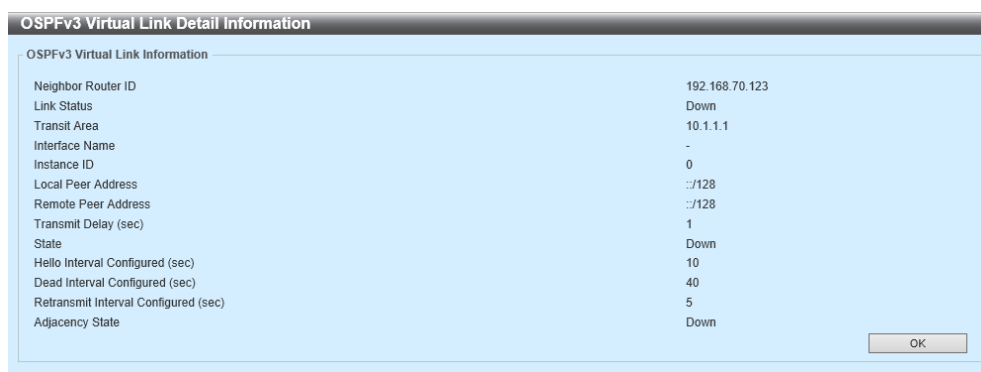


Figure 6-57 OSPFv3 Virtual link Detail Information

Click the **OK** button to return to the previous window.

6.13.2.6 OSPFv3 LSDB Table

This window is used to display the OSPFv3 LSDB table and information.

Click **L3 Features > OSPF > OSPFv3 > OSPFv3 LSDB Table** to view the following window:

Figure 6-58 OSPFv3 LSDB Table

The following parameters can be configured in the **OSPFv3 LSDB Table** section:

Parameter	Description
LS Type	Select the LS display type here. Options to choose from are: <ul style="list-style-type: none"> • All - Specifies to display all types of LSDB information. • Router-LSA - Specifies to display information only about the router LSAs. • Network-LSA - Specifies to display information only about the network LSAs. • Prefix - Specifies to display information on the intra-area-prefix LSAs. • Link-LSA - Specifies to display information about the link LSAs. • Inter-Area Prefix-LSA - Specifies to display information only about LSAs based on inter-area prefix LSAs. • Inter-Area Router-LSA - Specifies to display information only about LSAs based on inter-area router LSAs. • AS-External-LSA - Specifies to display information only about the external LSAs.
Area ID	Select the area ID option here. Options to choose from are All and Area ID . To display all the LSAs of the specified area, select the Area ID option and enter the OSPF area ID in the space provided. It can be specified as an IPv4 address.

Parameter	Description
Link State	<p>Select the link state option here. Options to choose from are:</p> <ul style="list-style-type: none"> • All - Specifies to display all the LSAs. • Self Originate - Specifies to display only self-originated LSAs (from the local router). • Adv Router - Specifies to display all the LSAs of the advertising router. Enter the router ID in the space provided. The router ID can be specified as an IPv4 address.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Show Detail** button to display detailed information related to the entry.

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

Click the **Show Detail** button to view the following window:

The screenshot shows a window titled "OSPFv3 LSA Detail Information". It contains two main sections: "OSPFv3 LSA Detail Information" and "Detail Information".

OSPFv3 LSA Detail Information

Process ID	1
Advertising Router ID	192.168.80.123
Area ID	0.0.0.0
LS Age	198
LS Type	Link-LSA
Link State ID	0.0.0.1
LS Seq. Number	0x80000001
Checksum	0x5fd5
Length	56

Back

Detail Information

Priority	1
Options	0x13 (-IRI- E V6)
Link-Local Address	FE80::250:40FF:FE3C:7781
Number of Prefixes	1
Prefix	2017::/64
Prefix Options	0 (- + +)

Figure 6-59 OSPFv3 LSDB Table (Show Detail)

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

6.13.2.7 OSPFv3 Neighbor Table

This window is used to display the OSPFv3 neighbor table and information.

Click **L3 Features > OSPF > OSPFv3 > OSPFv3 Neighbor Table** to view the following window:

OSPFv3 Neighbor Table

OSPFv3 Neighbor Table

Interface VLAN (1-4094)

Neighbor

Find

Total Entries: 0

Neighbor ID	Priority	State	Link Local Address	Interface	Instance ID
-------------	----------	-------	--------------------	-----------	-------------

Figure 6-60 OSPFv3 Neighbor Table

The following parameters can be configured in the **OSPFv3 Neighbor Table** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Neighbor	Enter the OSPF neighbor ID here. It can be specified as an IPv4 address.

Click the **Find** button to find and display entries based on the search criteria specified.

6.13.2.8 OSPFv3 Border Router Table

This window is used to display the OSPFv3 border router table and information.

Click **L3 Features > OSPF > OSPFv3 > OSPFv3 Border Router Table** to view the following window:



OSPFv3 Border Router Table						
OSPFv3 Border Router Table						
Total Entries: 0						
Route Type	Router ID	Metric	Next Hop	Interface	Router State	Area ID

Figure 6-61 OSPFv3 Border Router Table

6.14 IP Multicast Routing Protocol

6.14.1 IGMP[ZEQUO6700RE/6600RE]

6.14.1.1 IGMP Interface Settings

The window is used to configure and display the IGMP interface settings.

Click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Interface Settings** to view the following window:

Interface	Version	IP Address / Netmask	State	Querier	Query Interval	Query Max...	Robustness Variable	Last Member...	Subscriber Source IP...
vlan1	3	192.168.70.123/24	Disabled	0.0.0.0	125	10	2	1	Enabled

Figure 6-62 IGMP Interface Settings

The following parameters can be configured in the **IGMP Interface Settings** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.

Click the **Find** button to find and display entries based on the search criteria specified.

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

Click the **Edit** button to edit the settings of the specified entry.

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

Click the **Edit** button to view the following window:

IGMP Interface Settings

IGMP Interface Settings

Interface: vian1

IP Address: 192.168.70.123/24

Querier: 0.0.0.0

Version: 3 ☐ Default

State: Disabled

Query Interval (1-31744): 125 sec ☐ Default

Query Max Response Time (1-25): 10 sec ☐ Default

Robustness Variable (1-7): 2 ☐ Default

Last Member Query Interval (1-25): 1 sec ☐ Default

Subscriber Source IP Check: Enabled

Back Apply

Figure 6-63 IGMP Interface Settings (Edit)

The following parameters can be configured in the **IGMP Interface Settings** section:

Parameter	Description
Version	Select the IGMP version number here. The range is from 1 to 3. Select the Default option to use the default version which is 3.
State	Select to enable or disable the IGMP state on this interface here.
Query Interval	Enter the query interval value here. The range is from 1 to 31744 seconds. The IGMP querier sends IGMP query messages at the interval specified here to discover the receivers attached to the interface interested in joining the multicast group. Hosts respond to the query with IGMP report messages to indicate the multicast group they are interested in joining. Select the Default option to use the default value.
Query Max Responses Time	Enter the maximum query response time value here. The range is from 1 to 25 seconds. This configures the period of time which the group member can respond to an IGMP query message before the router removes the membership. The group membership lifetime is equal to the query interval times the robustness plus the maximum response time. Select the Default option to use the default value.
Robustness Variable	Enter the robustness variable value here. The range is from 1 to 7. The robustness variable provides fine tuning to allow for expected packet loss on an interface. Select the Default option to use the default value.

Parameter	Description
Last Member Query Interval	Enter the Last Member Query Interval value here. The range is from 1 to 25 seconds. When the router receives a leave message from a receiver to leave a group or a channel, the router will send the Group Specific Query or Group-Source Specific Query message to the receiver interface. The IGMP Last Member Query Interval will be advertised in the query message and conveyed to the receiver. This configures the period that the router will send the next group-specific query or group-source specific query message if there is no report from receiver for the specific group or specific channel. The router will retry for the last member query count. If no report messages are received after the retry count, the interface will remove the membership from the specific group or specific channel. Select the Default option to use the default value.
Subscriber Source IP Check	Select to enable or disable the subscriber source IP check feature here. By default, the IGMP report or leave messages received by the interface will be checked to determine whether its source IP is in the same network as the interface. If they are not in the same network, the message information won't be learned by the IGMP protocol.

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

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

6.14.1.2 IGMP Static Group Settings

This window is used to configure and display the IGMP static group settings.

Click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Static Group Settings** to view the following window:

Figure 6-64 IGMP Static Group Settings

The following parameters can be configured in the **IGMP Static Group Table** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Group	Enter the IP multicast group address here.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.1.3 IGMP Dynamic Group Table

This window is used to display the IGMP dynamic group table and information.

Click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Dynamic Group Table** to view the following window:

Figure 6-65 IGMP Dynamic Group Table

The following parameters can be configured in the **IGMP Dynamic Group Table** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Group	Enter the IP multicast group address here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.2 MLD[ZEQUO6700RE/6600RE]

6.14.2.1 MLD Interface Settings

This window is used to configure and display the MLD interface settings.

Click **L3 Features > IP Multicast Routing Protocol > MLD > MLD Interface Settings** to view the following window:

The screenshot shows the 'MLD Interface Settings' window. At the top, there is a search bar for 'Interface VLAN (1-4094)' with 'Find' and 'Show All' buttons. Below this, a table displays the configuration for 'vlan1'. The table has columns for Interface, Version, IPv6 Address / Netmask, State, Querier, Query Interval, Query Max Response Time, Robustness Variable, and Last Listener Query Interval. The entry for 'vlan1' shows Version 2, IPv6 Address FE80::250:40F..., State Disabled, Querier ::, Query Interval 125, Query Max Response Time 10, Robustness Variable 2, and Last Listener Query Interval 1. There is an 'Edit' button next to the entry. At the bottom right, there are pagination controls showing '1/1' and a 'Go' button.

Interface	Version	IPv6 Address / Netmask	State	Querier	Query Interval	Query Max Response Time	Robustness Variable	Last Listener Query Interval
vlan1	2	FE80::250:40F...	Disabled	::	125	10	2	1

Figure 6-66 MLD Interface Settings

The following parameters can be configured in the **MLD Interface Settings** section:

Parameter	Description
Interface VLAN	Enter the associated VLAN ID of the interface here. The range is from 1 to 4094.

Click the **Find** button to find and display entries based on the search criteria specified.

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

Click the **Edit** button to edit the settings of the specified entry.

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

Click the **Edit** button to view the following window:

The screenshot shows the 'MLD Interface Settings (Edit)' window. It contains a list of configuration parameters for 'vlan1'. The parameters and their values are: Interface (vlan1), IPv6 Address (FE80::250:40FF:FE3C:7781/128), Querier (::), Version (2), MLD State (Disabled), Query Interval (1-31744) (125 sec), Query Max Response Time (1-25) (10 sec), Robustness Variable (1-7) (2), and Last Listener Query Interval (1-25) (1 sec). Each value is in a text box, and there are checkboxes for 'Default' next to Version, Query Interval, Query Max Response Time, Robustness Variable, and Last Listener Query Interval. At the bottom right, there are 'Apply' and 'Back' buttons.

Figure 6-67 MLD Interface Settings (Edit)

The following parameters can be configured in the **MLD Interface Settings** section:

Parameter	Description
Version	Select the MLD version that will be used on the interface here. Options to choose from are 1 and 2. Select the Default option to use the default version, which is MLDv2.
MLD State	Select to enable or disable the MLD feature on this interface here.
Query Interval	Enter the query interval here. This specifies the frequency at which the designated router sends MLD general-query messages. On receiving the general query, the MLD listener needs to respond the report packet to claim that it is interested in the specified multicast group. The range is from 1 to 31744 seconds. Select the Default option to use the default value, which is 125 seconds.
Query Max Response Time	Enter the maximum response time of the query here. This specifies the maximum response time advertised in MLD queries. The range is from 1 to 25 seconds. Select the Default option to use the default value, which is 10 seconds.
Robustness Variable	Enter the robustness variable value here. The robustness variable provides fine-tuning to allow for expected packet loss on an interface. The range is from 1 to 7. Select the Default option to use the default value, which is 2.
Last Listener Query Interval	Enter the interval for the amount of time between group-specific or group-source-specific queries here. When an MLD querier receives a packet to leave the group or channel, it will send a group-specific query or group-source-specific query. The leave timer starts once the MLD querier receives the packet on an interface. If the interface does not receive the report packet before the leave timer expires, then the interface's membership will be removed from the group or channel that it is leaving. The value of the leave timer is the value of the Last Listener Query Interval times the Last Listener Query Count. The range is from 1 to 25 seconds. Select the Default option to use the default value, which is 1 seconds.

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

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

6.14.2.2 MLD Group Table

This window is used to display the MLD group table and information.

Click **L3 Features > IP Multicast Routing Protocol > MLD > MLD Group Table** to view the following window:

MLD Group Table

☒ Interface VLAN (1-4094) ☐ Group

Total Entries: 0

Interface	Group Address	Up Time	Expire Time
-----------	---------------	---------	-------------

Figure 6-68 MLD Group Table

The following parameters can be configured in the **MLD Group Table** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Group	Enter the group IPv6 address here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.3 IGMP Proxy

6.14.3.1 IGMP Proxy Settings

This window is used to configure and display the IGMP proxy settings.

Click **L3 Features > IP Multicast Routing Protocol > IGMP Proxy > IGMP Proxy Settings** to view the following window:

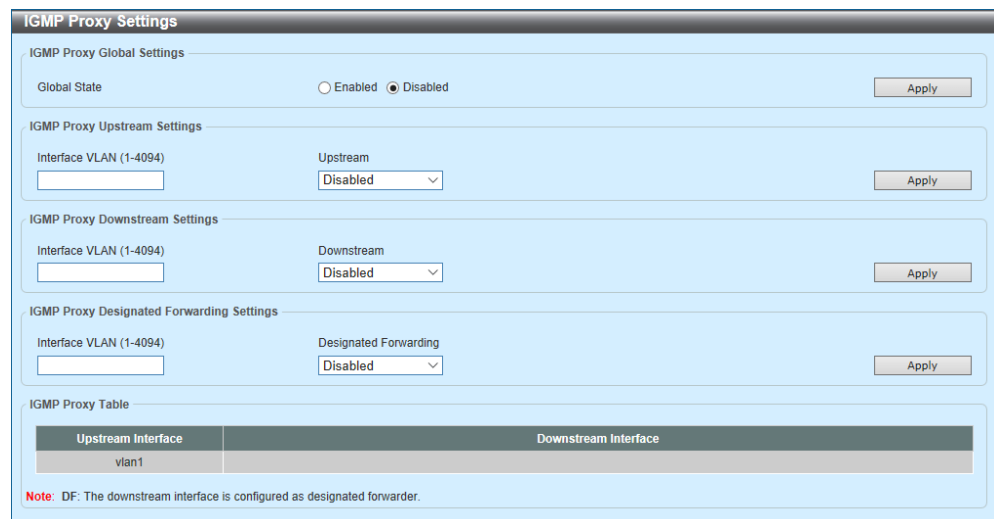


Figure 6-69 IGMP Proxy Settings

The following parameters can be configured in the **IGMP Proxy Global Settings** section:

Parameter	Description
Global State	Select to globally enable or disable the IGMP proxy feature here.

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

The following parameters can be configured in the **IGMP Proxy Upstream Settings** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Upstream	Select to enable or disable the interface as the upstream IGMP proxy here.

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

The following parameters can be configured in the IGMP Proxy Downstream Settings section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Downstream	Select to enable or disable the interface as the downstream in IGMP proxy here.

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

The following parameters can be configured in the **IGMP Proxy Designated Forwarding Settings** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Designated Forwarding	Select to enable or disable designated forwarding on a non-querier IGMP proxy downstream interface here. To avoid local loops and redundant traffic for links that are considered downstream links by multiple IGMP-based forwarders, IGMP proxies use the IGMP querier election to elect a single forwarder on a LAN. Use this option to make a non-querier device a forwarder. The feature does not take effect if the interface is not set as the downstream interface or set as the upstream interface.

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

6.14.3.2 IGMP Proxy Group Table

This window is used to display the IGMP proxy group table and information.

Click **L3 Features > IP Multicast Routing Protocol > IGMP Proxy > IGMP Proxy Group Table** to view the following window:

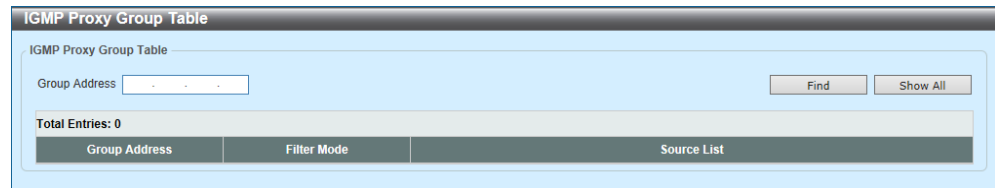


Figure 6-70 IGMP Proxy Group Table

The following parameters can be configured in the **IGMP Proxy Group Table** section:

Parameter	Description
Group Address	Enter the IPv4 group multicast address here.

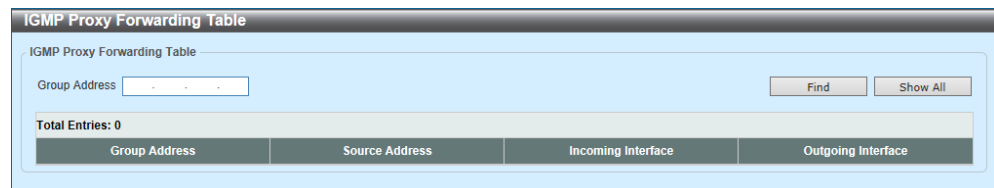
Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.3.3 IGMP Proxy Forwarding Table

This window is used to display the IGMP proxy forwarding table and information.

Click **L3 Features > IP Multicast Routing Protocol > IGMP Proxy > IGMP Proxy Forwarding Table** to view the following window:



Group Address	Source Address	Incoming Interface	Outgoing Interface
---------------	----------------	--------------------	--------------------

Figure 6-71 IGMP Proxy Forwarding Table

The following parameters can be configured in the **IGMP Proxy Forwarding Table** section:

Parameter	Description
Group Address	Enter the IPv4 group multicast address here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.4 MLD Proxy

6.14.4.1 MLD Proxy Settings

This window is used to configure and display the MLD proxy settings.

Click **L3 Features > IP Multicast Routing Protocol > MLD Proxy > MLD Proxy Settings** to view the following window:

Figure 6-72 MLD Proxy Settings

The following parameters can be configured in the **MLD Proxy Global Settings** section:

Parameter	Description
Global State	Select to globally enable or disable the MLD proxy feature here.

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

The following parameters can be configured in the MLD Proxy Upstream Settings section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Upstream	Select to enable or disable the interface as the upstream MLD proxy here. This feature only takes effect if the interface has an IPv6 address configured. Only one upstream interface can exist on a MLD proxy device.

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

The following parameters can be configured in the **MLD Proxy Downstream Settings** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Downstream	Select to enable or disable the interface as the downstream MLD proxy here. This feature only takes effect when the interface has an IPv6 address configured. Multiple downstream interfaces can be configured on an MLD proxy device.

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

The following parameters can be configured in the **MLD Proxy Designated Forwarding Settings** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094.
Designated Forwarding	Select to enable or disable designated forwarding on a non-querier MLD proxy downstream interface here. To avoid local loops and redundant traffic for links that are considered downstream links by multiple MLD-based forwarders, MLD proxies use the MLD querier election to elect a single forwarder on a LAN. Administrators can use this command to make a non-querier device a forwarder. This feature does not take effect if the interface is not set as the downstream interface or set as upstream interface.

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

6.14.4.2 MLD Proxy Group Table

This window is used to display the MLD proxy group table and information.

Click **L3 Features > IP Multicast Routing Protocol > MLD Proxy > MLD Proxy Group Table** to view the following window:

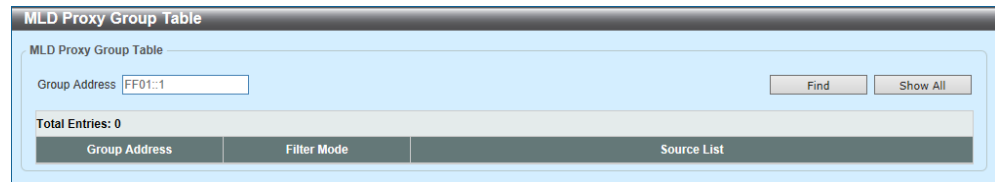


Figure 6-73 MLD Proxy Group Table

The following parameters can be configured in the **MLD Proxy Group Table** section:

Parameter	Description
Group Address	Enter the IPv6 group multicast address here.

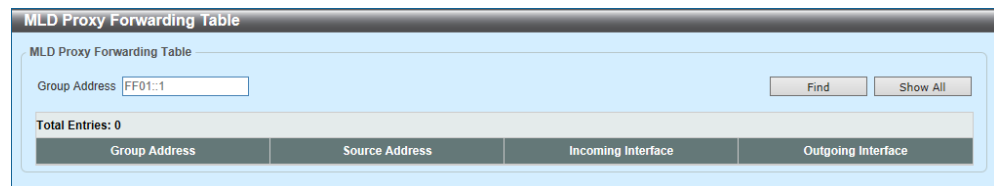
Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.4.3 MLD Proxy Forwarding Table

This window is used to display the MLD proxy forwarding table and information.

Click **L3 Features > IP Multicast Routing Protocol > MLD Proxy > MLD Proxy Forwarding Table** to view the following window:



Group Address	Source Address	Incoming Interface	Outgoing Interface
---------------	----------------	--------------------	--------------------

Figure 6-74 MLD Proxy Forwarding Table

The following parameters can be configured in the **MLD Proxy Forwarding Table** section:

Parameter	Description
Group Address	Enter the IPv6 group multicast address here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.5 DVMRP[ZEQUO6700RE/6600RE]

6.14.5.1 DVMRP Interface Settings

This window is used to configure and display the Distance Vector Multicast Routing Protocol (DVMRP) interface settings.

Click **L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Interface Settings** to view the following window:

The screenshot shows the 'DVMRP Interface Settings' window. At the top, there is a search bar with 'vlan1' entered and buttons for 'Find' and 'Show All'. Below this, it says 'Total Entries: 2'. A table displays the following data:

Interface	Address	Neighbor Timeout	Probe Time	Metric	Generation ID	State	
vlan1	192.168.70.123	35	10	1	0	Disabled	Edit
vlan100	0.0.0.0	35	10	1	0	Disabled	Edit

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

Figure 6-75 DVMRP Interface Settings

The following parameters can be configured in the **DVMRP Interface Settings** section:

Parameter	Description
Interface Name	Enter the VLAN interface name used here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

Click the **Edit** button to edit the settings of the specified entry.

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

Click the **Edit** button to view the following window:

The screenshot shows the 'DVMRP Interface Settings (Edit)' window. It has the same search bar and 'Find'/'Show All' buttons as Figure 6-75. Below the search bar, it says 'Total Entries: 2'. A table displays the following data with edit fields:

Interface	Address	Neighbor Timeout	Probe Time	Metric	Generation ID	State	
vlan1	192.168.70.123	<input type="text" value="35"/>	<input type="text" value="10"/>	<input type="text" value="1"/>	0	Disabled	Apply
vlan100	0.0.0.0	35	10	1	0	Disabled	Edit

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

Figure 6-76 DVMRP Interface Settings (Edit)

The following parameters can be configured:

Parameter	Description
Neighbor Timeout	Enter the neighbor lifetime value here. If the router has not received a probe message from a neighbor after the neighbor timeout interval, the neighbor is considered to be down. The range is from 1 to 65535 seconds. By default, this value is 35 seconds.
Probe Time	Enter the DVMRP probe interval value here. The range is from 1 to 65535 seconds. By default, this value is 10 seconds.
Metric	Enter the metric value here. The range is from 1 to 32. A value of 32 means it is unreachable. For each source network reported, a route metric is associated with the route being reported. The metric is the sum of the interface metrics between the router originating the report and the source network. For DVMRP, the metric with 32 means it is unreachable. This limits the breadth across the whole DVMRP network and is necessary to place an upper limit on the convergence time of the protocol.
State	Select to enable or disable the DVMRP feature on the selected interface.

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

6.14.5.2 DVMRP Routing Table

This window is used to display the DVMRP routing table and information.

Click **L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Routing Table** to view the following window:

DVMRP Routing Table

Source Network: 20.0.1.0/8 Find Show All

Total Entries: 0

Source Network	Upstream Neighbor	Metric	Learned	Interface	State	Expire Time
----------------	-------------------	--------	---------	-----------	-------	-------------

Note: State :H = Hold-down

Figure 6-77 DVMRP Routing Table

The following parameters can be configured in the **DVMRP Routing Table** section:

Parameter	Description
Source Network	Enter the source IPv4 network address and mask length here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.5.3 DVMRP Neighbor Table

This window is used to display the DVMRP neighbor table and information.

Click **L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Neighbor Table** to view the following window:

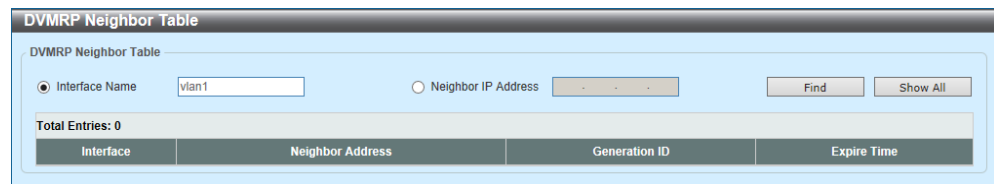


Figure 6-78 DVMRP Neighbor Table

The following parameters can be configured in the **DVMRP Neighbor Table** section:

Parameter	Description
Interface name	Enter the VLAN interface name here.
Neighbor IP Address	Select and enter the IPv4 address of the neighbor here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.6 PIM[ZEQUO6700RE/6600RE]

6.14.6.1 PIM for IPv4

6.14.6.1.1 PIM Interface

This window is used to configure and display the Protocol-Independent Multicast (PIM) interface settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Interface** to view the following window:

Figure 6-79 PIM Interface

The following parameters can be configured in the **PIM Interface Search** section:

Parameter	Description
Interface Name	Select and enter the name of the interface here.
Mode	Select the operation mode of PIM entries used in this filtered search here. Options to choose from are Dense Mode , Sparse Mode , and Sparse-Dense Mode .

Click the **Find** button to find and display entries based on the search criteria specified.

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

Click the **Edit** button to edit the settings of the specified entry.

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

Click the **Edit** button to view the following window:

PIM Interface Detail

PIM Interface Detail

Interface Name: vlan1

Interface Address: 192.168.70.124

Neighbor Count: 0

Generation ID: 0

PIM State: Disabled

Mode: Sparse Mode

Query Interval (1-18724): 30 sec ☐ Default

Designated Router: ☐ Default

DR Priority (0-4294967295): ☐ Default

Join Prune Interval (1-18000): sec ☐ Default

Apply Back

Figure 6-80 PIM Interface (Edit)

The following parameters can be configured in the **PIM Interface Detail** section:

Parameter	Description
PIM State	Select to enable or disable the PIM state on this interface here.
Mode	<p>Select the PIM mode here. Options to choose from are:</p> <ul style="list-style-type: none"> • Dense Mode - PIM-DM assumes that when a source starts sending, all downstream routers want to receive the multicast data stream. Initially multicast data stream are flooded to all downstream routers and the interfaces that have group members. If there are no downstream routers or group members, the router will send prune message to indicate that the multicast data stream is not desired. • Sparse Mode - When multicast traffic is received on a sparse mode interface, the first hop router will encapsulate and send the register message to RP. If the router is not the first hop router, the traffic will be forwarded based on the mroute entry. A sparse mode interface will only be populated as mroute member interface if receive join message from the downstream router or if group member on a sparse mode interface, PIM join process will be triggered to create the shared tree or the source tree. • Sparse-Dense Mode - When interface is configured as PIM Sparse-Dense mode, a multicast group received by the interface can operate in either sparse mode or dense mode of operation. When the interface receives multicast traffic, if there is a known RP for the group, then this group will operate in sparse mode, otherwise this multicast group will operate in dense mode.

Parameter	Description
Query Interval	Enter the interval at which hello messages are sent here. The range is from 1 to 18724 seconds. A PIMv2 router learns PIM neighbors via the PIM hello message. This feature configures the frequency of the hello message. Routers configured for IP multicasting send PIM hello messages to detect PIM routers. For SM, hello messages also determine the router to act as the designated router for each LAN segment. The configured query interval is also used as the value for hold time. By configuring a smaller period for the interval, the unresponsive neighbor can be discovered faster and thus the failover and recovery will become more efficient. Select the Default option to use the default value, which is 30 seconds.
DR Priority	After selecting Sparse Mode or Sparse-Dense Mode , enter the Designated Router's (DR) priority value here. The range is from 0 to 4294967295. A larger value represents the higher priority. In the Dense Mode (DM), the DR priority option will not be carried in the hello message. The router with the highest priority value will be the DR. If multiple routers are with the same priority status, the router with the highest IP address will be the DR. If there is a router that does not support the DR priority in its hello message on the LAN, all routers on the LAN will ignore DR priority and only use IP address to elect DR. Select the Default option to use the default value, which is 1.
Join Prune Interval	After selecting Sparse Mode or Sparse-Dense Mode , enter the Join/Prune message interval value here. The range is from 1 to 18000 seconds. When configuring the Join/Prune interval, consider the factors, such as the configured bandwidth and expected average number of multicast route entries for the attached network or link. For the Sparse Mode (SM), routers will periodically send join messages based on this interval. The hold-time in a Join/Prune message is 3.5 times the join-prune-interval. The receiving router will start a timer based on this hold-time, and prune the interface if no join message was received on this interface. Select the Default option to use the default value, which is 60 seconds.

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

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

6.14.6.1.2 PIM BSR Candidate

This window is used to configure and display the PIM BSR candidate settings. This feature requires an IP address to be configured on the interface in the PIM sparse mode.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM BSR Candidate** to view the following window:

Figure 6-81 PIM BSR Candidate

The following parameters can be configured in the **BSR Candidate Settings** section:

Parameter	Description
Interface Name	Enter the name of the interface here.
Hash Mask Length	Enter the hash mask length for RP selection here. The range is from 0 to 32. Select the Default option to use the default value, which is 30.
Priority	Enter the Candidate Bootstrap Router (CBSR) priority value here. The candidate with the highest priority is preferred. If the priority values are the same, the router with the highest IP address is preferred. The range is from 0 to 255. Select the Default option to use the default value, which is 64.
Interval	Enter the interval value between originating bootstrap messages here. The range is from 1 to 255 seconds. Select the Default option to use the default value, which is 60 seconds.

Click the **Add** button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

6.14.6.1.3 PIM RP Address

This window is used to configure and display the PIM RP address settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Address** to view the following window:

Figure 6-82 PIM RP Address

The following parameters can be configured in the **RP Address Settings** section:

Parameter	Description
RP Address	Enter the RP IPv4 address here.
Group Access List Name	Enter the standard access list that will be used here. Alternatively, click the Show List button to find and select any of the exiting ACL configured on this Switch to be used in this configuration. Select the All Groups option to map the RP to all multicast groups.

Click the **Show List** button to display the configured access control lists that can be used in this window.

Click the **Add** button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

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

Click the **Show List** button to view the following window:

Figure 6-83 PIM RP Address (Show List)

The following parameters can be configured:

Parameter	Description
ACL Type	Select the ACL type that will be used to display the type of existing access lists in the table here. Options to choose from are IP ACL , Expert IP ACL , IPv6 ACL , Expert IPv6 ACL , MAC ACL , and Expert ACL .
ACL List	Select the radio button of the access list in the table that will be used here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

Click the **Apply** button to use the selected access control list.

6.14.6.1.4 PIM RP Candidate

This window is used to configure and display the PIM RP candidate settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Candidate** to view the following window:

Figure 6-84 PIM RP Candidate

The following parameters can be configured in the **RP Candidate Global Settings** section:

Parameter	Description
Priority	Enter the candidate RP's priority value here. The range is from 0 to 255. Select the Default option to use the default value, which is 192.
Interval	Enter the candidate RP's advertisement interval value here. The range is from 1 to 16383 seconds. Select the Default option to use the default value, which is 60 seconds.
Wildcard Prefix Count	Enter the multicast group address wildcard (224.0.0.0/4) prefix count value in the Candidate RP (C-RP) message here. This value can either be 1 or 0. Select the Default option to use the default value, which is 0.

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

The following parameters can be configured in the **RP Candidate Settings** section:

Parameter	Description
Interface Name	Enter the name of the interface here.
Group Access List Name	Enter the standard access list that will be used here. Alternatively, click the Show List button to find and select any of the existing access lists configured on this Switch to be used in this configuration. Select the All Groups option to map the candidate RP to all multicast groups.

Click the **Show List** button to display the configured access control lists that can be used in this window.

Click the Add button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

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

Click the **Show List** button to view the following window:

Figure 6-85 PIM RP Candidate (Show List)

The following parameters can be configured:

Parameter	Description
ACL Type	Select the ACL type that will be used to display the type of existing access lists in the table here. Options to choose from are IP ACL , Expert IP ACL , IPv6 ACL , Expert IPv6 ACL , MAC ACL , and Expert ACL .
ACL List	Select the radio button of the access list in the table that will be used here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

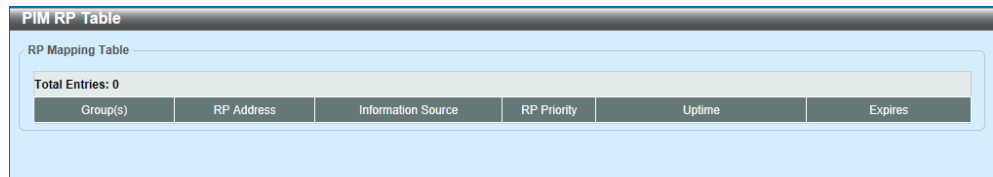
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Apply** button to use the selected access control list.

6.14.6.1.5 PIM RP Table

This window is used to display the PIM RP table and information.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Table** to view the following window:



The screenshot shows a window titled "PIM RP Table". Inside, there is a section labeled "RP Mapping Table". Below this label, it says "Total Entries: 0". Underneath, there is a table with six columns: "Group(s)", "RP Address", "Information Source", "RP Priority", "Uptime", and "Expires". The table is currently empty.

Group(s)	RP Address	Information Source	RP Priority	Uptime	Expires
----------	------------	--------------------	-------------	--------	---------

Figure 6-86 PIM RP Table

6.14.6.1.6 PIM Register Settings

This window is used to configure and display the PIM register settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Register Settings** to view the following window:

Figure 6-87 PIM Register Settings

The following parameters can be configured in the **Register Checksum Whole Packet** section:

Parameter	Description
RP Address Access List Name	Enter the standard access list that will be used here. Alternatively, click the Show List button to find and select any of the exiting access lists configured on this Switch to be used in this configuration.

Click the **Show List** button to display the configured access control lists that can be used in this window.

Click the **Add** button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Register Probe Time** section:

Parameter	Description
Register Probe	Enter the register probe time value here. The range is from 1 to 127 seconds. The register probe time is the time before the Register Stop Timer (RST) expires when a DR may send a Null-Register to the RP to cause it to resend a Register-Stop message. Select the Default option to use the default value, which is 5 seconds.

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

The following parameters can be configured in the **Register Suppression Time** section:

Parameter	Description
Register Suppression	Enter the register suppression timeout value here. The range is from 3 to 65535 seconds. When a DR receives the register stop message, it will start the suppression timer. During the suppression period, a DR stops sending the register message to the RP. Use this feature on the first hop router. The value of the register probe time must be less than half the value of the register suppression time to prevent a possible negative value in the setting of the register stop timer. The minimal value for the register suppression time is 3. Select the Default option to use the default value, which is 60 seconds.

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

Click the **Show List** button to view the following window:

Figure 6-88 PIM Register Settings (Show List)

The following parameters can be configured:

Parameter	Description
ACL Type	Select the ACL type that will be used to display the type of existing access lists in the table here. Options to choose from are IP ACL , Expert IP ACL , IPv6 ACL , Expert IPv6 ACL , MAC ACL , and Expert ACL .
ACL List	Select the radio button of the access list in the table that will be used here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

Click the **Apply** button to use the selected access control list.

6.14.6.1.7 PIM SPT Threshold Settings

This window is used to configure and display the **PIM SPT threshold** settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM SPT Threshold Settings** to view the following window:

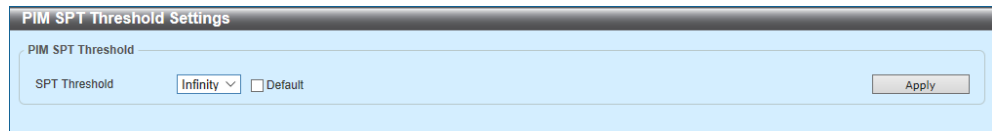


Figure 6-89 PIM SPT Threshold Settings

The following parameters can be configured in the **PIM SPT Threshold** section:

Parameter	Description
SPT Threshold	Select the SPT threshold option here. Options to choose from are: <ul style="list-style-type: none">• 0 - Specifies to establish the source tree right at the arrival of the first packet.• Infinity - Specifies to rely on the shared tree always. Select the Default option to use the default setting, which is Infinity .

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

6.14.6.1.8 PIM SSM Settings

This window is used to configure and display the PIM Source-Specific Multicast (SSM) settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM SSM Settings** to view the following window:

Figure 6-90 PIM SSM Settings

The following parameters can be configured in the **PIM SSM Settings** section:

Parameter	Description
Multicast Group Address Name	Enter the standard IP access list name here that defines the user-specified SSM group addresses. The group address should be defined in the destination IP address field of the rule entry. Alternatively, click the Show List button to find and select any of the exiting access lists configured on this Switch to be used in this configuration. Selecting the Default SSM Group (232.0.0.0/8) option specifies to use the default SSM group addresses. The default SSM group address range is 232/8.

Click the **Show List** button to display the configured access control lists that can be used in this window.

Click the **Add** button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

Click the **Show List** button to view the following window:

Figure 6-91 PIM SSM Settings (Show List)

The following parameters can be configured:

Parameter	Description
ACL Type	Select the ACL type that will be used to display the type of existing access lists in the table here. Options to choose from are IP ACL , Expert IP ACL , IPv6 ACL , Expert IPv6 ACL , MAC ACL , and Expert ACL .
ACL List	Select the radio button of the access list in the table that will be used here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

Click the **Apply** button to use the selected access control list.

6.14.6.1.9 PIM Neighbor Table

This window is used to display the PIM neighbor table and information.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Neighbor Table** to view the following window:

Figure 6-92 PIM Neighbor Table

The following parameters can be configured in the **Neighbor Information Table** section:

Parameter	Description
Interface Name	Enter the VLAN interface name here to display PIM-SM neighbor information.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.6.2 PIM for IPv6

6.14.6.2.1 PIM for IPv6 Interface

This window is used to configure and display the PIM IPv6 interface settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 Interface** to view the following window:

Interface Name	Interface Link-Local Address	Interface Global Address	Mode	Neighbor Count	Designated Router	DR Priority	Hello Interval	Join Prune Interval	Border	Edit
vlan1	FE80::250:40FF:FE3C:77...	::	None	0	not elected	1	30	60	Disabled	Edit
vlan3	FE80::250:40FF:FE3C:77...	::	None	0	not elected	1	30	60	Disabled	Edit

Figure 6-93 PIM for IPv6 Interface

The following parameters can be configured in the **PIM for IPv6 Interface Search** section:

Parameter	Description
Interface Name	Enter the VLAN interface name here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

Click the **Edit** button to edit the settings of the specified entry.

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

Click the **Edit** button to view the following window:

PIM for IPv6 Interface Detail	
PIM for IPv6 Interface Detail	
Interface Name	vlan1
Interface Link-Local Address	FE80::250:40FF:FE3C:7781
Interface Global Address	::
Mode	None
Designated Router	not elected
Designated Router Priority (0-4294967295)	1 <input type="checkbox"/> Default
Designated Router Priority Enabled	True
Generation ID	0
Hello Interval (1-18000)	30 sec <input type="checkbox"/> Default
Triggered Hello Interval	5 sec
Hello Holdtime	105 sec
Join Prune Interval (1-18000)	60 sec <input type="checkbox"/> Default
Join Prune Holdtime	210 sec
LAN Delay Enabled	True
Propagation Delay	1 sec
Override Interval	3 sec
Effective Propagation Delay	1 sec
Effective Override Interval	3 sec
Join Suppression Enabled	False
Bidirectional Capable	False
BSR Domain Border	Disabled
PIM Passive Mode	Disabled
<input type="button" value="Apply"/> <input type="button" value="Back"/>	

Figure 6-94 PIM for IPv6 Interface (Edit)

The following parameters can be configured in the **PIM for IPv6 Interface Detail** section:

Parameter	Description
Mode	Select the IPv6 PIM mode used in this interface here. Options to choose from are None and Sparse Mode . PIM for IPv6 will be disabled in this interface when the None option was selected.
Designated Router Priority	Enter the DR priority value here. The range is from 0 to 4294967295. A larger value means a higher priority. Select the Default option to use the default value, which is 1. This feature only takes effective when the VLAN interface is PIM-SM mode enabled. When a DR is a candidate for election, the following conditions apply: <ul style="list-style-type: none"> The router with the highest priority value configured on an interface will be elected as the DR. If multiple routers have the same highest priority, then the router with the highest IPv6 address configured on the interface will be elected as the DR. If a router does not advertise a priority value in its hello messages, the router is regarded as having the highest priority and will be elected as the DR. If there are multiple routers do not include the DR priority option in their hello messages, then the router with the highest IPv6 address will be elected as the DR.

Parameter	Description
Hello Interval	Enter hello message interval value here. The range is from 1 to 18000 seconds. A PIM router learns PIM neighbors via the hello message. Routers configured for IP multicast send PIM hello messages to detect PIM routers. For SM, hello messages are also used to determine which router will be elected as the designated router for each LAN segment. Select the Default option to use the default value, which is 30 seconds.
Join Prune Interval	Enter the Join/Prune message interval value here. The range is from 1 to 18000 seconds. When configuring the Join/Prune interval, the user needs to consider the factors, such as configured bandwidth and expected average number of multicast route entries for the attached network or link (for example, the period would be longer for lower-speed links, or for routers in the center of the network that expect to have a larger number of entries). For SM-mode, the router will periodically send the join message based on this interval. The hold-time in a Join/Prune message is 3.5 times the join-prune-interval. The receiving router will start a timer based on this hold-time, and prune the interface if no join message is received on this interface. Select the Default option to use the default value, which is 60 seconds.
BSR Domain Border	Select to enable or disable the BSR domain border feature here. When an interface is configured as a border, it will prevent bootstrap router (BSR) messages from being sent or received through it.
PIM Passive Mode	Select to enable or disable the PIM passive mode for this interface here. This feature only takes effect when the interface is IPv6 PIM enabled. When the passive mode is enabled, the interface will neither send PIM messages out nor accept PIM messages from this interface. The router will act as it is the only PIM router on the network. Use this feature only when there is only one PIM router on the LAN.

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

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

6.14.6.2.2 PIM for IPv6 BSR Candidate Settings

This window is used to configure and display the PIM IPv6 BSR candidate settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 BSR Candidate Settings** to view the following window:

Figure 6-95 PIM for IPv6 BSR Candidate Settings

The following parameters can be configured in the **BSR Candidate Settings** section:

Parameter	Description
Interface Name	Enter the VLAN interface name used here.
Hash Mask Length	Enter the hash mask length for RP selection here. The range is from 0 to 128. The mask (128 bits maximum) that is to be logically AND with the group address before the hash function is executed. All groups with the same seed hash (correspond) to the same RP. Therefore one RP can be derived for multiple groups. Select the Default option to use the default value, which is 126.
Priority	Enter the priority value for the BSR candidate here. The range is from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IPv6 address is the BSR. Select the Default option to use the default value, which is 64.

Click the **Add** button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

6.14.6.2.3 PIM for IPv6 BSR Table

This window is used to display the PIM IPv6 BSR table and information.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 BSR Table** to view the following window:

PIM for IPv6 BSR Table				
BSR Candidate RP Cache				
Total Entries: 0				
Group(s)	RP Address	RP Priority	RP Uptime	RP Expires
BSR Candidate RP Information				
Total Entries: 0				
Candidate RP	Priority	Holdtime	Advertisement Interval	Next Advertisement

Figure 6-96 PIM for IPv6 BSR Table

6.14.6.2.4 PIM for IPv6 RP Address

This window is used to configure and display the PIM RP IPv6 address settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Address** to view the following window:

Figure 6-97 PIM for IPv6 RP Address

The following parameters can be configured in the **RP Address Settings** section:

Parameter	Description
RP Address	Enter the RP IPv6 address here.
Group Access List Name	Enter the standard IPv6 access list that will be used here. Alternatively, click the Show List button to find and select any of the exiting access lists configured on this Switch to be used in this configuration. Select the All Groups option to map the RP to all multicast groups.
Override	Selecting this option specifies that the static RP will override dynamically learned RPs.

Click the **Show List** button to display the configured access control lists that can be used in this window.

Click the **Add** button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

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

Click the **Show List** button to view the following window:

Figure 6-98 PIM for IPv6 RP Address (Show List)

The following parameters can be configured:

Parameter	Description
ACL Type	Select the ACL type that will be used to display the type of existing access lists in the table here. Options to choose from are IP ACL , Expert IP ACL , IPv6 ACL , Expert IPv6 ACL , MAC ACL , and Expert ACL .
ACL List	Select the radio button of the access list in the table that will be used here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

Click the **Apply** button to use the selected access control list.

6.14.6.2.5 PIM for IPv6 RP Candidate

This window is used to configure and display the PIM IPv6 RP candidate settings. Only one group access list can be specified for each interface.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Candidate** to view the following window:

PIM for IPv6 RP Candidate

RP Candidate Settings

Interface Name:

Group Access List Name: ☐ All Groups Show List

Priority (0-255): ☐ Default

Interval (1-16383): sec ☐ Default Add

RP Candidate Table

Total Entries: 1

Interface Name	Group Access List	Interval	Priority	
vlan1	FF00::8	60	192	Edit Delete

1/1 Go

Figure 6-99 PIM for IPv6 RP Candidate

Click the **Edit** button to view the following window:

PIM for IPv6 RP Candidate

RP Candidate Settings

Interface Name:

Group Access List Name: ☐ All Groups Show List

Priority (0-255): ☐ Default

Interval (1-16383): sec ☐ Default Add

RP Candidate Table

Total Entries: 1

Interface Name	Group Access List	Interval	Priority	
vlan1	FF00::8	<input type="text" value="60"/>	<input type="text" value="192"/>	Apply Delete

1/1 Go

Figure 6-100 PIM for IPv6 RP Candidate (Edit)

The following parameters can be configured in the **RP Candidate Settings** section:

Parameter	Description
Interface Name	Enter the interface name here whose IPv6 address will be advertised as the candidate RP (C-RP).
Group Access List Name	Enter the standard IPv6 access list that will be used here. Alternatively, click the Show List button to find and select any of the exiting access lists configured on this Switch to be used in this configuration. Select the All Groups option to map the candidate RP to all multicast groups.
Priority	Enter the RP priority value here. The range is from 0 to 255. Select the Default option to use the default value, which is 192.
Interval	Enter the RP candidate advertisement interval value here. The range is from 1 to 16383 seconds. Select the Default option to use the default value, which is 60 seconds.

Click the **Show List** button to display the configured access control lists that can be used in this window.

Click the **Add** button to add a new entry.

Click the **Edit** button to edit the settings of the specified 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.

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

Click the **Show List** button to view the following window:

The screenshot shows the 'Access Control List' configuration window. At the top, there's a header bar with the title 'Access Control List'. Below it, the 'ACL Type' is set to 'IP ACL'. There are 'Find' and 'Show All' buttons. A section indicates 'Total Entries: 1'. Below this is a table with two columns: 'ACL Name' and 'Type'. The entry 'Standard_IP_ACL' is listed with the type 'Standard IP ACL'. Below the table, there are navigation controls showing '1/1' and a 'Go' button. At the bottom, there's a section for 'Standard_IP_ACL Rule' with a table showing 'Action' as 'Permit' and 'Rule' as 'any any'. An 'Apply' button is at the bottom right.

Figure 6-101 PIM for IPv6 RP Candidate (Show List)

The following parameters can be configured:

Parameter	Description
ACL Type	Select the ACL type that will be used to display the type of existing access lists in the table here. Options to choose from are IP ACL , Expert IP ACL , IPv6 ACL , Expert IPv6 ACL , MAC ACL , and Expert ACL .
ACL List	Select the radio button of the access list in the table that will be used here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

Click the **Apply** button to use the selected access control list.

6.14.6.2.6 PIM for IPv6 RP Embedded Settings

This window is used to configure and display the PIM IPv6 RP embedded settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Embedded Settings** to view the following window:

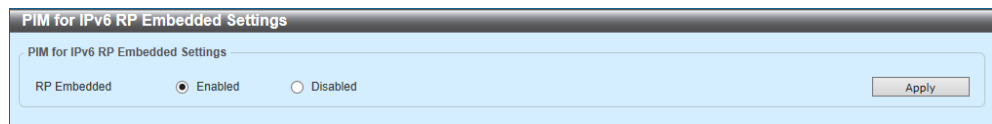


Figure 6-102 PIM for IPv6 RP Embedded Settings

The following parameters can be configured in the **PIM for IPv6 Embedded Settings** section:

Parameter	Description
RP Embedded	Select to enable or disable the RP embedded feature here.

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

6.14.6.2.7 PIM for IPv6 RP Table

This window is used to display the PIM IPv6 RP table and information.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Table** to view the following window:

Figure 6-103 PIM for IPv6 RP Table

The following parameters can be configured in the **RP Mapping Table** section:

Parameter	Description
Group Address/Prefix Length	Enter the multicast group IPv6 address and prefix length here.
Information Source	<p>Select the source to display here. Options to choose from are:</p> <ul style="list-style-type: none"> • Bootstrap - Specifies to display ranges learned through the BSR. • Embedded RP - Specifies to display group ranges learned through the embedded rendezvous point (RP). • Static - Specifies to display ranges enabled by static configuration.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

6.14.6.2.8 PIM for IPv6 Register Settings

This window is used to configure and display the PIM IPv6 register settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 Register Settings** to view the following window:

Figure 6-104 PIM for IPv6 Register Settings

The following parameters can be configured in the **Register Checksum Whole Packet** section:

Parameter	Description
Register Checksum Wholepkt	Select the enable or disable the register checksum whole-packet feature here. When enabled, it configures the router to calculate the checksum of register message over the entire PIM message including the data portion. By default, the register checksum methodology is PIM RFC-compliant, excluding the data portion in the Register message.

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

The following parameters can be configured in the **Register Probe Time** section:

Parameter	Description
Register Probe	Enter the register probe time value here. The range is from 1 to 127 seconds. The register-probe time is the time before the Register-Stop Timer (RST) expires when a DR may send a Null-Register to the RP to cause it to resend a Register-Stop message. Select the Default option to use the default value, which is 5 seconds.

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

The following parameters can be configured in the **Register Suppression Time** section:

Parameter	Description
Register Suppression	Enter the register suppression timeout value here. The range is from 3 to 65535 seconds. When a DR receives the register-stop message, it will start the suppression timer. During the suppression time a DR will stop sending Register-encapsulated data to the RP. This timer should be configured on the designated router. The value of the Register Probe Time must be less than half the value of the Register Suppression Time to prevent a possible negative value in the setting of the Register-Stop Timer. The minimal value for Register Suppression Time is 3. Select the Default option to use the default value, which is 60 seconds.

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

6.14.6.2.9 PIM for IPv6 SPT Threshold Settings

This window is used to configure and display the PIM IPv6 SPT threshold settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 SPT Threshold Settings** to view the following window:

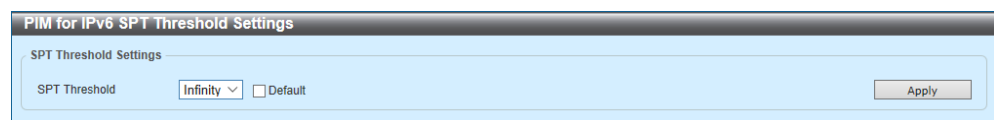


Figure 6-105 PIM for IPv6 SPT Threshold Settings

The following parameters can be configured in the **SPT Threshold** section:

Parameter	Description
SPT Threshold	Select the SPT threshold value here. Options to choose from are: <ul style="list-style-type: none">• 0 - Specifies to establish the source tree right at the arrival of the first packet.• Infinity - Specifies to rely on the shared tree always. Select the Default option to use the default setting, which is Infinity.

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

6.14.6.2.10 PIM for IPv6 (S,G) Keepalive Time

This window is used to configure and display the PIM IPv6 (S,G) keep-alive time settings.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 (S,G) Keepalive Time** to view the following window:

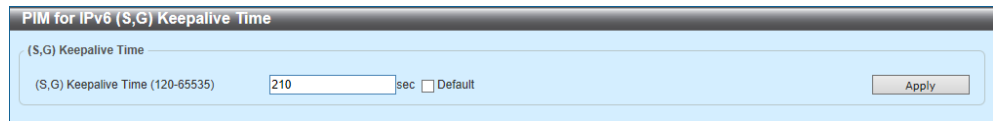


Figure 6-106 PIM for IPv6 (S,G) Keepalive Time

The following parameters can be configured in the **(S,G) Keepalive Time** section:

Parameter	Description
(S,G) Keepalive Time	Enter the (S,G) keep-alive time value here. This specifies the period during which the PIM router will maintain the (S, G) state in the absence of explicit (S, G) local membership or (S, G) join messages received to maintain it. The range is from 120 to 65535 seconds. Select the Default option to use the default value, which is 210 seconds.

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

6.14.6.2.11 PIM for IPv6 Multicast Route Table

This window is used to display the PIM IPv6 multicast route table and information.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 Multicast Route Table** to view the following window:

Source Address	Group Address	RPT	Uptime	Flags	RP Address	RPF Neighbor Address	Join/Prune State
Note: JP State- Join Prune State, ET - Expiry Timer, PPT - Prune Pending Timer, KAT - Keep Alive Timer Flags: S - Sparse, T - SPT-bit set							

Figure 6-107 PIM for IPv6 Multicast Route Table

6.14.6.2.12 PIM for IPv6 Neighbor Table

This window is used to display the PIM IPv6 neighbor table and information.

Click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 Neighbor Table** to view the following window:

PIM for IPv6 Neighbor Table

Neighbor Information Search

Interface Name

Neighbor Information Table

Total Entries: 0

Neighbor Address	Interface Name	Uptime	Expires	Version	DR Priority	Mode
------------------	----------------	--------	---------	---------	-------------	------

Note: Mode: B - Bidirectional Capable, DR - Designated Router, N - Default DR Priority, G - Supports Generation ID

Figure 6-108 PIM for IPv6 Neighbor Table

The following parameters can be configured in the **Neighbor Information Search** section:

Parameter	Description
Interface Name	Enter the VLAN interface name used in this display here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.7 IPMC

6.14.7.1 IP Multicast Global Settings

This window is used to configure and display the global IP Multicast (IPMC) settings.

Click **L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Global Settings** to view the following window:

Figure 6-109 IP Multicast Global Settings

The following parameters can be configured in the **IP Multicast Routing Global State** section:

Parameter	Description
Global State	Select to globally enable or disable the IP multicast routing feature here. When IP multicast routing is disabled, the system will stop routing multicast packets even though the multicast routing protocol is enabled.

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

The following parameters can be configured in the **IP Multicast Interface Table** section:

Parameter	Description
Interface Name	Enter the interface name that will be used for the search here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

6.14.7.2 IP Multicast Route Settings

This window is used to configure and display the IP multicast route settings.

Click **L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Route Settings** to view the following window:

Figure 6-110 IP Multicast Route Settings

The following parameters can be configured in the **IP Multicast Route Table** section:

Parameter	Description
Summary	Selecting this option specifies to display a one-line, abbreviated summary of each entry in the IP multicast routing table.
Multicast Protocol	Select this option and then select the multicast protocol that will be used in this display here. Options to choose from are: <ul style="list-style-type: none"> • PIM-DM - Specifies to display only the PIM-DM routes. • PIM-SM - Specifies to display only the PIM-SM routes. • DVMRP - Specifies to display only the DVMRP routes.
Group Address	Select and enter the multicast group IP address here.
Source Address	Enter the multicast source IP address here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.7.3 IP Multicast Forwarding Cache

This window is used to display IP multicast forwarding cache information.

Click **L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Forwarding Cache** to view the following window:

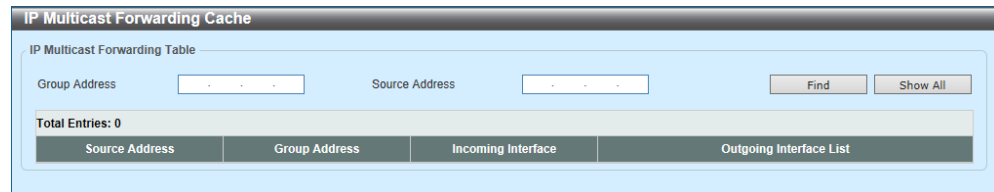


Figure 6-111 IP Multicast Forwarding Cache

The following parameters can be configured in the **IP Multicast Forwarding Table** section:

Parameter	Description
Group Address	Enter the multicast group IP address here.
Source Address	Enter the multicast source IP address here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.8 IPv6MC

6.14.8.1 IPv6 Multicast Global Settings [ZEQUO6700RE/6600RE]

This window is used to configure and display the global IPv6 multicast settings.

Click **L3 Features > IP Multicast Routing Protocol > IPv6MC > IPv6 Multicast Global Settings** to view the following window:

Figure 6-112 IPv6 Multicast Global Settings

The following parameters can be configured in the **IPv6 Multicast Routing** section:

Parameter	Description
IPv6 Multicast Routing Global State	Select to globally enable or disable the IPv6 multicast routing feature here. When IPv6 multicast routing is disabled, the system will stop routing multicast packets even though the multicast routing protocol is enabled.

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

The following parameters can be configured in the **IPv6 Multicast Interface Table** section:

Parameter	Description
Interface Name	Enter the VLAN interface name that will be used here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

6.14.8.2 IPv6 Multicast Routing Table [ZEQUO6700RE/6600RE]

This window is used to display the IPv6 multicast routing table and information.

Click **L3 Features > IP Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Table** to view the following window:

Figure 6-113 IPv6 Multicast Routing Table

The following parameters can be configured in the **IPv6 Multicast Routing Table** section:

Parameter	Description
Group IPv6 Address	Enter the multicast group IPv6 address here.
Source IPv6 Address	Enter the multicast source IPv6 address here. Selecting the Summary option specifies to display a one-line, abbreviated summary of each entry in the IPv6 multicast routing table.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.14.8.3 IPv6 Multicast Routing Forwarding Cache Table

This window is used to display IPv6 multicast routing forwarding cache information.

Click **L3 Features > IP Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Forwarding Cache Table** to view the following window:

Figure 6-114 IPv6 Multicast Routing Forwarding Cache Table

The following parameters can be configured in the **IPv6 Multicast Routing Forwarding Cache Table** section:

Parameter	Description
Group IPv6 Address	Enter the multicast group IPv6 address here.
Source IPv6 Address	Enter the multicast source IPv6 address here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

6.15 IP Route Filter[ZEQUO6700RE/6600RE]

6.15.1 Route Map

This window is used to configure and display the IP route map settings.

Click **L3 Features > IP Route Filter > Route Map** to view the following window:

Figure 6-115 Route Map

The following parameters can be configured in the **Route Map** section:

Parameter	Description
Route Map Name	Enter the route map name here. This name can be up to 16 characters long.
Direction	Select the direction for this rule here. Options to choose from are: <ul style="list-style-type: none"> • Permit - Specifies that routes that match the rule entry are permitted. • Deny - Specifies that routes that match the rule entry are denied.
Sequence ID	Enter the sequence ID for this rule here. The range is from 1 to 65535.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

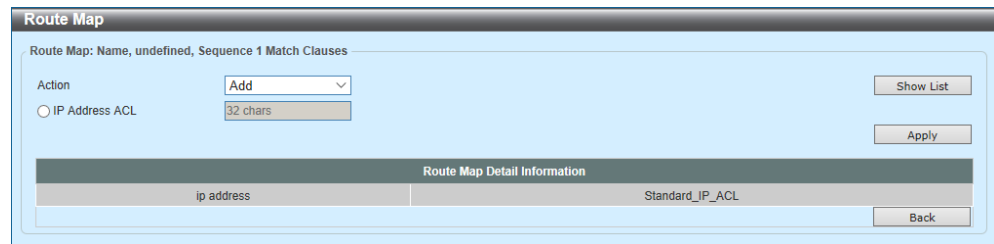
Click the **Edit** button under **Match Clauses** to edit the match clause settings of the specified entry.

Click the **Edit** button under **Set Clauses** to edit the set clause settings of the specified 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.

Click the **Edit** button under Match Clauses to view the following window:



The screenshot shows the 'Route Map' configuration window. At the top, it says 'Route Map: Name, undefined, Sequence 1 Match Clauses'. Below this, there is an 'Action' dropdown menu set to 'Add' and a text input field for 'IP Address ACL' with a '32 chars' limit. To the right of these fields are 'Show List' and 'Apply' buttons. Below the input fields is a table titled 'Route Map Detail Information' with two columns: 'ip address' and 'Standard_IP_ACL'. At the bottom right is a 'Back' button.

Figure 6-116 Route Map (Edit, Match Clauses)

The following parameters can be configured:

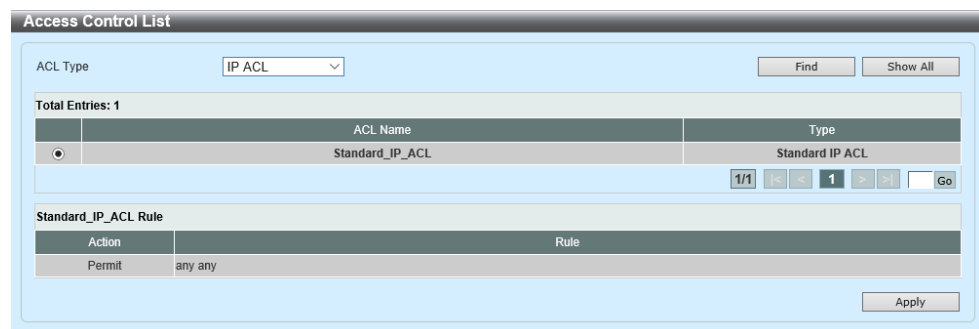
Parameter	Description
Action	Select Add to add a new entry based in the information entered. Select Delete to delete an entry based in the information entered.
IP Address ACL	Select and enter the standard or extended IP access list name here. This option is used to define a clause to match the route based on the standard or extended IP access list. This string can be up to 32 characters long.

Click the **Show List** button to display the configured access control lists that can be used in this window.

Click the **Apply** button to add a new entry.

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

Click the **Show List** button to view the following window:



The screenshot shows the 'Access Control List' configuration window. At the top, there is an 'ACL Type' dropdown menu set to 'IP ACL'. To the right are 'Find' and 'Show All' buttons. Below this, it says 'Total Entries: 1'. There is a table with two columns: 'ACL Name' and 'Type'. The first row shows 'Standard_IP_ACL' under 'ACL Name' and 'Standard IP ACL' under 'Type'. Below the table is a pagination control showing '1/1' and a 'Go' button. Below the pagination control is a section titled 'Standard_IP_ACL Rule' with a table. The table has two columns: 'Action' and 'Rule'. The first row shows 'Permit' under 'Action' and 'any any' under 'Rule'. At the bottom right is an 'Apply' button.

Figure 6-117 Route Map (Edit, Match Clauses, Show List)

The following parameters can be configured:

Parameter	Description
ACL Type	Select the ACL type that will be used to display the type of existing access lists in the table here. Options to choose from are IP ACL , Expert IP ACL , IPv6 ACL , Expert IPv6 ACL , MAC ACL , and Expert ACL .
ACL List	Select the radio button of the access list in the table that will be used here.

Click the **Find** button to find and display entries based on the search criteria specified.

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

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

Click the **Apply** button to use the selected access control list.

Click the **Edit** button under **Set Clauses** to view the following window:

The screenshot shows the 'Route Map' configuration window. At the top, it says 'Route Map: Name, undefined, Sequence 1 Set Clauses'. Below this, there are three radio buttons for 'Action': 'IP Default Next Hop' (selected), 'IP Next Hop', and 'IP Precedence'. To the right of these is a note: 'Note: 16 default next-hops can be specified at most.' Below the radio buttons are three input fields: a dropdown for 'Add', a text field for 'IP Address', and a dropdown for 'Routine(0)'. There is an 'Apply' button on the right. Below this is a table titled 'Route Map Detail Information' with two rows: 'ip precedence' with value '0' and 'default next-hop' with value '192.168.80.1'. There is a 'Back' button at the bottom right.

Figure 6-118 Route Map (Edit, Set Clauses)

The following parameters can be configured:

Parameter	Description
Action	Select Add to add a new entry based in the information entered. Select Delete to delete an entry based in the information entered.
IP Default Next Hop	Enter the default next-hop IP addresses in the spaces provided that will be used to route the packet.
IP Next Hop	Select the IP next hop type here. This feature is used to configure the next-hop router to route the packet that passes the match clauses of the configured route map sequence. Options to choose from are: <ul style="list-style-type: none"> • IP Address - Specifies the IP addresses of the next-hops to route the packet. Enter the next-hop IP addresses in the spaces provided here. Up to 8 next-hop IP addresses can be entered. • Recursive - Specifies the IP address of the recursive as the next-hop router. Enter the recursive next-hop IP address in the space provided here.
IP Precedence	Select the IP precedence option here. Options to choose from are Routine (0), Priority (1), Immediate (2), Flash (3), Flash Override (4), Critical (5), Internet (6), and Network (7) . Use this feature to set the precedence value in the IP header. This option only takes effect when policy routing involves the IPv4 packet.

Click the **Apply** button to add a new entry.

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

6.16 Policy Route[ZEQUO6700RE/6600RE]

This window is used to configure and display the policy route settings.

Click **L3 Features > Policy Route** to view the following window:

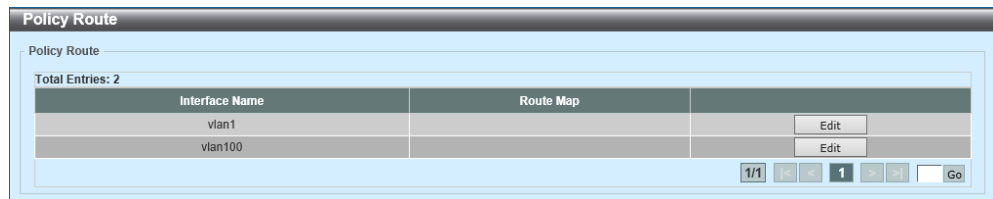


Figure 6-119 Policy Route

Click the **Edit** button to view the following window:

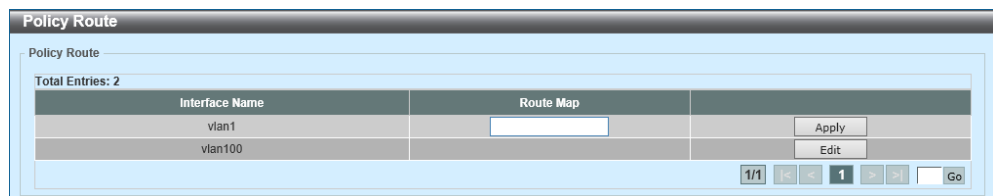


Figure 6-120 Policy Route (Edit)

The following parameters can be configured in the **Policy Route** section:

Parameter	Description
Route Map	Enter the route map name here that will be used in this policy route entry.

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

Click the **Edit** button to edit the settings of the specified entry.

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

6.17 VRRP Settings

This window is used to configure and display the Virtual Router Redundancy Protocol (VRRP) settings.

Click **L3 Features > VRRP Settings** to view the following window:

Figure 6-121 VRRP Settings

The following parameters can be configured in the **VRRP Settings** section:

Parameter	Description
SNMP Server Traps VRRP New master	Select to enable or disable the SNMP server traps feature for the new VRRP master. If enabled, once the device has transitioned to the master state, a trap will be sent out.
SNMP Server Traps VRRP Auth Fail	Select to enable or disable the SNMP server traps feature for authentication failures. If enabled, if a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type, then a trap will be sent out.
Non-owner-ping Response	Select to enable or disable the non-owner ping response feature here. This feature is used to enable the virtual router in the master state to respond to Internet Control Message Protocol (ICMP) echo requests for an IP address not owned but associated with this virtual router.

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

The following parameters can be configured in the **Virtual Router Settings** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
VRID	Enter the virtual router ID used here. This ID is used to identify the virtual router in the VRRP group. The range is from 1 to 255.
Virtual IP Address	Enter the IPv4 address for the created virtual router group here.
VRRP Authentication	Select to enable and then enter the plain text authentication password for VRRP authentication on the interface here. This string can be up to 8 characters long. The authentication is applied to all virtual routers on this interface. The devices in the same VRRP group must have the same authentication password.
Interface Name	Enter the interface name used here. This name can be up to 12 characters long.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Edit** button to edit the settings of the specified 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.

Click the **Edit** button to view the following window:

VRRP Virtual Router Settings

vlan1 - Group 1

State: Master

Virtual IP Address: 192.168.70.151

Virtual MAC Address: 00-00-5E-00-01-01

Advertisement Interval (1-255): 1 sec ☐ Default

Preemption: ☒ Enabled

Priority (1-254): 100 ☐ Default

Master Router: 192.168.70.123

Critical IP Address: - - -

Authentication: - - -

Shutdown: ☐ Disabled

Back Apply

Figure 6-122 VRRP Settings (Edit)

The following parameters can be configured:

Parameter	Description
Advertisement Interval	Enter the advertisement interval value here. This is the time interval between successive VRRP advertisements by the master router. The range is from 1 to 255 seconds. By default, this value is 1 second.
Preemption	Select to enable or disable the preemption feature here. This feature is used to allow a router to take over the master role if it has a better priority than the current master.
Priority	Enter the priority value here. The range is from 1 to 254.
Critical IP Address	Enter the critical IPv4 address here. If the critical IP is configured on one virtual router, the virtual router cannot be activated when the critical IP address is unreachable. One VRRP group can only track one critical IP.
Shutdown	Select to enable or disable the shutdown feature here. This feature is used to disable a virtual router on an interface. Avoid the common mistake of shutting down the IP address owner router before shutting down other non-owner routers.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

7 QoS (Quality of Service)

7.1 Basic Settings

7.1.1 Port Default CoS

This window is used to configure and display the default Class of Service (CoS) settings per port interface.

Click **QoS > Basic Settings > Port Default CoS** to view the following window:

Port	Default CoS	Override
Gi1/0/1	0	No
Gi1/0/2	0	No
Gi1/0/3	0	No
Gi1/0/4	0	No
Gi1/0/5	0	No
Gi1/0/6	0	No
Gi1/0/7	0	No
Gi1/0/8	0	No
Gi1/0/9	0	No
Gi1/0/10	0	No

Figure 7-1 Port Default CoS

The following parameters can be configured in the **Port Default CoS** 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.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are 0 to 7. <ul style="list-style-type: none"> Select the Override option to override the CoS of the packets. The default CoS will be applied to all incoming packets, tagged or untagged, received by the port. Select the None option to specify that the CoS of the packets will be the packet's CoS if the packets are tagged, and will be the port default CoS if the packet is untagged.

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

7.1.2 Port Scheduler Method

This window is used to configure and display the method settings related to the port scheduler feature.

Click **QoS > Basic Settings > Port Scheduler Method** to view the following window:

Unit	From Port	To Port	Scheduler Method
1	Gi1/0/1	Gi1/0/1	Weighted Round Robin

Unit 1 Settings	
Port	Scheduler Method
Gi1/0/1	WRR
Gi1/0/2	WRR
Gi1/0/3	WRR
Gi1/0/4	WRR
Gi1/0/5	WRR
Gi1/0/6	WRR
Gi1/0/7	WRR
Gi1/0/8	WRR
Gi1/0/9	WRR
Gi1/0/10	WRR

Figure 7-2 Port Scheduler Method

The following parameters can be configured in the **Port Scheduler Method** 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.

Parameter	Description
Scheduler Method	<p>Select the scheduler method that will be applied to the specified port(s). Options to choose from are:</p> <ul style="list-style-type: none"> • Strict Priority (SP) - Specifies that all queues use strict priority scheduling. It provides strict priority access to the queues from the highest CoS queue to the lowest. • Round Robin (RR) - Specifies that all queues use round robin scheduling. It provides fair access to service a single packet at each queue before moving on to the next one. • Weighted Round Robin (WRR) - Operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1 and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time. This is the default option. • Weighted Deficit Round Robin (WDRR) - Operates by serving an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time. All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different, based on the user configuration. <p>To set a CoS queue, in the SP mode, any higher priority CoS queue must also be in the strict priority mode.</p>

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

7.1.3 Queue Settings

This window is used to configure and display the QoS queue settings.

Click **QoS > Basic Settings > Queue Settings** to view the following window:

Port	Queue ID	WRR Weight	WDRR Quantum
Gi1/0/1	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1
Gi1/0/2	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1

Figure 7-3 Queue Settings

The following parameters can be configured in the **Queue 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.
Queue ID	Enter the queue ID value here. The range is from 0 to 7.
WRR Weight	Enter the WRR weight value here. The range is from 0 to 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. The weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. The range is from 0 to 127.

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

7.1.4 CoS to Queue Mapping

This window is used to configure and display the CoS-to-Queue mapping settings.

Click **QoS > Basic Settings > CoS to Queue Mapping** to view 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

The following parameters can be configured:

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

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

7.1.5 Port Rate Limiting

This window is used to configure and display the port rate limiting settings.

Click **QoS > Basic Settings > Port Rate Limiting** to view the following window:

Port Rate Limiting

Port Rate Limiting

Unit: 1 From Port: Gi1/0/1 To Port: Gi1/0/1 Direction: Input

Rate Limit: ☒ Bandwidth (8-40000000) Kbps Kbps Kbyte

☐ Percent (1-100) % % Kbyte

☐ None

Unit 1 Settings

Port	Input		Output	
	Rate	Burst	Rate	Burst
Gi1/0/1	No Limit	No Limit	No Limit	No Limit
Gi1/0/2	No Limit	No Limit	No Limit	No Limit
Gi1/0/3	No Limit	No Limit	No Limit	No Limit
Gi1/0/4	No Limit	No Limit	No Limit	No Limit
Gi1/0/5	No Limit	No Limit	No Limit	No Limit
Gi1/0/6	No Limit	No Limit	No Limit	No Limit
Gi1/0/7	No Limit	No Limit	No Limit	No Limit
Gi1/0/8	No Limit	No Limit	No Limit	No Limit
Gi1/0/9	No Limit	No Limit	No Limit	No Limit
Gi1/0/10	No Limit	No Limit	No Limit	No Limit

Figure 7-5 Port Rate Limiting

The following parameters can be configured in the **Port Rate Limiting** 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.
Direction	Select the direction option here. Options to choose from are: <ul style="list-style-type: none"> Input - The rate limit for ingress packets is configured. Output - The rate limit for egress packets is configured.

Parameter	Description
Rate Limit	<p>Select and enter the rate limit value here.</p> <ul style="list-style-type: none">• When Bandwidth is selected, enter the input/output bandwidth value used in the space provided. The range is from 8 to 40000000 kbps. Enter the Burst Size value in the space provided. The range is from 0 to 128000 kilobytes.• When Percent is selected, enter the input/output bandwidth percentage value used in the space provided. The range is from 1 and 100 percent. Enter the Burst Size value in the space provided. The range is from 0 to 128000 kilobytes.• When None is selected, the rate limit on the specified port(s) will be removed. The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress will send a pause frame or a flow control frame when the received traffic exceeds the limitation.

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

7.1.6 Queue Rate Limiting

This window is used to configure and display the queue rate limiting settings.

Click **QoS > Basic Settings > Queue Rate Limiting** to view the following window:

Queue Rate Limiting

Queue Rate Limiting

Unit: 1 From Port: Gi1/0/1 To Port: Gi1/0/1 Queue ID: 0 Rate Limit: ☒ Min Bandwidth (8-40000000) Kbps Kbps
☐ Min Percent (1-100) % %
☐ None

Unit 1 Settings

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
Gi1/0/1	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...
Gi1/0/2	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...
Gi1/0/3	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...
Gi1/0/4	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...
Gi1/0/5	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...
Gi1/0/6	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...
Gi1/0/7	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Gi1/0/8	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Gi1/0/9	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Gi1/0/10	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...

Figure 7-6 Queue Rate Limiting

The following parameters can be configured in the **Queue Rate Limiting** 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.
Queue ID	Select the queue ID that will be configured here. Options to choose from are 0 to 7.
Rate Limit	<p>Select and enter the rate limit settings of the queue here.</p> <ul style="list-style-type: none"> When the Min Bandwidth option is selected, enter the minimum bandwidth rate limit in the space provided. The range is from 8 to 40000000 kbps. Enter the maximum bandwidth (Max Bandwidth) rate limit in the space provided. The range is from 8 to 40000000 kbps. When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available. When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied. The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum guaranteed bandwidth of one CoS cannot be used across physical ports. When the Min Percent option is selected, enter the minimum bandwidth percentage value in the space provided. The range is from 1 to 100 percent (%). Enter the maximum percentage value (Max Percent) in the space provided. The range is from 1 to 100 percent (%). When None is selected, then no rate limit will be assigned to the specified port(s).

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

7.2 Advanced Settings

7.2.1 DSCP Mutation Map

This window is used to configure and display the Differentiated Services Code Point (DSCP) mutation map settings.

Click **QoS > Advanced Settings > DSCP Mutation Map** to view the following window:

Figure 7-7 DSCP Mutation Map

The following parameters can be configured in the **DSCP Mutation Map** section:

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

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.

7.2.2 Port Trust State and Mutation Binding

This window is used to configure and display the port trust state and mutation binding settings.

Click **QoS > Advanced Settings > Port Trust State and Mutation Binding** to view the following window:

Port Trust State and Mutation Binding

Port Trust State and Mutation Binding

Unit: 1 From Port: Gi1/0/1 To Port: Gi1/0/1 Trust State: CoS DSCP Mutation Map: 32 chars ☐ None

Unit 1 Settings

Port	Trust State	DSCP Mutation Map
Gi1/0/1	Trust CoS	
Gi1/0/2	Trust CoS	
Gi1/0/3	Trust CoS	
Gi1/0/4	Trust CoS	
Gi1/0/5	Trust CoS	
Gi1/0/6	Trust CoS	
Gi1/0/7	Trust CoS	
Gi1/0/8	Trust CoS	
Gi1/0/9	Trust CoS	
Gi1/0/10	Trust CoS	

Figure 7-8 Port Trust State and Mutation Binding

The following parameters can be configured in the **Port Trust State and Mutation Binding** 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.
Trust State	Select the port trust state here. Options to choose from are CoS and DSCP .
DSCP Mutation Map	Select and enter the DSCP mutation map name used here. This name can be up to 32 characters long. Select the None option not to allocate a DSCP mutation map to the port(s).

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

7.2.3 DSCP CoS Mapping

This window is used to configure and display the DSCP CoS mapping settings.

Click **QoS > Advanced Settings > DSCP CoS Mapping** to view the following window:

Port	CoS	DSCP List
Gi1/0/1	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63
Gi1/0/2	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63

Figure 7-9 DSCP CoS Mapping

The following parameters can be configured in the **DSCP CoS Mapping** 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.
CoS	Select the CoS value to map to the DSCP list. Options to choose from are 0 to 7.
DSCP List	Enter the DSCP list value to map to the CoS value here. The range is from 0 to 63.

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

7.2.4 CoS Color Mapping

This window is used to configure and display the CoS color mapping settings.

Click **QoS > Advanced Settings > CoS Color Mapping** to view the following window:

Port	Color	CoS List
Gi1/0/1	Green	0-7
	Yellow	
	Red	
Gi1/0/2	Green	0-7
	Yellow	
	Red	
Gi1/0/3	Green	0-7
	Yellow	
	Red	
Gi1/0/4	Green	0-7
	Yellow	
	Red	

Figure 7-10 CoS Color Mapping

The following parameters can be configured in the **CoS Color Mapping** 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.
CoS List	Enter the CoS value that will be mapped to the color. The range is from 0 to 7.
Color	Select the color option that will be mapped to the CoS value. Options to choose from are Green , Yellow , and Red .

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

7.2.5 DSCP Color Mapping

This window is used to configure and display the DSCP color mapping settings.

Click **QoS > Advanced Settings > DSCP Color Mapping** to view the following window:

Port	Color	DSCP List
Gi1/0/1	Green	0-63
	Yellow	
	Red	
Gi1/0/2	Green	0-63
	Yellow	
	Red	
Gi1/0/3	Green	0-63
	Yellow	
	Red	
Gi1/0/4	Green	0-63
	Yellow	
	Red	

Figure 7-11 DSCP Color Mapping

The following parameters can be configured in the **DSCP Color Mapping** 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.
DSCP List	Enter the DSCP list value here that will be mapped to a color. The range is from 0 to 63.
Color	Select the color option that will be mapped to the DSCP value. Options to choose from are Green , Yellow , and Red .

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

7.2.6 Class Map

This window is used to configure and display the class map settings.

Click **QoS > Advanced Settings > Class Map** to view the following window:

Figure 7-12 Class Map

The following parameters can be configured:

Parameter	Description
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.
Multiple Match Criteria	Select the multiple match criteria option here. Options to choose from are Match All and Match Any .

Click the **Apply** button to add a new entry.

Click the **Match** button to configure the match rule settings for the specified 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.

Click the **Match** button to view the following window:

Figure 7-13 Class Map (Match)

The following parameters can be configured:

Parameter	Description
None	Select this option to match nothing to this class map.
Specify	Select the option to match something to this class map.
ACL Name	Select and enter the access list name that will be matched with this class map here. This name can be up to 32 characters long.
CoS List	Select and enter the CoS list value that will be matched with this class map here. The range is from 0 to 7.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. The range is from 0 to 63. Tick the IPv4 only option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. The range is from 0 to 7. Tick the IPv4 only option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are ARP, BGP, DHCP, DNS, EGP, FTP, IPv4, IPv6, NetBIOS, NFS, NTP, OSPF, PPPOE, RIP, RTSP, SSH, Telnet, and TFTP .
VID List	Select and enter the VLAN ID(s) that will be matched with the class map here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

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

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

7.2.7 Aggregate Policer

This window is used to configure and display the aggregate policer settings.

Click **QoS > Advanced Settings > Aggregate Policer** to view the following window:

The screenshot shows the 'Aggregate Policer' configuration window with the 'Single Rate Settings' tab selected. The window contains several input fields and dropdown menus for configuring policer parameters. Below the configuration fields is a table showing the current entry.

Total Entries: 1							
Name	Average Rate	Normal Burst Size	Max. Burst Size	Conform Action	Exceed Action	Violate Action	Color Aware
Name	12000	10000		Transmit	Transmit		Disabled

Figure 7-14 Aggregate Policer (Single Rate Settings)

The following parameters can be configured in the **Single Rate Settings** section:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer name here.
Average Rate	Enter the average rate value here. The range is from 0 to 10000000 kbps.
Normal Burst Size	Enter the normal burst size value here. The range is from 0 to 16384 Kbytes.
Maximum Burst Size	Enter the maximum burst size value here. The range is from 0 to 16384 Kbytes.

Parameter	Description
Confirm Action	<p>Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to Transmit. Options to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Exceed Action	<p>Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is Drop. Options to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.

Parameter	Description
Violate Action	<p>Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for single rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are:</p> <ul style="list-style-type: none"> • None - Specifies that no action will be taken. • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Color Aware	<p>Select to enable or disable the color aware feature here.</p> <ul style="list-style-type: none"> • When color aware is Enabled, the policer works in the color aware mode. • When color aware is Disabled, the policer works in the color blind mode.

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.

Click the **Two Rate Settings** tab to view the following window:

Aggregate Policer

Single Rate Settings **Two Rate Settings**

Aggregate Policer Name:

CIR * (0-10000000): Kbps

PIR * (0-10000000): Kbps

Conform Action: DSCP IP

Violate Action: DSCP IP

* Mandatory Field

Confirm Burst (0-16384): Kbyte

Peak Burst (0-16384): Kbyte

Exceed Action: DSCP IP

Color Aware:

Apply

Total Entries: 1

Name	CIR	Confirm Burst	PIR	Peak Burst	Conform Action	Exceed Action	Violate Action	Color Aware
Name	12000	10000	12000	16000	Transmit	Drop	Drop	Disabled

1/1 1 Go

Figure 7-15 Aggregate Policer (Two Rate Settings)

The following parameters can be configured in the **Two Rate Settings** section:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer name here.
CIR	Enter the Committed Information Rate (CIR) value here. The range is from 0 to 10000000 kbps. The committed packet rate is the first token bucket for the two-rate metering.
Confirm Burst	Enter the confirm burst value here. The range is from 0 to 16384 Kbytes. The confirm burst value specifies the burst size for the first token bucket in kbps.
PIR	Enter the Peak Information Rate (PIR) value here. The range is from 0 to 10000000 kbps. The peak information rate is the second token bucket for the two-rate metering.
Peak Burst	Enter the peak burst value here. The range is from 0 to 16384 Kbytes. The peak burst value is the burst size for the second token bucket in kilobytes.

Parameter	Description
Confirm Action	<p>Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to Transmit. Options to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Exceed Action	<p>Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is Drop. Options to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.

Parameter	Description
Violate Action	<p>Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for single rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR.</p> <ul style="list-style-type: none"> For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. <p>Options to choose from are:</p> <ul style="list-style-type: none"> Drop - Specifies that the packet will be dropped. Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. Transmit - Specifies that the packet will be transmitted unaltered. Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Color Aware	<p>Select to enable or disable the color aware feature here.</p> <ul style="list-style-type: none"> When color aware is Enabled, the policer works in the color-aware mode. When color aware is Disabled, the policer works in the color-blind mode.

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.

7.2.8 Policy Map

This window is used to configure and display the policy map settings.

Click **QoS > Advanced Settings > Policy Map** to view the following window:

Figure 7-16 Policy Map

The following parameters can be configured in the **Create/Delete Policy Map** section:

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

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.

The following parameters can be configured in the **Traffic Policy** section:

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

Click the **Apply** button to add a new entry.

Click the **Set Action** button to configure the set action settings for the specified entry.

Click the **Policer** button to configure the police action settings for the specified 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.

Click the **Set Action** button to view the following window:

Figure 7-17 Policy Map (Set Action)

The following parameters can be configured in the **Set Action** section:

Parameter	Description
None	Select this option to specify that no action will be taken.
Specify	Select this option to specify that action will be taken based on the configurations made.
New Precedence	Select the new precedence value for the packet here. The range is from 0 to 7. Select the IPv4 only option to specify that IPv4 precedence will be marked only. If not selected, then both IPv4 and IPv6 precedence will be marked. For IPv6 packets, the precedence is the most three significant bits of the traffic class of the IPv6 header.
New DSCP	Select the new DSCP value for the packet here. The range is from 0 to 63. Select the IPv4 only option to specify that the IPv4 DSCP will be marked only. If not selected, then both the IPv4 and IPv6 DSCP will be marked.
New CoS	Select the new CoS value to the packet here. The range is from 0 to 7.
New Cos Queue	Select the new CoS queue value to the packets here. This will overwrite the original CoS queue selection. Setting the CoS queue will not take effect if the policy map is applied for the egress flow on the interface.

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

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

Click the **Policer** button and specify the police action as **Police** to view the following window:

Figure 7-18 Policy Map (Policer, Police)

The following parameters can be configured in the **Police Action** section:

Parameter	Description
None	Select this option to specify that no policer settings will be configured for this entry.
Specify	Select this option to specify that the following policer settings will be applied to this entry.
Average Rate	Enter the average rate value here. The range is from 0 to 10000000 Kbps.
Normal Burst Size	Enter the normal burst size value here. The range is from 0 to 16384 Kbps.
Maximum Burst Size	Enter the maximum burst size value here. The range is from 0 to 16384 Kbps.
Conform Action	<p>Select the conform action that will be taken here. This action will be taken on green color packets. Option to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.

Parameter	Description
Exceed Action	<p>Select the exceed action that will be taken here. This action will be taken on yellow color packets that exceed the rate limit. Option to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Violate Action	<p>Select the violate action that will be taken here. This action will be taken on red color packets. Option to choose from are:</p> <ul style="list-style-type: none"> • None - Specifies that no violate action will be taken. • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Color Aware	<p>Select to enable or disable the color aware feature here.</p> <ul style="list-style-type: none"> • When Enabled, the policer works in the color-aware mode. • When Disabled, the policer works in the color-blind mode.

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

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

Click the **Policer** button and specify the police action as **Police CIR** to view the following window:

Figure 7-19 Policy Map (Policer, Police CIR)

The following parameters can be configured in the **Police Action** section:

Parameter	Description
None	Select this option to specify that no policer settings will be configured for this entry.
Specify	Select this option to specify that the following policer settings will be applied to this entry.
CIR	Enter the Committed Information Rate (CIR) value here. This is the first token bucket for two-rate metering. The range is from 0 to 10000000 kbps.
Confirm Burst	Enter the confirm burst value here. This is the size of the first token bucket. The range is from 0 to 16384 kilobytes.
PIR	Enter the Peak Information Rate (PIR) value here. This is the second token bucket for two-rate metering. The range is from 0 to 10000000.
Peak Burst	Enter the peak burst value here. This is the size of the second token bucket. The range is from 0 to 16384 kilobytes.

Parameter	Description
Conform Action	<p>Select the conform action that will be taken here. This action will be taken on green color packets. Option to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Exceed Action	<p>Select the exceed action that will be taken here. This action will be taken on yellow color packets that exceed the rate limit. Option to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.

Parameter	Description
Violate Action	<p>Select the violate action that will be taken here. This action will be taken on red color packets. Option to choose from are:</p> <ul style="list-style-type: none"> • None - Specifies that no violate action will be taken. • Drop - Specifies that the packet will be dropped. • Set-DSCP-Transmit - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • Set-1P-Transmit - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • Transmit - Specifies that the packet will be transmitted unaltered. • Set-DSCP-1P - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Color Aware	<p>Select to enable or disable the color aware feature here.</p> <ul style="list-style-type: none"> • When Enabled, the policer works in the color-aware mode. • When Disabled, the policer works in the color-blind mode.

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

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

Click the **Policer** button and specify the police action as **Police Aggregate** to view the following window:

Figure 7-20 Policy Map (Policer, Police Aggregate)

The following parameters can be configured in the **Police Action** section:

Parameter	Description
None	Select this option to specify that no policer settings will be configured for this entry.
Specify	Select this option to specify that the following policer settings will be applied to this entry.

Parameter	Description
Aggregate Policer Name	Enter the name for the aggregate policing rule here. This can be up to 32 characters long.

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

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

7.2.9 Policy Binding

This window is used to configure and display the policy binding settings.

Click **QoS > Advanced Settings > Policy Binding** to view the following window:

Port	Direction	Policy Map Name
Gi1/0/1		
Gi1/0/2		
Gi1/0/3		
Gi1/0/4		
Gi1/0/5		
Gi1/0/6		
Gi1/0/7		
Gi1/0/8		
Gi1/0/9		
Gi1/0/10		

Figure 7-21 Policy Binding

The following parameters can be configured in the **Policy Binding Setting** 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.
Direction	Select the direction option here. Options to choose from are Input and Output . Input specified ingress traffic and output specifies egress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. <ul style="list-style-type: none"> Select the None option not to tie a policy map to this entry.

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

7.3 WRED (Weighted Random Early Detection)

7.3.1 WRED Profile

This window is used to configure and display the WRED profile settings.

Click **QoS > WRED > WRED Profile** to view the following window:

WRED Profile	Packet Type	Min Threshold	Max Threshold	Max Drop Rate
1	TCP-GREEN	20	80	0
	TCP-YELLOW	20	80	0
	TCP-RED	20	80	0
	NON-TCP-GREEN	20	80	0
	NON-TCP-YELLOW	20	80	0
	NON-TCP-RED	20	80	0
2	TCP-GREEN	20	80	0
	TCP-YELLOW	20	80	0
	TCP-RED	20	80	0
	NON-TCP-GREEN	20	80	0
	NON-TCP-YELLOW	20	80	0
	NON-TCP-RED	20	80	0

Figure 7-22 WRED Profile

The following parameters can be configured in the **WRED Profile** section:

Parameter	Description
Profile	Enter the WRED profile ID here. The range is from 1 to 128.
Packet Type	Select the packet type here. Options to choose from are: <ul style="list-style-type: none"> TCP - Specifies the WRED drop parameters for the TCP packets to be set. Non-TCP - Specifies the WRED drop parameters for non-TCP packets to be set.
Packet Color	Select the packet color here. Options to choose from are: <ul style="list-style-type: none"> Green - Specifies the WRED drop parameters for green packets to be set. Yellow - Specifies the WRED drop parameters for yellow packets to be set. Red - Specifies the WRED drop parameters for red packets to be set.
Min Threshold	Enter the minimum threshold value here that will be used to start WRED dropping. The range is from 0 to 100.

Parameter	Description
Max Threshold	Enter the maximum threshold value here over which WRED will drop all packets destined for this queue. The range is from 0 to 100.
Max Drop Rate	Enter the maximum drop-rate value here. The range is from 0 to 14. This feature specifies the drop probability when the average queue size reaches the maximum threshold. When this value is zero, then the packet will not be dropped or remarked for ECN.

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

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Reset Configuration** button to reset the configuration for the specified entry.

7.3.2 WRED Queue

This window is used to configure and display the WRED queue settings.

Click **QoS > WRED > WRED Queue** to view the following window:

Unit	From Port	To Port	CoS	WRED State	Profile (1-128)	Weight (0-15)
1	Gi1/0/1	Gi1/0/1	0	Disabled		9

Port	CoS	WRED State	Exp-weight-constant	Profile
Gi1/0/1	0	Disabled	9	1
	1	Disabled	9	1
	2	Disabled	9	1
	3	Disabled	9	1
	4	Disabled	9	1
	5	Disabled	9	1
	6	Disabled	9	1
	7	Disabled	9	1
Gi1/0/2	0	Disabled	9	1
	1	Disabled	9	1
	2	Disabled	9	1
	3	Disabled	9	1
	4	Disabled	9	1
	5	Disabled	9	1
	6	Disabled	9	1
	7	Disabled	9	1

Figure 7-23 WRED Queue

The following parameters can be configured in the **WRED Queue** 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.
CoS	Select the CoS value here. The range is from 0 to 7.
WRED State	Select to enable or disable the WRED feature state on the specified port(s) here.
Profile	Enter the WRED profile ID here. The range is from 1 to 128.
Weight	Enter the exponential weight value here. The range is from 0 to 15. This feature is used to configure the WRED exponential weight factor for the average queue size calculation for the queue.

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

7.4 Egress Buffer Settings

Use the following window to configure the threshold of output buffering and display the threshold specified. Regarding the threshold of output buffering, operating with the default configuration is recommended. Egress Buffer changes the status to "High" regarding the environment where the traffics instantaneously exceeding the maximum quantity of communications for a port occur frequently.

Choose **QoS > Egress Buffer Settings** to display the following window.

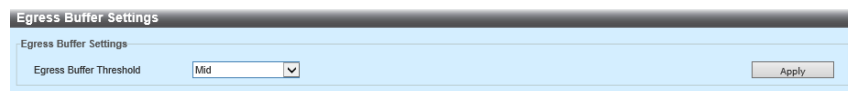


Figure 7-24 Egress Buffer Settings

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

Parameter	Overview
Threshold Settings for Egress Buffer	Choose the threshold of an output buffering. The options (values) available are Mid and High . If the value is configured in advance, the threshold is displayed. The default (or initial) value is Mid .

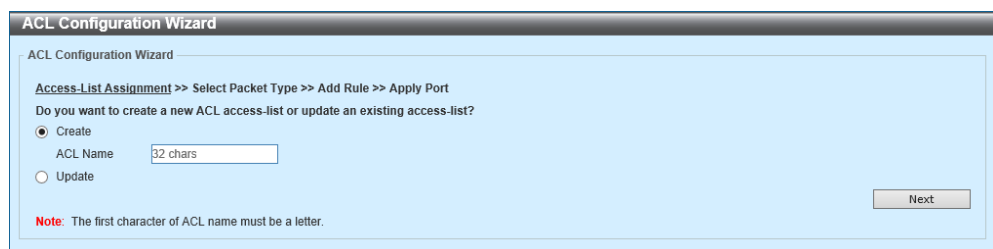
Click **Apply** to reflect the change.

8 ACL (Access Control List)

8.1 ACL Configuration Wizard

This window is used to configure new and existing ACLs using the ACL Configuration Wizard.

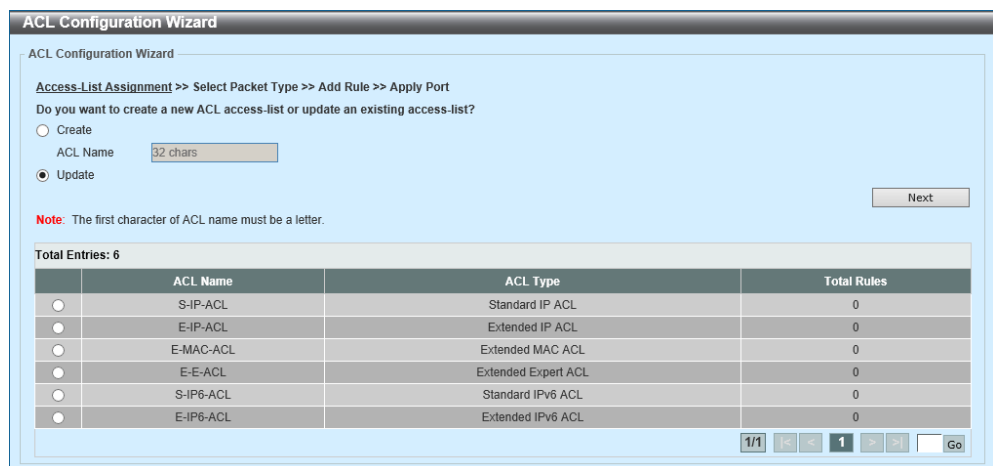
Click **ACL > ACL Configuration Wizard** to view the following window:



The screenshot shows the 'ACL Configuration Wizard' window in the 'Create' mode. The title bar reads 'ACL Configuration Wizard'. Below the title bar, the breadcrumb path is 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port'. The main question is 'Do you want to create a new ACL access-list or update an existing access-list?'. The 'Create' radio button is selected. There is a text field for 'ACL Name' with a '32 chars' limit. The 'Update' radio button is unselected. A 'Next' button is on the right. A red note at the bottom states: 'Note: The first character of ACL name must be a letter.'

Figure 8-1 ACL Configuration Wizard (Create)

Click the **Update** option to view the following window:



The screenshot shows the 'ACL Configuration Wizard' window in the 'Update' mode. The title bar reads 'ACL Configuration Wizard'. Below the title bar, the breadcrumb path is 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port'. The main question is 'Do you want to create a new ACL access-list or update an existing access-list?'. The 'Update' radio button is selected. There is a text field for 'ACL Name' with a '32 chars' limit. The 'Create' radio button is unselected. A 'Next' button is on the right. A red note at the bottom states: 'Note: The first character of ACL name must be a letter.'

Below the note, there is a table showing the total entries for various ACL types:

Total Entries: 6			
	ACL Name	ACL Type	Total Rules
<input type="radio"/>	S-IP-ACL	Standard IP ACL	0
<input type="radio"/>	E-IP-ACL	Extended IP ACL	0
<input type="radio"/>	E-MAC-ACL	Extended MAC ACL	0
<input type="radio"/>	E-E-ACL	Extended Expert ACL	0
<input type="radio"/>	S-IP6-ACL	Standard IPv6 ACL	0
<input type="radio"/>	E-IP6-ACL	Extended IPv6 ACL	0

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

Figure 8-2 ACL Configuration Wizard (Update)

The following parameters can be configured:

Parameter	Description
Create	Select this option to create a new ACL access list using the configuration wizard.
ACL Name	Enter the new ACL name here. This name can be up to 32 characters long.
Update	Select this option to update an existing ACL access list. Select the existing ACL in the table to process with the update.

Click the **Next** button to proceed to the next step in the wizard.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After select to **Create** an ACL and clicking the **Next** button, the following window will be displayed:

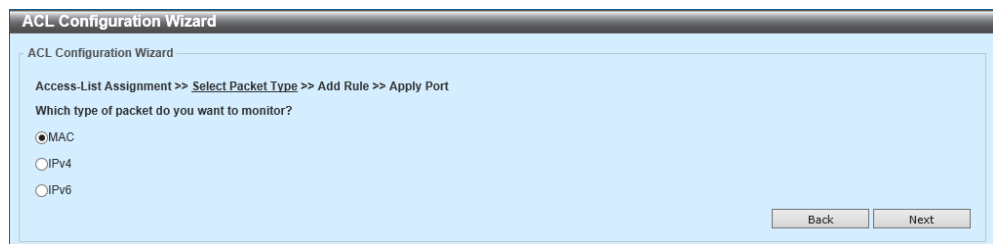


Figure 8-3 ACL Configuration Wizard (Select ACL Type)

The following parameters can be configured:

Parameter	Description
MAC	Select this option to create a MAC ACL.
IPv4	Select this option to create an IPv4 ACL.
IPv6	Select this option to create an IPv6 ACL.

Click the **Next** button to proceed to the next step in the wizard.
Click the **Back** button to return to the previous step in the wizard.

8.1.1 MAC ACL

After selecting to **Create/Update** a **MAC ACL**, the following window will be displayed:

Figure 8-4 ACL Configuration Wizard (Configure MAC ACL)

The following parameters can be configured:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select Auto Assign to generate an ACL rule number automatically for this entry.
Source	Select and enter the source MAC address information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Specifies that any source traffic will be evaluated according to the conditions of this rule. • Host - Enter the source host MAC address here. • MAC - Enter the source MAC address and Wildcard value in the spaces provided.
Destination	Select and enter the destination MAC address information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • Host - Enter the destination host MAC address here. • MAC - Enter the destination MAC address and Wildcard value in the spaces provided.

Parameter	Description
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are aarp , appletalk , decent-iv , etype-6000 , etype-8042 , lat , lvc-sca , mop-console , mop-dump , vines-echo , vines-ip , xns-idp , and arp .
Ethernet Type	Enter the Ethernet type hexadecimal value here. The range is from 0x600 to 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. The range is from 0x0 to 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from 0 to 7. <ul style="list-style-type: none"> Mask - Enter the CoS mask value here. The range is from 0x0 to 0x7.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. <ul style="list-style-type: none"> Mask - Enter the VLAN ID mask value here. The range is from 0x0 to 0xFF.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit, Deny and Deny CPU.

Click the **Next** button to proceed to the next step in the wizard.

Click the **Back** button to return to the previous step in the wizard.

After clicking the **Next** button (in the previous step), the following window will be displayed:

Figure 8-5 ACL Configuration Wizard (Select Ports and Direction)

The following parameters can be configured:

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.
Direction	Select the direction here. Options to choose from are In and Out.

Click the **Apply** button to accept the changes made and return to the **ACL Configuration Wizard** window.

Click the **Back** button to return to the previous step in the wizard.

8.1.2 IPv4

After selecting to **Update** a **Standard IP ACL**, the following window will be displayed:

The screenshot shows the 'ACL Configuration Wizard' window for configuring a Standard IP ACL. The title bar reads 'ACL Configuration Wizard'. Inside, the breadcrumb path is 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port'. Below this, it says 'Please assign a sequence number to create a new rule.' with two radio buttons: 'Sequence No. (1-65535)' (selected) and 'Auto Assign'. A text box for the sequence number is present. The 'Assign Rule Criteria' section has a tab labeled 'IPv4 Address'. Under this tab, there are two columns for 'Source' and 'Destination'. Each column has three radio buttons: 'Any' (selected), 'Host', and 'IP'. Below these are text boxes for 'Wildcard'. At the bottom left, there is a 'Time Range' text box with '32 chars' and an 'Action' section with 'Permit' (selected) and 'Deny' radio buttons. 'Back' and 'Next' buttons are at the bottom right.

Figure 8-6 ACL Configuration Wizard (Configure Standard IP ACL)

After selecting to **Update** an **Extended IP ACL** or to **Create** an **IPv4 ACL**, the following window will be displayed:

The screenshot shows the 'ACL Configuration Wizard' window for configuring an Extended IP ACL. The title bar reads 'ACL Configuration Wizard'. The breadcrumb path is 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port'. It says 'Please assign a sequence number to create a new rule.' with 'Sequence No. (1-65535)' (selected) and 'Auto Assign' radio buttons. Below is the 'Protocol Type' dropdown set to 'TCP', followed by a port range '(0-255)' and a 'Mask (0x0-0xFF)' text box. There is also a 'Fragments' checkbox. The 'Assign Rule Criteria' section has four tabs: 'IPv4 Address', 'Port', 'IPv4 DSCP', and 'TCP Flag'. The 'IPv4 Address' tab is active. It has 'Source' and 'Destination' columns with 'Any' (selected), 'Host', and 'IP' radio buttons, and 'Wildcard' text boxes. The 'Port' section has 'Source Port' and 'Destination Port' dropdowns, each followed by a port range '(0-65535)'. The 'IPv4 DSCP' section has 'IP Precedence' (selected) and 'ToS' radio buttons, each followed by a 'Value' dropdown and a 'Mask (0x0-0xF)' text box. The 'TCP Flag' section has checkboxes for 'ack', 'fin', 'psh', 'rst', 'syn', and 'urg'. At the bottom left, there is a 'Time Range' text box with '32 chars' and an 'Action' section with 'Permit' (selected) and 'Deny' radio buttons. 'Back' and 'Next' buttons are at the bottom right.

Figure 8-7 ACL Configuration Wizard (Configure Extended IP ACL)

The following parameters can be configured:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select Auto Assign to generate an ACL rule number automatically for this entry.
Protocol Type	<p>Select the protocol type option here. Options to choose from 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 - The protocol ID can also manually be entered here. 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 to include packet fragment filtering.
Source	<p>Select and enter the source information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any source traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter a source host IP address here. • IP - Specifies to use and enter a group of source IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	<p>Select and enter the destination information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter a destination host IP address here. • IP - Specifies to use and enter a group of destination IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.

Parameter	Description
Source Port	<p>Select and enter the source port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>
Destination Port	<p>Select and enter the destination port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available when ICMP is selected 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 the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available when ICMP is selected as the Protocol Type.</p>

Parameter	Description
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available when ICMP is selected as the Protocol Type .
IP Precedence	Select the IP precedence value used here. Options to choose from 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 - The IP precedence value can also manually be entered here. The range is from 0 to 7. • Mask - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.
ToS	Select the Type-of-Service (ToS) value that will be used here. Options to choose from are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4), and min-delay (8). <ul style="list-style-type: none"> • Value - The ToS value can also manually be entered here. The range is from 0 to 15. • Mask - Enter the ToS mask value here. The range is from 0x0 to 0xF.
DSCP	Select the DSCP value that will be used here. Options to choose from 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 - The DSCP value can also manually be entered here. The range is from 0 to 63. • Mask - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
TCP Flag	Select the TCP flag that will be evaluated in this ACL here. Options to choose from are ack , fin , psh , rst , syn , and urg . This parameter is only available when TCP is selected as the Protocol Type .
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

Click the **Next** button to proceed to the next step in the wizard.

Click the **Back** button to return to the previous step in the wizard.

After clicking the **Next** button (in the previous step), the following window will be displayed:

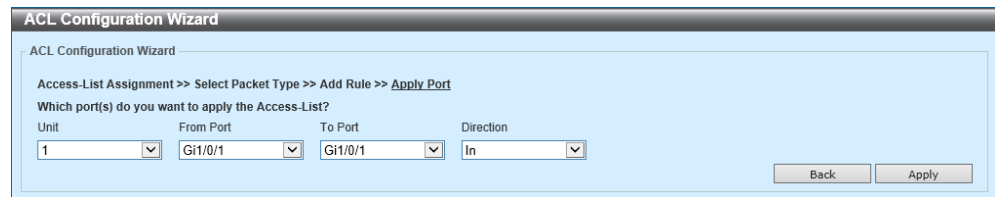


Figure 8-8 ACL Configuration Wizard (IPv4, Step 3)

The following parameters can be configured:

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.
Direction	Select the direction here. Options to choose from are In and Out.

Click the **Apply** button to accept the changes made and return to the ACL Configuration Wizard window.

Click the **Back** button to return to the previous step in the wizard.

8.1.3 IPv6

After selecting to **Update** a **Standard IPv6 ACL**, the following window will be 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

IPv6 Address

IPv6 Address

☒ Any ☐ Host ☐ Any ☐ Host

Source ☐ IPv6 Destination ☐ IPv6

Prefix Length Prefix Length

Time Range

Action ☒ Permit ☐ Deny

Back Next

Figure 8-9 ACL Configuration Wizard (Configure Standard IPv6 ACL)

After selecting to **Update** an **Extended IPv6 ACL** or to **Create** an **IPv6 ACL**, the following window will be 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

Protocol Type (0-255) Mask (0x0-0xFF) ☐ Fragments

Assign Rule Criteria

IPv6 Address **Port** **IPv6 DSCP** **TCP Flag** **Flow Label**

IPv6 Address

☒ Any ☐ Host ☐ Any ☐ Host

Source ☐ IPv6 Destination ☐ IPv6

Prefix Length Prefix Length

Port

Source Port (0-65535) (0-65535)

Destination Port (0-65535) (0-65535)

IPv6 DSCP

☒ DSCP (0-63) Mask (0x0-0x3F)

☐ Traffic Class (0-255) Mask (0x0-0xFF)

TCP Flag

TCP Flag ☐ ack ☐ fin ☐ psh ☐ rst ☐ syn ☐ urg

Flow Label

Flow Label (0-1048575) Mask (0x0-0xFFFF)

Time Range

Action ☒ Permit ☐ Deny

Back Next

Figure 8-10 ACL Configuration Wizard (Configure Extended IPv6 ACL)

The following parameters can be configured:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select Auto Assign to generate an ACL rule number automatically for this entry.
Protocol Type	<p>Select the protocol type option here. Options to choose from 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 here. 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 to include packet fragment filtering.
Source	<p>Select and enter the source information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any source traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter the source host IPv6 address here. • IPv6 - Specifies to use and enter the source IPv6 address and Prefix Length value in the spaces provided.
Destination	<p>Select and enter the destination information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter the destination host IPv6 address here. • IPv6 - Specifies to use and enter the destination IPv6 address and Prefix Length value in the spaces provided.

Parameter	Description
Source Port	<p>Select and enter the source port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>
Destination Port	<p>Select and enter the destination port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available when ICMP is selected 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 the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available when ICMP is selected as the Protocol Type.</p>

Parameter	Description
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available when ICMP is selected as the Protocol Type .
DSCP	Select the DSCP value that will be used here. Options to choose from 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 - The DSCP value can also manually be entered here. The range is from 0 to 63. • Mask - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
Traffic Class	Select and enter the traffic class value here. The range is from 0 to 255. <ul style="list-style-type: none"> • Mask - Enter the traffic class mask value here. The range is from 0x0 to 0xFF.
TCP Flag	Select the TCP flag that will be evaluated in this ACL here. Options to choose from are ack , fin , psh , rst , syn , and urg . This parameter is only available when TCP is selected as the Protocol Type .
Flow Label	Enter the flow label value here. The range is from 0 to 1048575. <ul style="list-style-type: none"> • Mask - Enter the flow label mask here. The range is from 0x0 to 0xFFFFF.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

Click the **Next** button to proceed to the next step in the wizard.

Click the **Back** button to return to the previous step in the wizard.

After clicking the **Next** button (in the previous step), the following window will be displayed:

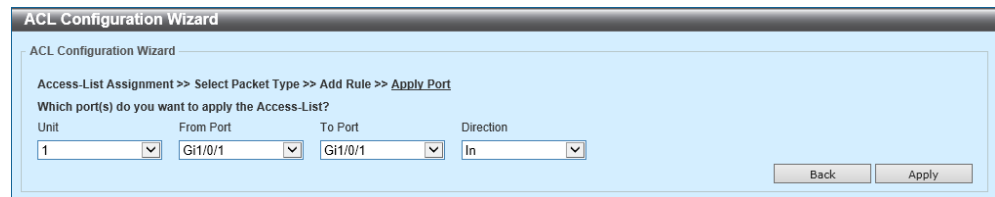


Figure 8-11 ACL Configuration Wizard (IPv6, Step 3)

The following parameters can be configured:

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.
Direction	Select the direction here. Options to choose from are In and Out.

Click the **Apply** button to accept the changes made and return to the ACL Configuration Wizard window.

Click the **Back** button to return to the previous step in the wizard.

8.2 ACL Access List

This window is used to configure and display the ACLs, ACL rules and settings.

Click **ACL > ACL Access List** to view the following window:

Figure 8-12 ACL Access List

The following parameters can be configured in the **ACL Access List** section:

Parameter	Description
ACL Type	Select the ACL type to find here. Options to choose from are All , IP ACL , IPv6 ACL , MAC ACL , and Expert ACL .
ID	Select and enter the access list ID here. The range is from 1 to 14999.
ACL Name	Select and enter the access list name here. This name can be up to 32 characters long.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Add ACL** button to add a new ACL profile entry.

Click the **Edit** button to edit the settings of the specified entry.

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

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

Click the **Clear Counter** button to clear the counter information related to the selected ACL profile.

Click the **Add Rule** button to add a new ACL rule entry for the selected ACL profile.

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

Click **Edit** button to view the following window:

ACL Access List

ACL Type: ☒ ID (1-14999) ☐ ACL Name

Total Entries: 6

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	S-IP-ACL	Standard IP ACL	10	10	Disabled		Apply	Delete
2000	E-IP-ACL	Extended IP ACL	10	10	Disabled		Edit	Delete
6000	E-MAC-ACL	Extended MAC ACL	10	10	Disabled		Edit	Delete
8000	E-E-ACL	Extended Expert ACL	10	10	Disabled		Edit	Delete
11000	S-IP6-ACL	Standard IPv6 ACL	10	10	Disabled		Edit	Delete
13000	E-IP6-ACL	Extended IPv6 ACL	10	10	Disabled		Edit	Delete

1/1 < < 1 > > Go

S-IP-ACL (ID: 1) Rule

Sequence No.	Action	Rule	Time Range	Counter	
10	Permit	any any			Delete

1/1 < < 1 > > Go

Figure 8-13 ACL Access List (Edit)

The following parameters can be configured in the **ACL Access List** section:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number step here. The step range is from 1 to 32. This specifies the number that the sequence numbers step. The default value is 10. For example, if the increment (step) value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this ACL here.

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

8.2.1 Standard IP ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

The screenshot shows a window titled "Add ACL Access List". Inside, there's a section "Add ACL Access List" with three input fields: "ACL Type" with a dropdown menu showing "Standard IP ACL", "ID (1-1999)" with a text box, and "ACL Name" with a text box labeled "32 chars". Below these fields is a red note: "Note: The first character of ACL name must be a letter." At the bottom right is an "Apply" button.

Figure 8-14 ACL Access List (Add ACL, Standard IP ACL)

The following parameters can be configured in the **Add ACL Access List** section:

Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL , and Extended Expert ACL . This section discusses how the Standard IP ACL .
ID	Enter the ID for the Standard IP ACL here. The range is from 1 to 1999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

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

Select a **Standard IP ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

The screenshot shows a window titled "Add ACL Rule". Inside, there's a section "Add ACL Rule" with several fields: "ID" (1), "ACL Name" (S-IP-ACL), "ACL Type" (Standard IP ACL), "Sequence No. (1-65535)" (with a note "(If it isn't specified, the system automatically assigns.)"), "Action" (radio buttons for Permit and Deny), "Match IP Address" (radio buttons for Any, Host, IP, and Wildcard for both Source and Destination), and "Time Range" (32 chars). At the bottom right are "Back" and "Apply" buttons.

Figure 8-15 ACL Access List (Add Rule, Standard IP ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source information here. Options to choose from are: <ul style="list-style-type: none">• Any - Specifies that any source traffic will be evaluated according to the conditions of this rule.• Host - Specifies to use and enter a source host IP address here.• IP - Specifies to use and enter a group of source IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: <ul style="list-style-type: none">• Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule.• Host - Specifies to use and enter a destination host IP address here.• IP - Specifies to use and enter a group of destination IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to add the new ACL rule.

Click the **Back** button to return to ACL Access List window.

8.2.2 Extended IP ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

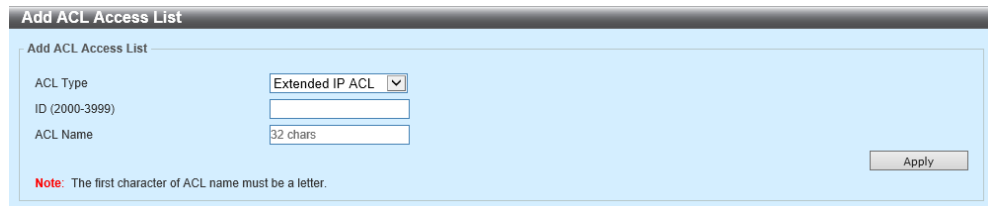


Figure 8-16 ACL Access List (Add ACL, Extended IP ACL)

The following parameters can be configured in the **Add ACL Access List** section:

Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL , and Extended Expert ACL . This section discusses how the Extended IP ACL .
ID	Enter the ID for the Extended IP ACL here. The range is from 2000 to 3999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

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

Select an **Extended IP ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

Figure 8-17 ACL Access List (Add Rule, Extended IP ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	<p>Select the protocol type option here. Options to choose from 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 - The protocol ID can also manually be entered here. 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 to include packet fragment filtering.

Parameter	Description
Source	<p>Select and enter the source information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any source traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter a source host IP address here. • IP - Specifies to use and enter a group of source IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	<p>Select and enter the destination information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter a destination host IP address here. • IP - Specifies to use and enter a group of destination IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	<p>Select and enter the source port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>

Parameter	Description
Destination Port	<p>Select and enter the destination port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>
TCP Flag	<p>Select the TCP flag that will be evaluated in this ACL here. Options to choose from are ack, fin, psh, rst, syn, and urg.</p> <p>This parameter is only available when TCP is selected as the Protocol Type.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available when ICMP is selected 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 the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available when ICMP is selected as the Protocol Type.</p>
Message Code	<p>When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available when ICMP is selected as the Protocol Type.</p>
IP Precedence	<p>Select the IP precedence value used here. Options to choose from 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 - The IP precedence value can also manually be entered here. The range is from 0 to 7. • Mask - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.

Parameter	Description
ToS	<p>Select the Type-of-Service (ToS) value that will be used here. Options to choose from 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 - The ToS value can also manually be entered here. The range is from 0 to 15. • Mask - Enter the ToS mask value here. The range is from 0x0 to 0xF.
DSCP	<p>Select the DSCP value that will be used here. Options to choose from 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 also manually be entered here. The range is from 0 to 63. • Mask - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
Time Range	<p>Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.</p>

Click the **Apply** button to add the new ACL rule.

Click the **Back** button to return to ACL Access List window.

8.2.3 Standard IPv6 ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

Figure 8-18 ACL Access List (Add ACL, Standard IPv6 ACL)

The following parameters can be configured in the **Add ACL Access List** section:

Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL , and Extended Expert ACL . This section discusses how the Standard IPv6 ACL .
ID	Enter the ID for the Standard IPv6 ACL here. The range is from 11000 to 12999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

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

Select a **Standard IPv6 ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

Figure 8-19 ACL Access List (Add Rule, Standard IPv6 ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source information here. Options to choose from are: <ul style="list-style-type: none">• Any - Specifies that any source traffic will be evaluated according to the conditions of this rule.• Host - Specifies to use and enter the source host IPv6 address here.• IPv6 - Specifies to use and enter the source IPv6 address and Prefix Length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: <ul style="list-style-type: none">• Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule.• Host - Specifies to use and enter the destination host IPv6 address here.• IPv6 - Specifies to use and enter the destination IPv6 address and Prefix Length value in the spaces provided.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to add the new ACL rule.

Click the **Back** button to return to ACL Access List window.

8.2.4 Extended IPv6 ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

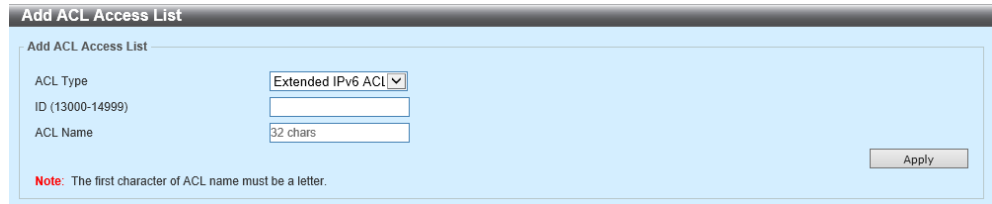


Figure 8-20 ACL Access List (Add ACL, Extended IPv6 ACL)

The following parameters can be configured in the **Add ACL Access List** section:

Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL , and Extended Expert ACL . This section discusses how the Extended IPv6 ACL .
ID	Enter the ID for the Extended IPv6 ACL here. The range is from 13000 to 14999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

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

Select an **Extended IPv6 ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

Figure 8-21 ACL Access List (Add Rule, Extended IPv6 ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , Protocol ID , ESP (50), PCP (108), SCTP (132), and None . <ul style="list-style-type: none"> Value - The protocol ID can also manually be entered here. 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 to include packet fragment filtering.

Parameter	Description
Source	<p>Select and enter the source information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any source traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter the source host IPv6 address here. • IPv6 - Specifies to use and enter the source IPv6 address and Prefix Length value in the spaces provided.
Destination	<p>Select and enter the destination information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter the destination host IPv6 address here. • IPv6 - Specifies to use and enter the destination IPv6 address and Prefix Length value in the spaces provided.
Source Port	<p>Select and enter the source port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>

Parameter	Description
Destination Port	<p>Select and enter the destination port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>
TCP Flag	<p>Select the TCP flag that will be evaluated in this ACL here. Options to choose from are ack, fin, psh, rst, syn, and urg.</p> <p>This parameter is only available when TCP is selected as the Protocol Type.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available when ICMP is selected 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 the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available when ICMP is selected as the Protocol Type.</p>
Message Code	<p>When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available when ICMP is selected as the Protocol Type.</p>

Parameter	Description
DSCP	<p>Select the DSCP value that will be used here. Options to choose from 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 also manually be entered here. The range is from 0 to 63. • Mask - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
Traffic Class	<p>Select and enter the traffic class value here. The range is from 0 to 255.</p> <ul style="list-style-type: none"> • Mask - Enter the traffic class mask value here. The range is from 0x0 to 0xFF.
Flow Label	<p>Enter the flow label value here. The range is from 0 to 1048575.</p> <ul style="list-style-type: none"> • Mask - Enter the flow label mask here. The range is from 0x0 to 0xFFFFF.
Time Range	<p>Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.</p>

Click the **Apply** button to add the new ACL rule.

Click the **Back** button to return to ACL Access List window.

8.2.5 Extended MAC ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

Add ACL Access List

Add ACL Access List

ACL Type: Extended MAC AC

ID (6000-7999):

ACL Name: 32 chars

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

Apply

Figure 8-22 ACL Access List (Add ACL, Extended MAC ACL)

The following parameters can be configured in the **Add ACL Access List** section:

Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL , and Extended Expert ACL . This section discusses how the Extended MAC ACL .
ID	Enter the ID for the Extended MAC ACL here. The range is from 6 to 7999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

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

Select an **Extended MAC ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

Add ACL Rule

Add ACL Rule

ID: 6000

ACL Name: E-MAC-ACL

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 ☐ MAC ☐ Wildcard

Destination: ☒ Any ☐ Host ☐ MAC ☐ Wildcard

Match Ethernet Type

Specify Ethernet Type: Please Select

Ethernet Type (0x0-0xFFFF):

Ethernet Type Mask (0x0-0xFFFF):

CoS: Please Select Mask (0x0-0x7):

VID(1-4094): Mask (0x0-0xFFFF):

Time Range: 32 chars

Back Apply

Figure 8-23 ACL Access List (Add Rule, Extended MAC ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source MAC address information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Specifies that any source traffic will be evaluated according to the conditions of this rule. • Host - Enter the source host MAC address here. • MAC - Enter the source MAC address and Wildcard value in the spaces provided.
Destination	Select and enter the destination MAC address information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • Host - Enter the destination host MAC address here. • MAC - Enter the destination MAC address and Wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are aarp , appletalk , decnet-iv , etype-6000 , etype-8042 , lat , lvc-sca , mop-console , mop-dump , vines-echo , vines-ip , xns-idp , and arp .
Ethernet Type	Enter the Ethernet type hexadecimal value here. The range is from 0x600 to 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. The range is from 0x0 to 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from 0 to 7. <ul style="list-style-type: none"> • Mask - Enter the CoS mask value here. The range is from 0x0 to 0x7.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. <ul style="list-style-type: none"> • Mask - Enter the VLAN ID mask value here. The range is from 0x0 to 0xFF.

Parameter	Description
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to add the new ACL rule.

Click the **Back** button to return to ACL Access List window.

8.2.6 Extended Expert ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

Figure 8-24 ACL Access List (Add ACL, Extended Expert ACL)

The following parameters can be configured in the **Add ACL Access List** section:

Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL , and Extended Expert ACL . This section discusses how the Extended Expert ACL .
ID	Enter the ID for the Extended Expert ACL here. The range is from 8000 to 9999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

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

Select an **Extended Expert ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

Figure 8-25 ACL Access List (Add Rule, Extended Expert ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	<p>Select the protocol type option here. Options to choose from 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 - The protocol ID can also manually be entered here. 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 to include packet fragment filtering.

Parameter	Description
Source (IP Address)	<p>Select and enter the source information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any source traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter a source host IP address here. • IP - Specifies to use and enter a group of source IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination (IP Address)	<p>Select and enter the destination information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • Host - Specifies to use and enter a destination host IP address here. • IP - Specifies to use and enter a group of destination IP addresses by using a Wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source (MAC Address)	<p>Select and enter the source MAC address information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any source traffic will be evaluated according to the conditions of this rule. • Host - Enter the source host MAC address here. • MAC - Enter the source MAC address and Wildcard value in the spaces provided.
Destination (MAC Address)	<p>Select and enter the destination MAC address information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • Host - Enter the destination host MAC address here. • MAC - Enter the destination MAC address and Wildcard value in the spaces provided.

Parameter	Description
Source Port	<p>Select and enter the source port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>
Destination Port	<p>Select and enter the destination port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The ACL will use the port number specified only. • > - The ACL will use all ports greater than the port number specified. • < - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • Range - The ACL will use the ports specified within the range. • Mask - The ACL will use 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. <p>This parameter is only available when TCP or UDP is selected as the Protocol Type.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available when ICMP is selected 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 the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available when ICMP is selected as the Protocol Type.</p>

Parameter	Description
Message Code	<p>When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available when ICMP is selected as the Protocol Type.</p>
IP Precedence	<p>Select the IP precedence value used here. Options to choose from 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 - The IP precedence value can also manually be entered here. The range is from 0 to 7. • Mask - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.
ToS	<p>Select the Type-of-Service (ToS) value that will be used here. Options to choose from 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 - The ToS value can also manually be entered here. The range is from 0 to 15. • Mask - Enter the ToS mask value here. The range is from 0x0 to 0xF.
DSCP	<p>Select the DSCP value that will be used here. Options to choose from 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 also manually be entered here. The range is from 0 to 63. • Mask - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
TCP Flag	<p>Select the TCP flag that will be evaluated in this ACL here. Options to choose from are ack, fin, psh, rst, syn, and urg.</p> <p>This parameter is only available when TCP is selected as the Protocol Type.</p>
VID	<p>Enter the VLAN ID that will be used here. The range is from 1 to 4094.</p> <ul style="list-style-type: none"> • Mask - Enter the VLAN ID mask value here. The range is from 0x0 to 0xFF.

Parameter	Description
CoS	Select the CoS value that will be used here. The range is from 0 to 7. <ul style="list-style-type: none">• Mask - Enter the CoS mask value here. The range is from 0x0 to 0x7.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to add the new ACL rule.

Click the **Back** button to return to ACL Access List window.

8.3 ACL Interface Access Group

This window is used to configure and display the ACL access group settings on the specified port(s).

Click **ACL > ACL Interface Access Group** to view the following window:

Port	In				Out			
	IP ACL	IPv6 ACL	MAC ACL	Expert ACL	IP ACL	IPv6 ACL	MAC ACL	Expert ACL
Gi1/0/1								
Gi1/0/2								
Gi1/0/3								
Gi1/0/4								
Gi1/0/5								
Gi1/0/6								
Gi1/0/7								
Gi1/0/8								
Gi1/0/9								
Gi1/0/10								

Figure 8-26 ACL Interface Access Group

The following parameters can be configured in the **ACL Interface Access Group** 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.
Direction	Select the direction here. Options to choose from are In and Out .
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the ACL type here. Options to choose from are IP ACL , IPv6 ACL , MAC ACL , and Expert ACL .
ACL Name	Enter the ACL name here. This name can be up to 32 characters long. Click the Please Select button to select an existing ACL from the list.

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

Click the **Please Select** button to display the configured access control lists that can be used in this window.

Click the **Please Select** button to view the following window:

The screenshot shows a window titled "ACL Access List". Inside, there's a section labeled "Total Entries: 2" above a table. The table has four columns: a selection column with radio buttons, "ID", "ACL Name", and "ACL Type".

	ID	ACL Name	ACL Type
<input type="radio"/>	1	S-IP-ACL	Standard IP ACL
<input checked="" type="radio"/>	2000	E-IP-ACL	Extended IP ACL

Below the table, there are pagination controls showing "1/1" and a "1" in a box, with navigation arrows. To the right is a "Go" button. At the bottom right of the window is an "OK" button.

Figure 8-27 ACL Interface Access Group (Please Select)

Click the **OK** button to use the selected access control list.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

8.4 ACL VLAN Access Map

This window is used to configure and display the ACL VLAN access map settings.

Click **ACL > ACL VLAN Access Map** to view the following window:

Figure 8-28 ACL VLAN Access Map

The following parameters can be configured in the **ACL VLAN Access Map** section:

Parameter	Description
Access Map Name	Enter the access map name here. This name can be up to 32 characters long.
Sub Map Number	Enter the sub-map number here. The range is from 1 to 65535.
Action	Select the action that will be taken here. Options to choose from are Forward , Drop , and Redirect . When the Redirect option is selected, select the redirected interface from the drop-down list.
Counter State	Select whether to enable or disable the counter state.

Click the **Apply** button to add a new entry.

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

Click the **Clear Counter** button to clear the counter information related to the specified access map.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Binding** button to configure the binding settings for the specified 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.

Click the **Binding** button to view the following window:

The 'Match Access-List' window displays the following configuration options:

- Access Map Name:** (Empty text field)
- Name:** 1
- Sub Map Number:** 1
- Match IP Access-List:** (Selected radio button, followed by a 'Please Select' button and 'Apply'/'Delete' buttons)
- Match IPv6 Access-List:** (Unselected radio button, followed by a 'Please Select' button and 'Apply'/'Delete' buttons)
- Match MAC Access-List:** (Unselected radio button, followed by a 'Please Select' button and 'Apply'/'Delete' buttons)

Figure 8-29 ACL VLAN Access Map (Binding)

The following parameters can be configured in the **Match Access List** section:

Parameter	Description
Match IP Access-List	Here the IP access list that will be matched will be displayed.
Match IPv6 Access-List	Here the IPv6 access list that will be matched will be displayed.
Match MAC Access-List	Here the MAC access list that will be matched will be displayed.

Click the **Please Select** button to display the configured access control lists that can be used in this window.

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

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

Click the **Please Select** button to view the following window:

The 'ACL Access List' window displays a table of ACL entries:

Total Entries: 2			
	ID	ACL Name	ACL Type
<input type="radio"/>	1	S-IP-ACL	Standard IP ACL
<input type="radio"/>	2000	E-IP-ACL	Extended IP ACL

Navigation controls at the bottom include a page indicator '1/1', navigation buttons, a page number '1', and a 'Go' button. An 'OK' button is located at the bottom right.

Figure 8-30 ACL VLAN Access Map (Binding, Please Select)

Click the **OK** button to use the selected access control list.

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

8.5 ACL VLAN Filter

This window is used to configure and display the ACL VLAN filter settings.

Click **ACL > ACL VLAN Filter** to view the following window:

Figure 8-31 ACL VLAN Filter

The following parameters can be configured in the **ACL VLAN Filter** section:

Parameter	Description
Access Map Name	Enter the access map name here. This name can be up to 32 characters long.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094. Select the All VLANs option to apply this configuration to all the VLANs configured on this Switch.

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 Security

9.1 Port Security

9.1.1 Port Security Global Settings

This window is used to configure and display the global port security settings.

Click **Security > Port Security > Port Security Global Settings** to view the following window:

VID	Max Learning Address	Current No.
1	No Limit	0

Figure 9-1 Port Security Global Settings

The following parameters can be configured in the **Port Security System Settings** section:

Parameter	Description
System Maximum Address	Enter the maximum number of secure MAC addresses allowed. If not specified, the default value is No Limit . The valid range is from 1 to 3328. Select No Limit to allow the maximum number of secure MAC address.

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

The following parameters can be configured in the **Port Security VLAN Settings** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
VLAN Max Learning Address	Enter the maximum number of allowed MAC addresses that can be learned on the specified VLAN(s) here. The range is from 1 to 3328. Select No Limit to allow the maximum number of secure MAC address.

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

The following parameters can be configured in the **Find VLAN** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries based on the search criteria specified.

9.1.2 Port Security Port Settings

This window is used to configure and display the port security settings on the specified port(s).

Click **Security > Port Security > Port Security Port Settings** to view the following window:

Port	Maximum	Current No.	Violation Action	Violation Count	Security Mode	Admin State	Current State	Aging Time	Aging Type
Gi1/0/1	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Gi1/0/2	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Gi1/0/3	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Gi1/0/4	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Gi1/0/5	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Gi1/0/6	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Gi1/0/7	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Gi1/0/8	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Gi1/0/9	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Gi1/0/10	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute

Figure 9-2 Port Security Port Settings

The following parameters can be configured in the **Port Security 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 port security feature on the port(s) specified.
Maximum	Enter the maximum number of secure MAC addresses that will be allowed on the port(s) specified. The range is from 0 to 3328. By default, this value is 32.
Violation Action	Select the violation action that will be taken here. Options to choose from are: <ul style="list-style-type: none"> • Protect - Specifies to drop all packets from insecure hosts at the port-security process level, but does not increment the security-violation count. • Restrict - Specifies to drop all packets from insecure hosts at the port-security process level and increments the security-violation count and record the system log. • Shutdown - Specifies to shut down the port if there is a security violation and record the system log.

Parameter	Description
Security Mode	Select the security mode option here. Options to choose from are: <ul style="list-style-type: none">• Permanent - Specifies that all learned MAC addresses will not be purged out unless the user manually deletes those entries.• Delete-on-Timeout - Specifies that all learned MAC addresses will be purged out when an entry is aged out or when the user manually deletes these entries.
Aging Time	Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. The range is from 0 to 1440 minutes.
Aging Type	Select the aging type here. Options to choose from are: <ul style="list-style-type: none">• Absolute - Specifies that all secure addresses on this port will age out, exactly after the time specified, and is removed from the secure address list. This is the default type.• Inactivity - Specifies that the secure addresses on this port age out only if there is no data traffic from the secure source address for the specified period.

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

9.1.3 Port Security Address Entries

This window is used to configure and display the MAC address entries for port security.

Click **Security > Port Security > Port Security Address Entries** to view the following window:

Figure 9-3 Port Security Address Entries

The following parameters can be configured in the **Port Security Address Entries** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
MAC Address	Enter the MAC address here. Select the Permanent option to specify that all learned MAC addresses will not be purged out unless the user manually deletes those entries.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Add** button to add a new entry.

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

Click the **Clear by Port** button to remove all the MAC addresses secured to the specified ports.

Click the **Clear by MAC** button to remove the specified MAC address secured to any of the ports.

Click the **Clear All** button to remove all the MAC addresses secured to ports.

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

9.2 802.1X

9.2.1 802.1X Global Settings

This window is used to configure and display the global IEEE 802.1X settings.

Click **Security > 802.1X > 802.1X Global Settings** to view the following window:

802.1X Global Settings

802.1X Global Settings

System Authentication Control: **Disabled** [Apply]

NAS ID: **nas1**

EAP Request Interval (1-3600): **5** sec [Apply]

802.1X Authentication Ports Settings

Authentication Ports Mode: **MAC-Based** Unit: **1** From Port: **Gi1/0/1** To Port: **Gi1/0/1** [Apply]

802.1X Port-Based Authentication Ports : Gi1/0/1-1/0/24,2/0/16,2/0/18-2/0/19,Te1/0/25-1/0/28,2/0/7-2/0/9,Gi2/0/1-2/0/6,2/0/11-2/0/15,2/0/17,2...

802.1X MAC-Based Authentication Ports:

Figure 9-4 802.1X Global Settings

The following parameters can be configured in the **802.1X Global Settings** section:

Parameter	Description
System Authentication Control	Select to enable or disable system authentication control here. This feature will restrict access to unauthorized hosts to the network.
NAS ID	Enter the ID of the Network Access Server (NAS) here.
EAP Request Interval	Enter the Extensible Authentication Protocol (EAP) request interval here. The range is from 1 to 3600 seconds.

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

The following parameters can be configured in the **802.1X Authentication Port Settings** section:

Parameter	Description
Authentication Ports Mode	Select the authentication mode that will be used on the specified port(s) here. Options to choose from are Port-Based and MAC-Based .
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.

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

9.2.2 802.1X Forced Authorized MAC Settings

This window is used to configure and display the IEEE 802.1X forced authorized MAC settings.

Click **Security > 802.1X > 802.1X Forced Authorized MAC Settings** to view the following window:

Figure 9-5 802.1X Forced Authorized MAC Settings

The following parameters can be configured in the **Forced Authorized MAC 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.
MAC Address	Enter the MAC address of the supplicant here.
Mask Length	Enter the MAC mask bit length here. The range is from 0 to 48.
Authentication Status	Select the authentication status here. Options to choose from are: <ul style="list-style-type: none"> Authorized - Select this option to force an authorized state. Unauthorized - Select this option to force an unauthorized state.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

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.

9.2.3 802.1X Unauthorized MAC Settings

This window is used to configure and display the IEEE 802.1X unauthorized MAC settings.

Click **Security > 802.1X > 802.1X Unauthorized MAC Settings** to view the following window:

Figure 9-6 802.1X Unauthorized MAC Settings

The following parameters can be configured in the **Unauthorized MAC Address Settings** section:

Parameter	Description
Age-Out Time	Enter the age-out time value here. This time is used in aging out static unauthorized hosts. The range is from 0 to 65535 seconds.
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.
MAC Address	Enter the MAC address of the unauthorized host here.
Find By MAC	Select this option to find and display configured and dynamic unauthorized hosts, sorted by MAC address.
Find By Port	Select to find and display configured and dynamic unauthorized hosts on the specified port(s). <ul style="list-style-type: none"> • 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.

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

Click the **Find** button to find and display entries based on the search criteria specified.

9.2.4 802.1X Port Settings

This window is used to configure and display the IEEE 802.1X port-based and MAC-based access control settings on the specified port(s).

Click **Security > 802.1X > 802.1X Port Settings** to view the following window:

The screenshot shows the '802.1X Ports Settings' window with the 'Port-Based Access Control' tab selected. The 'MAC-Based Access Control' tab is also visible. The configuration includes fields for Unit (1), From Port (Gi1/0/1), To Port (Gi1/0/1), Port Control (Force Authorized), AdminControlDirection (Both), Quiet Period (60 sec), Transmission Period (30 sec), Supplicant Timeout (30 sec), Server Timeout (30 sec), Re-authentication Period (3600 sec), Maximum Request (2), Per-Port Re-authentication (Disabled), and Re-authentication Time Local (Disabled). There are buttons for 'Apply', 'Show', 'Init', and 'Re-authenticate'. Below the configuration fields is a table showing the current settings for the selected port.

Total Entries: 1			
NAS ID	nas1	Port Number	Gi1/0/1
Re-authentication Timer Mode	RADIUS	Authorized MAC Address	---
Port Status	Authorized	OperControlDirection	Both
Port Control	Force Authorized	AdminControlDirection	Both
Quiet Period	60	Transmission Period	30
Supplicant Timeout	30	Server Timeout	30
Re-authentication Period	3600	Maximum Request	2
Per-Port Re-authentication	Disabled	Current PVID	1
Guest VLAN ID	---	Default VLAN ID	---

Figure 9-7 802.1X Port Settings (Port-Based Access Control)

The following parameters can be configured in the **Port-Based Access Control** 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.
Port Control	Select the authorization state of the port(s) here. Options to choose from are: <ul style="list-style-type: none"> Auto - Specifies to enable IEEE 802.1X authentication on the port(s). Force Authorized - Specifies to force an authorized state on the port(s). Force Unauthorized - Specifies to force an unauthorized state on the port(s).

Parameter	Description
Admin Control Direction	Select the control direction of traffic on the port(s) here. Options to choose from are: <ul style="list-style-type: none"> • Both - Specifies to control traffic in a bidirectional direction. • In - Specifies to control traffic in an inbound direction only.
Quiet Period	Enter the quiet period here. This is the number or seconds that the switch will remain in the quiet state after a failed authentication process. The range is from 1 to 65535 seconds.
Transmission Period	Enter the transmission period here. This is the number of seconds that the switch will wait for an EAP-request or identity frame from the supplicant before retransmitting the request. The range is from 1 to 65535 seconds.
Supplicant Timeout	Enter the supplicant timeout value here. This is the number of seconds the switch will wait for a response from the supplicant before timing out the supplicant message. This does not apply to the EAP request ID. The range is from 1 to 65535 seconds.
Server Timeout	Enter the server timeout value here. This is the number of seconds the switch will wait for a response from the authentication server before timing out the connection. The range is from 1 to 65535 seconds.
Re-authentication Period	Enter the re-authentication period here. This is the number of seconds between re-authentication attempts. The range is from 1 to 65535 seconds.
Maximum Request	Enter the maximum number of EAP requests that will be allowed from a backend authentication machine here before the authentication process is restarted. The range is from 1 to 10.
Per-Port Re-authentication	Select to enable or disable periodic re-authentication on the port(s) here.
Re-authentication Time Local	Select to enable or disable the use of the local settings for the timer to re-authenticate a session here.

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

Click the **Show** button to display the port-based access control settings associated to the specified port(s).

Click the **Init** button to initiate the port-based access control settings on the specified port(s).

Click the **Re-authenticate** button to re-authenticate all the connections to the specified port(s).

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

Click the **MAC-Based Access Control** tab to view the following window:

802.1X Ports Settings

Port-Based Access Control | **MAC-Based Access Control**

MAC-Based Authentication Ports: Gi1/0/11

Unit: 1

From Port: Gi1/0/1 To Port: Gi1/0/1

Number of Supplicant (1-512):

Quiet Period (1-65535): 60 sec

Supplicant Timeout (1-65535): 30 sec

Re-authentication Period (1-65535): 3600 sec

Re-authentication Time Local: Disabled

Force Authentication Timeout (0-65535): 3600 sec

AdminControlDirection: Both

Transmission Period (1-65535): 30 sec

Server Timeout (1-65535): 30 sec

Maximum Request (1-10): 2

Per-Port Re-authentication: Disabled

Apply

Unit: 1 Port: Gi1/0/11

Show Init Re-authenticate

NAS ID	Port Number	Number of Supplicant
nas1	Gi1/0/11	512

Show Detail

Figure 9-8 802.1X Port Settings (MAC-Based Access Control)

The following parameters can be configured in the **MAC-Based Access Control** 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.
Number of Supplicant	Enter the maximum number of authenticated users that will be allowed on the port(s) here. The range is from 1 to 512.
Admin Control Direction	Select the control direction of traffic on the port(s) here. Options to choose from are: <ul style="list-style-type: none"> Both - Specifies to control traffic in a bidirectional direction. In - Specifies to control traffic in an inbound direction only.
Quiet Period	Enter the quiet period here. This is the number or seconds that the switch will remain in the quiet state after a failed authentication process. The range is from 1 to 65535 seconds.
Transmission Period	Enter the transmission period here. This is the number of seconds that the switch will wait for an EAP-request or identity frame from the supplicant before retransmitting the request. The range is from 1 to 65535 seconds.

Parameter	Description
Supplicant Timeout	Enter the supplicant timeout value here. This is the number of seconds the switch will wait for a response from the supplicant before timing out the supplicant message. This does not apply to the EAP request ID. The range is from 1 to 65535 seconds.
Server Timeout	Enter the server timeout value here. This is the number of seconds the switch will wait for a response from the authentication server before timing out the connection. The range is from 1 to 65535 seconds.
Re-authentication Period	Enter the re-authentication period here. This is the number of seconds between re-authentication attempts. The range is from 1 to 65535 seconds.
Maximum Request	Enter the maximum number of EAP requests that will be allowed from a backend authentication machine here before the authentication process is restarted. The range is from 1 to 10.
Re-authentication Time Local	Select to enable or disable the use of the local settings for the timer to re-authenticate a session here.
Per-Port Re-authentication	Select to enable or disable periodic re-authentication on the port(s) here.
Force Authentication Timeout	Enter the forced authentication timeout value here. This is the number of seconds the switch will wait before timing out a forced authorized/unauthorized entry. The range is from 0 to 65535 seconds. Enter 0 to never timeout an entry.

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

Click the **Show** button to display the MAC-based access control settings associated to the specified port.

Click the **Init** button to initiate the MAC-based access control settings on the specified port.

Click the **Re-authenticate** button to re-authenticate all the connections to the specified port.

Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:

MAC-Based Port Information

MAC-Based Port Information

NAS ID	nas1	Port Number	Gi1/0/11
Number of Supplicant	2	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: 1

Supplicant MAC Address	Type	MAC Control	Authentication Status	Re-Authentication	
00-23-7D-BC-2E-18	Dynamic	Auto	Unauthorized	Disabled	<input type="button" value="Edit"/> <input type="button" value="Init"/> <input type="button" value="Re-authenticate"/>

1/1

Figure 9-9 802.1X Port Settings (MAC-Based Access Control, Show Detail)

Click the **Edit** button to enable or disable the re-authentication function.
 Click the **Init** button to initiate the MAC-based access control settings on the specified port.

Click the **Re-authenticate** button to re-authenticate the specified supplicant MAC address connection.

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

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

9.2.5 EAP Port Config

This window is used to configure and display the EAP settings on the specified port(s).

Click **Security > 802.1X > EAP Port Config** to view the following window:

Figure 9-10 EAP Port Config

The following parameters can be configured:

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.
EAP Request	Select to enable or disable the EAP request function on the specified port(s) here.
EAP Forward	Select to enable or disable the EAP forward function on the specified port(s) here. This is used to enable/disable the forwarding of IEEE 802.1X Protocol Data Units (PDUs).

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

9.2.6 802.1X Authenticator Statistics

This window is used to display and clear IEEE 802.1X authenticator statistics on the specified port.

Click **Security > 802.1X > 802.1X Authenticator Statistics** to view the following window:

Port	Gi1/0/1	Elapsed Time Since Reset	00:00:00:22
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 Authenticator Statistics

The following parameters can be configured in the **Statistics** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Since	Select the time range here. Options to choose from are: <ul style="list-style-type: none"> Since-Reset - Specifies to display statistics since the last switch reset. Since-Up - Specifies to display statistics since the last time the switch was booted up.

Click the **Find** button to display the information based on the search criteria specified.

Click the **Reset All** button to reset all the statistics information.

9.3 AAA (Authentication, Authorization, and Accounting)

9.3.1 AAA Global Settings

This window is used to globally enable or disable the AAA feature.

Click **Security > AAA > AAA Global Settings** to view the following window:

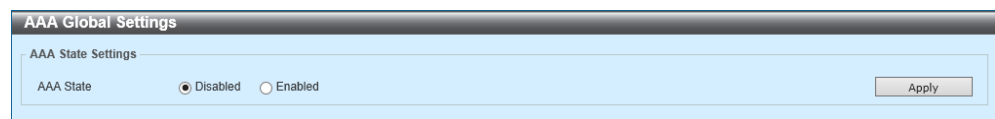


Figure 9-12 AAA Global Settings

The following parameters can be configured in the **AAA State Settings** section:

Parameter	Description
AAA State	Select to globally enable or disable the AAA feature here.

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

9.3.2 AAA Authentication Settings

This window is used to configure and display the AAA authentication settings.

Click **Security > AAA > AAA Authentication Settings** to view the following window:

Figure 9-13 AAA Authentication Settings

The following parameters can be configured in the **AAA Web Authentication Settings** section:

Parameter	Description
Primary Database	Select the primary database that will be used for web authentication here. Options to choose from are: <ul style="list-style-type: none"> • RADIUS - Specifies to use the database on the RADIUS server as the primary database. • Local - Specifies to use local database on the switch as the primary database.
Secondary Database	Select the secondary database that will be used for web authentication here. Options to choose from are: <ul style="list-style-type: none"> • None - Authentication on the secondary database is treated as approved. • RADIUS - Specifies to use the database on the RADIUS server as the secondary database. • Local - Specifies to use local database on the 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.

Parameter	Description
Authentication Fail Block Time	Enter the amount of seconds that a host will be blocked after web authentication failed. The range is from 1 to 65535 seconds.

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

The following parameters can be configured in the **AAA MAC Authentication Settings** section:

Parameter	Description
Primary Database	Select the primary database that will be used for MAC authentication here. Options to choose from are: <ul style="list-style-type: none"> • RADIUS - Specifies to use the database on the RADIUS server as the primary database. • Local - Specifies to use local database on the switch as the primary database.
Secondary Database	Select the secondary database that will be used for MAC authentication here. Options to choose from are: <ul style="list-style-type: none"> • None - Authentication on the secondary database is treated as approved. • RADIUS - Specifies to use the database on the RADIUS server as the secondary database. • Local - Specifies to use local database on the 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 Fail Block Time	Enter the amount of seconds that a host will be blocked after MAC authentication failed. The range is from 1 to 65535 seconds.

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

The following parameters can be configured in the **AAA 802.1X Authentication Settings** section:

Parameter	Description
Primary Database	<p>Select the primary database that will be used for IEEE 802.1X authentication here. Options to choose from are:</p> <ul style="list-style-type: none"> • RADIUS - Specifies to use the database on the RADIUS server as the primary database. • Local - Specifies to use local database on the switch as the primary database.
Secondary Database	<p>Select the secondary database that will be used for IEEE 802.1X authentication here. Options to choose from are:</p> <ul style="list-style-type: none"> • None - Specifies that no secondary database will be used. • Local - Specifies to use local database on the switch as the secondary database.

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

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:

The screenshot shows the 'AAA Authentication User Settings' window. It contains the following configuration fields:

- User Name:** 32 chars
- Password:** Selected (radio button), with an 'Encrypt' checkbox.
- Authentication Type:** Both (dropdown menu)
- VLAN ID (1-4094):** (text input field)
- 2-Step Authentication:** Disabled (dropdown menu)
- Apply** button

Below the configuration fields is a table showing the current settings:

User Name	Password	VLAN	Authentication Type	2-Step Authentication	
user	password	1	Both	Disabled	Delete

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

Figure 9-14 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.

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

This window is used to configure and display the AAA authentication MAC settings.

Click **Security > AAA > AAA Authentication MAC Settings** to view the following window:

Figure 9-15 AAA Authentication MAC Settings

The following parameters can be configured in the **AAA Authentication MAC Settings** section:

Parameter	Description
MAC Address	Enter the MAC address for the local authentication account here. This will be used in MAC authentication.
VLAN ID	Enter the target VLAN ID for the local authentication account here. The range is from 1 to 4094.
2-Step Authentication	<p>Select to enable or disable two-step authentication here. Options to choose from are:</p> <ul style="list-style-type: none"> • No - Specifies to disable two-step authentication for the local authentication account. • Web - Specifies to enable two-step authentication and use web authentication as the second authentication method. • 802.1X - Specifies to enable two-step authentication and use IEEE 802.1X authentication as the second authentication method. • Any - Specifies to enable two-step authentication and use IEEE 802.1X and web authentication as the second authentication methods.

Click the **Apply** button to add a new entry.

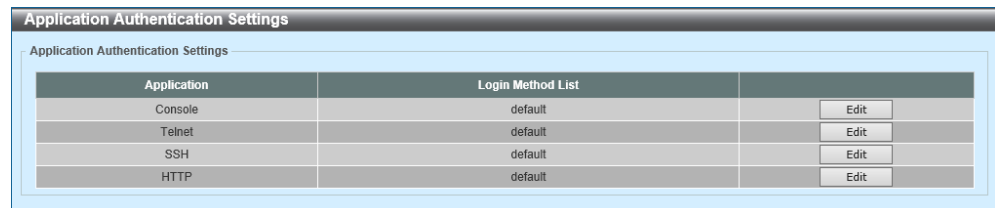
Click the **Delete** button to delete the specified entry.

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

9.3.5 Application Authentication Settings

This window is used to configure and display the application authentication settings.

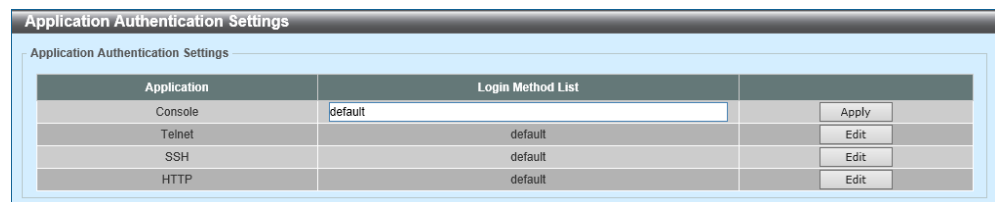
Click **Security > AAA > Application Authentication Settings** to view the following window:



Application	Login Method List	
Console	default	Edit
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 9-16 Application Authentication Settings

Click the **Edit** button to view the following window:



Application	Login Method List	
Console	default	Apply
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 9-17 Application Authentication Settings (Edit)

The following parameters can be configured in the **Application Authentication Settings** section:

Parameter	Description
Login Method List	Enter the name for the login method list here.

Click the **Edit** button to edit the settings of the specified entry.

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

9.3.6 Application Accounting Settings

This window is used to configure and display the application accounting settings.

Click **Security > AAA > Application Accounting Settings** to view the following window:

Figure 9-18 Application Accounting Settings

Click the **Edit** button to view the following window:

Figure 9-19 Application Accounting Settings (Edit)

The following parameters can be configured in the **Application Accounting Exec Method List** section:

Parameter	Description
Exec Method List	Enter the name for the EXEC method list here.

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

The following parameters can be configured in the **Application Accounting Method List** section:

Parameter	Description
Application	Select the application used here. Options to choose from are Console , Telnet , and SSH .
Level	Select the privilege level used here. Options to choose from are levels 1 to 15.
Commands Method List	Enter the commands method list name used here.

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.

Click the **AAA Accounting Commands** tab to view the following window:

Figure 9-20 Accounting Settings (AAA Accounting Commands)

The following parameters can be configured in the **AAA Accounting Commands** section:

Parameter	Description
Level	Select the privilege level used here. Options to choose from are levels 1 to 15.
List Name	Enter the method list name that will be used with the AAA accounting commands option here.
Method 1 – Method 4	Select the method lists that will be used for this configuration here. Options to choose from are None , Group , and TACACS+ . The None option is only available for Method 1.

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.

9.3.7 Authentication EXEC Settings

This window is used to configure and display the authentication execution settings.

Click **Security > AAA > Authentication EXEC Settings** to view the following window:

Figure 9-21 Authentication EXEC Settings

The following parameters can be configured in the **AAA Authentication Enable** section:

Parameter	Description
Status	Select to enable or disable the AAA authentication enable state here.
Method 1 – Method 4	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> • None - Specifies that the user will pass the authentication if it is not denied by previous method authentication. Normally, the method is listed as the last method. • Enable - Specifies to use the local enable password for authentication. • Group - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • RADIUS - Specifies to use the servers defined by the RADIUS server host command. • TACACS+ - Specifies to use the servers defined by the TACACS+ server host command.

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

The following parameters can be configured in the **AAA Authentication Login** section:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA authentication login option here.
Method 1 – Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: <ul style="list-style-type: none">• None - Specifies that the user will pass authentication if it is not denied by previous method's authentication. Normally, the method is listed as the last method.• Local - Specifies to use the local database for authentication.• Group - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long.• RADIUS - Specifies to use the servers defined by the RADIUS server host command.• TACACS+ - Specifies to use the servers defined by the TACACS+ server host command.

Click the **Apply** button to add a new entry.

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

9.3.8 Accounting Settings

This window is used to configure and display the AAA accounting settings.

Click **Security > AAA > Accounting Settings** to view the following window:

Figure 9-22 Accounting Settings (AAA Accounting Network)

The following parameters can be configured in the **AAA Accounting Network** section:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 – Method 4	Select the method lists that will be used for this configuration here. Options to choose from are None , Group , RADIUS , and TACACS+ . The None option is only available for Method 1.

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

Click the **AAA Accounting System** tab to view the following window:

Figure 9-23 Accounting Settings (AAA Accounting System)

The following parameters can be configured in the **AAA Accounting System** section:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 – Method 4	Select the method lists that will be used for this configuration here. Options to choose from are None , Group , RADIUS , and TACACS+ . The None option is only available for Method 1.

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

Click the **AAA Accounting Exec** tab to view the following window:

The screenshot shows the 'Accounting Settings' window with the 'AAA Accounting Exec' tab selected. The configuration includes a 'List Name' field (32 chars), and four method selection fields (Method 1: Group, Method 2: Group, Method 3: RADIUS, Method 4: TACACS+). Each method field has a '32 chars' label. An 'Apply' button is on the right. Below the fields, a table shows 'Total Entries: 1' with columns for Name, Method 1, Method 2, Method 3, and Method 4. The table contains one entry with 'Name' in the Name column, 'radius' in Method 1, 'tacacs+' in Method 2, and empty cells for Method 3 and Method 4. A 'Delete' button is at the bottom right of the table.

Figure 9-24 Accounting Settings (AAA Accounting Exec)

The following parameters can be configured in the **AAA Accounting Exec** section:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA accounting EXEC option here.
Method 1 – Method 4	Select the method lists that will be used for this configuration here. Options to choose from are None , Group , RADIUS , and TACACS+ . The None option is only available for Method 1.

Click the **Apply** button to add a new entry.

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

9.4 Authentication

9.4.1 Authentication Dynamic VLAN Settings

This window is used to configure and display the dynamic VLAN settings used in authentication.

Click **Security > Authentication > Authentication Dynamic VLAN Settings** to view the following window:

Port	Current PVID	Authentication Status	Guest VLAN	Default VLAN
Gi1/0/1	1	Authorized	---	---
Gi1/0/2	1	Authorized	---	---
Gi1/0/3	1	Authorized	---	---
Gi1/0/4	1	Authorized	---	---
Gi1/0/5	1	Authorized	---	---
Gi1/0/6	1	Authorized	---	---
Gi1/0/7	1	Authorized	---	---
Gi1/0/8	1	Authorized	---	---
Gi1/0/9	1	Authorized	---	---
Gi1/0/10	1	Authorized	---	---

Figure 9-25 Authentication Dynamic VLAN Settings

The following parameters can be configured in the **Authentication Dynamic VLAN Settings** section:

Parameter	Description
Accept RADIUS Attribute	Select to enable or disable the acceptance of RADIUS attributes here.
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.
Guest VLAN	Select to enable or disable the guest VLAN here. When this is enabled, hosts will be allowed access to the guest VLAN without the need for authentication.
Guest VLAN ID	Enter the guest VLAN ID here. The range is from 1 to 4094.
Default VLAN	Select to enable or disable the default VLAN here. After hosts were successfully authenticated, they will be assigned to the default VLAN if the dynamic VLAN feature is disabled or the target VLAN for the host is invalid.

Parameter	Description
Default VLAN ID	Enter the default VLAN ID here. The range is from 1 to 4094.

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

9.4.2 Authentication Status Table

This window is used to display the authentication status table and information. Additionally, the authentication aging time can also be configured in this window.

Click **Security > Authentication > Authentication Status Table** to view the following window:

Figure 9-26 Authentication Status Table

The following parameters can be configured in the **Authentication Status Table** section:

Parameter	Description
Authentication Aging Time	Enter the timeout value for MAC/Web authentication sessions here. The range is from 0 to 65535 minutes.
Sort By MAC	Select this option to display authentication sessions, sorted by MAC address.
Sort By Port	Select this option to display authentication sessions on the specified port(s). <ul style="list-style-type: none"> 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.

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

Click the **Find** button to find and display entries based on the search criteria specified.

9.4.3 2-Step Authentication Settings

This window is used to configure and display the 2-step authentication settings on the specified port(s).

Click **Security > Authentication > 2-Step Authentication Settings** to view the following window:

Figure 9-27 2-Step Authentication Settings

The following parameters can be configured in the **2-Step Authentication Settings** section:

Parameter	Description
2-Step Authentication Timeout	Enter the timeout value after which the second step of authentication will be attempted. The range is from 0 to 65535 minutes.
Unit	Select the Switch unit that will be used here.
From Port - To Port	Select the port(s) that will be used here.
2-Step Authentication Mode	Select the two-step authentication mode here. Options to choose from are: <ul style="list-style-type: none"> • MAC-Web - Specifies that MAC and Web authentication will both be used in the first step in the two-step authentication method. • MAC-Dot1X - Specifies that MAC and IEEE 802.1X authentication will both be used in the first step in the two-step authentication method. • Dot1X-Web - Specifies that IEEE 802.1X and Web authentication will both be used in the first step in the two-step authentication method.

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

Click the **Clear** button to clear the information based on the criteria specified.

9.5 RADIUS (Remote Authentication Dial-In User Service)

9.5.1 RADIUS Global Settings

This window is used to configure and display the global settings associated with the RADIUS feature.

Click **Security > RADIUS > RADIUS Global Settings** to view the following window:

Figure 9-28 RADIUS Global Settings

The following parameters can be configured in the **RADIUS Global Settings** section:

Parameter	Description
Dead Time	Enter the dead time value here. When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time. The range is from 1 to 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead. This setting can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries.

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

The following parameters can be configured in the **RADIUS Global IPv4 Source Interface** section:

Parameter	Description
IPv4 RADIUS Source Interface Name	Enter the name of the IPv4 RADIUS source interface here.

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

The following parameters can be configured in the **RADIUS Global IPv6 Source Interface** section:

Parameter	Description
IPv6 RADIUS Source Interface Name	Enter the name of the IPv6 RADIUS source interface here.

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

9.5.2 RADIUS Server Settings

This window is used to configure and display the RADIUS server settings.

Click **Security > RADIUS > RADIUS Server Settings** to view the following window:

Figure 9-29 RADIUS Server Settings

The following parameters can be configured in the **RADIUS Server Settings** section:

Parameter	Description
IP Address	Enter the IPv4 address of the RADIUS server here.
IPv6 Address	Enter the IPv6 address of the RADIUS server here.
Authentication Port	Enter the authentication port number used here. The range is from 0 to 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Accounting Port	Enter the accounting port number used here. The range is from 0 to 65535. By default, this value is 1813. If no accounting is used, use the value 0.
Retransmit	Enter the retransmit value used here. The range is from 0 to 20. By default, this value is 3. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. The range is from 1 to 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are Plain Text and Encrypted .
Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 32 characters long.

Click the **Apply** button to add a new entry.

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

9.5.3 RADIUS Group Server Settings

This window is used to configure and display the RADIUS group server settings.

Click **Security > RADIUS > RADIUS Group Server Settings** to view the following window:

Group Server Name	IPv4/IPv6 Address
Group	2017::1
radius	-

Figure 9-30 RADIUS Group Server Settings

The following parameters can be configured in the **RADIUS Group Server Settings** section:

Parameter	Description
Group Server Name	Enter the RADIUS group server name here. This name can be up to 32 characters long.
IP Address	Enter the IPv4 address of the RADIUS group server here.
IPv6 Address	Enter the IPv6 address of the RADIUS 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 view the following window:

IPv4/IPv6 Address
2017::1

Figure 9-31 RADIUS Group Server Settings (Show Detail)

The following parameters can be configured:

Parameter	Description
IPv4 RADIUS Source Interface Name	Enter the name of the source IPv4 RADIUS interface here.
IPv6 RADIUS Source Interface Name	Enter the name of the source IPv6 RADIUS 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.

9.5.4 RADIUS Statistics

This window is used to display and clear the RADIUS statistics information.

Click **Security > RADIUS > RADIUS Statistics** to view the following window:

Figure 9-32 RADIUS Statistics

The following parameters can be configured in the **RADIUS Statistic** section:

Parameter	Description
Group Server Name	Select the RADIUS 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.

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

Click the second **Clear** button to clear the statistics information in the 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+ feature.

Click **Security > TACACS+ > TACACS+ Global Settings** to view the following window:

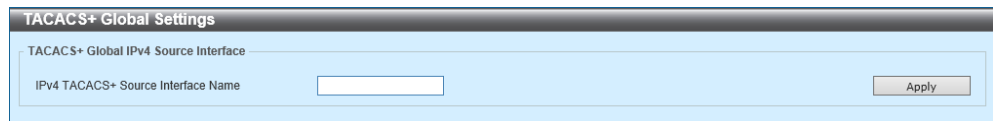


Figure 9-33 TACACS+ Global Settings

The following parameters can be configured in the **TACACS+ Global IPv4 Source Interface** section:

Parameter	Description
IPv4 TACACS+ Source Interface Name	Enter the name of the IPv4 TACACS+ source interface here.

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

9.6.2 TACACS+ Server Settings

This window is used to configure and display the TACACS+ server settings.

Click **Security > TACACS+ > TACACS+ Server Settings** to view the following window:

The screenshot shows the 'TACACS+ Server Settings' window. It contains the following fields and controls:

- IP Address:** A text input field.
- Port (1-65535):** A text input field with the value '49'.
- Key Type:** A dropdown menu with 'Plain Text' selected.
- Timeout (1-255):** A text input field with the value '5' and a 'sec' label.
- Key:** A text input field with the value '254 chars'.
- Apply:** A button to save the settings.
- Total Entries: 1:** A summary label above a table.
- Table:** A table with 5 columns: IPv4 Address, Port, Timeout, Key, and an action button. The first row contains the values: 192.168.70.1, 49, 5, *****, and a Delete button.

Figure 9-34 TACACS+ Server Settings

The following parameters can be configured in the **TACACS+ Server Settings** section:

Parameter	Description
IP Address	Enter the IPv4 address of the TACACS+ server here.
Port	Enter the port number used here. The range is from 1 to 65535. By default, this value is 49.
Timeout	Enter the timeout value here. The range is from 1 to 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are Plain Text and Encrypted .
Key	Enter the key, used to communicate with the TACACS+ server, here. This key can be up to 254 characters long.

Click the **Apply** button to add a new entry.

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

9.6.3 TACACS+ Group Server Settings

This window is used to configure and display the TACACS+ group server settings.

Click **Security > TACACS+ > TACACS+ Group Server Settings** to view the following window:

Group Server Name	IPv4 Address	
Name	192.168.70.35	Show Detail Delete
tacacs+	192.168.70.35	Show Detail Delete

Figure 9-35 TACACS+ Group Server Settings

The following parameters can be configured 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 view the following window:

IPv4 Address	Delete
192.168.70.35	Delete

Figure 9-36 TACACS+ Group Server Settings (Show Detail)

The following parameters can be configured 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.

9.6.4 TACACS+ Statistics

This window is used to display and clear the TACACS+ statistics information.

Click **Security > TACACS+ > TACACS+ Statistics** to view the following window:

TACACS+ Server Address	State	Socket Opens	Socket Closes	Total Packets Sent	Total Packets Recv	Reference Count
192.168.70.1/49	Up	0	0	0	0	0

Figure 9-37 TACACS+ Statistics

The following parameters can be configured 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 for 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

This window is used to configure and display the global settings associated with the DHCP snooping feature.

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings** to view the following window:

Parameter	Enabled	Disabled
DHCP Snooping	<input type="radio"/>	<input checked="" type="radio"/>
Information Option Allow Untrusted	<input type="radio"/>	<input checked="" type="radio"/>
Source MAC Verification	<input checked="" type="radio"/>	<input type="radio"/>
Station Move Deny	<input type="radio"/>	<input checked="" type="radio"/>

Figure 9-38 DHCP Snooping Global Settings

The following parameters can be configured in the **DHCP Snooping Global Settings** section:

Parameter	Description
DHCP Snooping	Select to globally enable or disable DHCP snooping here.
Information Option Allow Untrusted	Select to globally enable or disable the option to allow DHCP packets with the relay Option 82 on the untrusted interface.
Source MAC Verification	Select to enable or disable the verification that the source MAC address in a DHCP packet matches the client hardware address.
Station Move Deny	Select to enable or disable the DHCP snooping station move state. When DHCP snooping station move is enabled, the dynamic DHCP snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if it detects that a new DHCP process belong to the same VLAN ID and MAC address.

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

9.7.1.1.2 DHCP Snooping Port Settings

This window is used to configure and display the DHCP snooping settings on the specified port(s).

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings** to view the following window:

Port	Trusted	Rate Limit	Entry Limit
Gi1/0/1	No	No Limit	No Limit
Gi1/0/2	No	No Limit	No Limit
Gi1/0/3	No	No Limit	No Limit
Gi1/0/4	No	No Limit	No Limit
Gi1/0/5	No	No Limit	No Limit
Gi1/0/6	No	No Limit	No Limit
Gi1/0/7	No	No Limit	No Limit
Gi1/0/8	No	No Limit	No Limit
Gi1/0/9	No	No Limit	No Limit
Gi1/0/10	No	No Limit	No Limit

Figure 9-39 DHCP Snooping Port Settings

The following parameters can be configured in the **DHCP Snooping 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.
Entry Limit	Enter the entry limit value here. The range is from 0 to 508. Tick the No Limit option to disable the function.
Rate Limit	Enter the rate limit value here. The range is from 1 to 300. Tick the No Limit option to disable the function.
Trusted	Select the trusted option here. Options to choose from are No and Yes . Ports connected to the DHCP server or to other switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping will act as a firewall between untrusted interfaces and DHCP servers.

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

9.7.1.1.3 DHCP Snooping VLAN Settings

This window is used to configure and display the DHCP snooping settings on the specified VLAN(s).

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings** to view the following window:

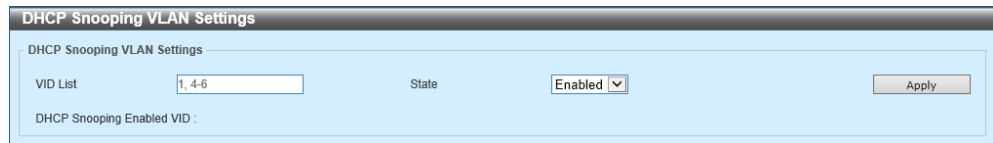


Figure 9-40 DHCP Snooping VLAN Settings

The following parameters can be configured in the **DHCP Snooping VLAN Settings** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
State	Select to enable or disable the DHCP snooping VLAN setting here.

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

9.7.1.1.4 DHCP Snooping Database

This window is used to configure and display the DHCP snooping database settings.

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Database** to view the following window:

Figure 9-41 DHCP Snooping Database

The following parameters can be configured in the **DHCP Snooping Database** section:

Parameter	Description
Write Delay	Enter the write delay time here. The range is from 60 to 86400 seconds. By default, this value is 300 seconds.

Click the **Reset** button to reset the DHCP snooping database.
Click the **Apply** button to accept the changes made.

The following parameters can be configured in the **Store DHCP Snooping Database** section:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be stored to here. Locations to choose from are TFTP , FTP , and Local .

Click the **Reset** button to reset the stored DHCP snooping database.
Click the **Apply** button to store the DHCP snooping database.

The following parameters can be configured in the **Load DHCP Snooping Database** section:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be loaded from here. Locations to choose from are TFTP , FTP , and Local .

Click the **Apply** button to load the DHCP snooping database.
Click the **Clear** button to clear the counter information.

9.7.1.1.5 DHCP Snooping Binding Entry

This window is used to configure and display DHCP snooping binding entries.

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry** to view the following window:

Figure 9-42 DHCP Snooping Binding Entry

The following parameters can be configured in the **DHCP Snooping Manual Binding** section:

Parameter	Description
MAC Address	Enter the MAC address of the DHCP snooping binding entry here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
IP Address	Enter the IP address of the DHCP snooping binding entry here.
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Expiry	Enter the expiry time value used here. The range is from 60 to 4294967295 seconds.

Click the **Add** 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.

9.7.1.2 Dynamic ARP Inspection

9.7.1.2.1 ARP Access List

This window is used to configure and display the ARP access list settings used in dynamic ARP inspection.

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Access List** to view the following window:

Figure 9-43 ARP Access List

The following parameters can be configured in the **ARP Access List** section:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.

Click the **Add** button to add a new entry.

Click the **Edit** button to edit the settings of the specified entry.

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

Click the **Edit** button to view the following window:

Figure 9-44 ARP Access List (Edit)

The following parameters can be configured:

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are Permit and Deny .
IP	Select the type of sender IP address that will be used here. Options to choose from are Any , Host , and IP with Mask .
Sender IP	After selecting the Host or IP with Mask options as the type of IP , enter the sender IP address used here.
Sender IP Mask	After selecting the IP with Mask option as the type of IP , enter the sender IP mask used here.
MAC	Select the type of sender MAC address that will be used here. Options to choose from are Any , Host , and MAC with Mask .
Sender MAC	After selecting the Host or MAC with Mask options as the type of MAC , enter the sender MAC address used here.
Sender MAC Mask	After selecting the MAC with Mask option as the type of MAC , enter the sender MAC mask used here.

Click the **Apply** button to add a new entry.

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

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

9.7.1.2.2 ARP Inspection Settings

This window is used to configure and display the dynamic ARP inspection settings.

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings** to view the following window:

Figure 9-45 ARP Inspection Settings

The following parameters can be configured in the **ARP Inspection Validation** section:

Parameter	Description
Src-MAC	Select to enable or disable the source MAC option here. This option specifies to check for ARP request and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.
Dst-MAC	Select to enable or disable the destination MAC option here. This option specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.

Parameter	Description
IP	Select to enable or disable the IP option here. This option specifies to check the ARP body for invalid and unexpected IP addresses. It also specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses. Target IP addresses are checked only in ARP responses.

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

The following parameters can be configured in the **ARP Inspection VLAN Logging** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
State	Select to enable or disable ARP inspection VLAN logging of the specified VLAN(s) here.

Click the **Apply** button to add a new entry.

Click the **Edit** button to edit the settings of the specified entry.

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

The following parameters can be configured in the **ARP Inspection Filter** section:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
Static ACL	Select whether to use a static ACL or not here by either selecting Yes or No .

Click the **Add** button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

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

9.7.1.2.3 ARP Inspection Port Settings

This window is used to configure and display the dynamic ARP inspection settings on the specified port(s).

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings** to view the following window:

Port	Trust State	Rate Limit (pps)	Burst Interval
Gi1/0/1	Untrusted	15	1
Gi1/0/2	Untrusted	15	1
Gi1/0/3	Untrusted	15	1
Gi1/0/4	Untrusted	15	1
Gi1/0/5	Untrusted	15	1
Gi1/0/6	Untrusted	15	1
Gi1/0/7	Untrusted	15	1
Gi1/0/8	Untrusted	15	1
Gi1/0/9	Untrusted	15	1
Gi1/0/10	Untrusted	15	1

Figure 9-46 ARP Inspection Port Settings

The following parameters can be configured:

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.
Rate Limit	Enter the rate limit value here. The range is from 1 to 150 packets per seconds.
Burst Interval	Enter the burst interval value here. The range is from 1 to 15. Tick the None option to disable the option.
Trust State	Select to enable or disable the trust state here.

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

Click the **Set to Default** button the set the trust state to the default setting.

9.7.1.2.4 ARP Inspection Statistics

This window is used to display and clear the dynamic ARP inspection statistics information.

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics** to view the following window:

VLAN	Forwarded	Dropped	DHCP Drops	ACL Drops	DHCP Permits	ACL Permits	Source MAC Failures	Dest MAC Failure	IP Validation Failure
1	24	1	1	0	0	24	0	0	0

Figure 9-47 ARP Inspection Statistics

The following parameters can be configured:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

Click the **Clear by VLAN** button to clear the statistics information related to the specified VLAN.

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

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

9.7.1.2.5 ARP Inspection Log

This window is used to display and clear the dynamic ARP inspection log information. The log buffer value can also be configured in this window.

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Log** to view the following window:

Figure 9-48 ARP Inspection Log

The following parameters can be configured in the **ARP Inspection Log** section:

Parameter	Description
Log Buffer	Enter the size of the log buffer here. The range is from 1 to 1024. By default, this value is 32. Select the Default option to use the default value.

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

Click the **Clear Log** button to clear the ARP inspection log.

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

9.7.1.3 IP Source Guard

9.7.1.3.1 IP Source Guard Port Settings

This window is used to configure and display the IP source guard settings on the specified port(s).

Click **Security > SAVI > IPv4 > IP Source Guard > IP Source Guard Port Settings** to view the following window:

Port	Validation Type
Gi1/0/10	ip

Figure 9-49 IP Source Guard Port Settings

The following parameters can be configured:

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 IP source guard's state for the specified port(s) here.
Validation	Select the validation method used here. Options to choose from are: <ul style="list-style-type: none"> IP - Specifies that the IP address of the received packets will be checked. IP-MAC - Specifies that the IP address and the MAC address of the received packets will be checked.

Click the **Apply** button to add a new entry.

9.7.1.3.2 IP Source Guard Binding

This window is used to configure and display the IP source guard binding settings.

Click **Security > SAVI > IPv4 > IP Source Guard > IP Source Guard Binding** to view the following window:

Figure 9-50 IP Source Guard Binding

The following parameters can be configured in the **IP Source Binding Settings** section:

Parameter	Description
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
IP Address	Enter the IP address of the binding entry here.
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.

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

The following parameters can be configured in the **IP Source Binding Entry** 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.
IP Address	Enter the IP address of the binding entry here.
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Type	Select the type of binding entry to find here. Options to choose from are: <ul style="list-style-type: none"> • All - Specifies that all the DHCP binding entries will be displayed. • DHCP Snooping - Specifies to display the IP-source guard binding entry learned by DHCP binding snooping. • Static - Specifies to display the IP-source guard binding entry that is manually configured.

Click the **Find** button to find and display entries based on the search criteria specified.

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.

9.7.1.3.3 IP Source Guard HW Entry

This window is used to display the IP source guard, hardware entries on the specified port(s).

Click **Security > SAVI > IPv4 > IP Source Guard > IP Source Guard HW Entry** to view the following window:

Port	Filter-type	Filter-mode	IP Address	MAC Address	VLAN
Gi1/0/10	ip	Active	192.168.70.56	-	1

Figure 9-51 IP Source Guard HW Entry

The following parameters can be configured:

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.

Click the **Find** button to find and display entries based on the search criteria specified.

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

9.8 DHCP Server Protect

9.8.1 DHCP Server Protect Global Settings

This window is used to configure and display the global settings associated with the DHCP server protect feature.

Click **Security > DHCP Server Protect > DHCP Server Protect Global Settings** to view the following window:

The screenshot shows the 'DHCP Server Protect Global Settings' window. It has two main sections: 'Profile Settings' and 'Log Information'.
 In 'Profile Settings', there are two input fields: 'Profile Name' with a hint '32 chars' and 'Client MAC' with the value '00-84-57-00-00-00'. To the right of these fields is an 'Apply' button. Below the input fields is a table header 'Total Entries: 1'. The table has two columns: 'Profile Name' and 'Client MAC'. The first row shows 'Name' and '00-33-11-22-55-44'. To the right of this row are two buttons: 'Delete' and 'Delete Profile'.
 In 'Log Information', there is an input field for 'Log Buffer Entries (10-1024)' with the value '32'. To the right of this field are 'Apply' and 'Clear Log' buttons. Below this is a table header 'Total Entries: 0'. The table has four columns: 'VLAN', 'Server IP', 'Client MAC', and 'Occurrence'.

Figure 9-52 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 1024. By default, this value is 32.

9.8.2 DHCP Server Protect Port Settings

This window is used to configure and display the DHCP server protect settings on the specified port(s).

Click **Security > DHCP Server Protect > DHCP Server Protect Port Settings** to view the following window:

Port	State	Server IP	Profile Name	
Gi1/0/1	Disabled	-	-	Delete
Gi1/0/2	Disabled	-	-	Delete
Gi1/0/3	Disabled	-	-	Delete
Gi1/0/4	Disabled	-	-	Delete
Gi1/0/5	Disabled	-	-	Delete
Gi1/0/6	Disabled	-	-	Delete
Gi1/0/7	Disabled	-	-	Delete
Gi1/0/8	Disabled	-	-	Delete
Gi1/0/9	Disabled	-	-	Delete
Gi1/0/10	Disabled	-	-	Delete

Figure 9-53 DHCP Server Protect Port Settings

The following parameters can be configured 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

This window is used to configure and display the state of the BPDU guard feature and the BPDU guard settings on the specified port(s).

Click **Security > BPDU Guard** to view the following window:

Port	State	Mode	Status
Gi1/0/1	Disabled	Shutdown	Normal
Gi1/0/2	Disabled	Shutdown	Normal
Gi1/0/3	Disabled	Shutdown	Normal
Gi1/0/4	Disabled	Shutdown	Normal
Gi1/0/5	Disabled	Shutdown	Normal
Gi1/0/6	Disabled	Shutdown	Normal
Gi1/0/7	Disabled	Shutdown	Normal
Gi1/0/8	Disabled	Shutdown	Normal
Gi1/0/9	Disabled	Shutdown	Normal
Gi1/0/10	Disabled	Shutdown	Normal

Figure 9-54 BPDU Guard

The following parameters can be configured in the **BPDU Guard Settings** section:

Parameter	Description
BPDU Guard State	Select to globally enable or disable the BPDU Guard feature here.
BPDU Guard Trap State	Select to enable or disable the BPDU Guard trap state here.

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

The following parameters can be configured in the **BPDU Guard 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 BPDU Guard on the port(s) specified.
Mode	Select the BPDU Guard mode that will be applied to the specified port(s). Options to choose from are: <ul style="list-style-type: none"> • Drop - Drop all received BPDU packets when the port enters under attack state. • Block - Drop all packets (include BPDU and normal packets) when the port enters under attack state. • Shutdown - Shut down the port when the port enters under attack state.

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

9.10 NetBIOS Filtering

This window is used to configure and display the NetBIOS filtering settings on the specified port(s).

Click **Security > NetBIOS Filtering** to view the following window:

Port	NetBIOS Filtering State	Extensive NetBIOS Filtering State
Gi1/0/1	Disabled	Disabled
Gi1/0/2	Disabled	Disabled
Gi1/0/3	Disabled	Disabled
Gi1/0/4	Disabled	Disabled
Gi1/0/5	Disabled	Disabled
Gi1/0/6	Disabled	Disabled
Gi1/0/7	Disabled	Disabled
Gi1/0/8	Disabled	Disabled
Gi1/0/9	Disabled	Disabled
Gi1/0/10	Disabled	Disabled

Figure 9-55 NetBIOS Filtering

The following parameters can be configured in the **NetBIOS Filtering** 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.
NetBIOS Filtering State	Select to enable or disable the NetBIOS filtering state on the specified port(s). This is used to permit or deny NetBIOS packets on physical ports.
Extensive NetBIOS Filtering State	Select to enable or disable the extensive NetBIOS filtering state on the specified port(s). This is used to permit or deny NetBIOS packets over 802.3 frames on physical ports.

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

9.11 MAC Authentication

This window is used to configure and display the MAC authentication settings.

Click **Security > MAC Authentication** to view the following window:

Figure 9-56 MAC Authentication

The following parameters can be configured in the **MAC Authentication Settings** section:

Parameter	Description
MAC Authentication State	Select to globally enable or disable the MAC Authentication feature here.

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

The following parameters can be configured in the **MAC Format Settings** section:

Parameter	Description
Case	Select the letter case that will be used in the MAC address. Options to choose from are: <ul style="list-style-type: none"> Upper Case - Specifies the use the uppercase format for the MAC address. For example, AA-BB-CC-DD-EE-FF. Lower Case - Specifies the use the lowercase format for the MAC address. For example, aa-bb-cc-dd-ee-ff.

Parameter	Description
Delimiter	Select the type of delimiters that will be used in the MAC address. Options to choose from are: <ul style="list-style-type: none"> • Hyphen - Specifies to use hyphens as delimiters in the MAC address. For example, AA-BB-CC-DD-EE-FF. • Colon - Specifies to use colons as delimiters in the MAC address. For example, AA:BB:CC:DD:EE:FF. • Dot - Specifies to use dots as delimiters in the MAC address. For example, AA.BB.CC.DD.EE.FF. • None - Specifies not to use delimiters in the MAC address. For example, AABBCCDDEEFF.
Delimiter Characters	Select the number of delimiters that will be used in the MAC address. Options to choose from are: <ul style="list-style-type: none"> • 2 - Specifies to use a single delimiter in the MAC address. For example, AABBCC-DDEEFF. • 4 - Specifies to use two delimiters in the MAC address. For example, AABB-CCDD-EEFF. • 6 - Specifies to use five delimiters in the MAC address. For example, AA-BB-CC-DD-EE-FF.

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

The following parameters can be configured in the **MAC Authentication Password Settings** section:

Parameter	Description
RADIUS Password Type	Select the RADIUS password type here. Options to choose from are: <ul style="list-style-type: none"> • MAC Address - Specifies to use the MAC address as the RADIUS password. • Manual - Specifies to use a manual string as the RADIUS password.
Manual	Enter the RADIUS password for the MAC authentication account here.

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

The following parameters can be configured in the **MAC Authentication Ports** 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 MAC authentication for the port(s) specified here.

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

9.12 Web Authentication

9.12.1 Web Authentication Settings

This window is used to configure and display the Web authentication settings.

Click **Security > Web Authentication > Web Authentication Settings** to view the following window:

Figure 9-57 Web Authentication Settings

The following parameters can be configured in the **Global Settings** section:

Parameter	Description
Authentication State	Select to globally enable or disable the Web authentication feature.

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

The following parameters can be configured in the **Authentication 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 Web authentication feature on the specified port(s).

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

The following parameters can be configured in the **Authentication Settings** section:

Parameter	Description
Virtual IP	Enter the virtual IPv4 address used here. All web authentication processes communicate with this virtual IP address, however, the virtual IP does not respond to any ICMP packets or ARP requests. The virtual IPv4 address and the IPv4 address of the switch must use different subnets. The virtual IPv4 address is an essential component for successful web authentication.
HTTP Port Number	Enter the HTTP TCP/UDP port number here. The range is from 1 to 65535. By default, this value is 80. HTTP stands for the Hypertext Transfer Protocol.
Redirect URL	Enter the redirection URL here. This can be up to 64 characters long.

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

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 9-58 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.
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.

9.13 Trusted Host

This window is used to configure and display the trusted host settings.

Click **Security > Trusted Host** to view the following window:

Figure 9-59 Trusted Host

The following parameters can be configured in the **Trusted Host** section:

Parameter	Description
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.
Type	Select the trusted host type here. Options to choose from are Telnet , SSH , Ping , HTTP , and Hyper Text Transfer Protocol Secure (HTTPS).

Click the **Apply** button to add a new entry.

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

9.14 Traffic Segmentation Settings

This window is used to configure and display the traffic segmentation settings on the specified port(s).

Click **Security > Traffic Segmentation Settings** to view the following window:

Port	Forwarding Domain
Gi1/0/24	Gi1/0/20-1/0/24, Te1/0/25-1/0/26
Te1/0/25	Gi1/0/20-1/0/24, Te1/0/25-1/0/26
Te1/0/26	Gi1/0/20-1/0/24, Te1/0/25-1/0/26

Figure 9-60 Traffic Segmentation Settings

The following parameters can be configured 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

This window is used to configure and display the storm control settings.

Click **Security > Storm Control** to view the following window:

Storm Control Settings

Storm Control Polling Settings

Polling Interval (5-600) sec Shutdown Retries (0-360) times ☐ Infinite

Storm Control Port Settings

Unit	From Port	To Port	Type	Action	Level Type	PPS Rise (0-255000)	PPS Low (0-255000)
1	Gi1/0/1	Gi1/0/1	Broadcast	None	PPS		

Total Entries: 84

Port	Storm	Action	Threshold	Current	State
Gi1/0/1	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
Gi1/0/2	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
Gi1/0/3	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
Gi1/0/4	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive

Figure 9-61 Storm Control (Level Type, PPS)

The following parameters can be configured in the **Storm Control Polling Settings** section:

Parameter	Description
Polling Interval	Enter the polling interval value used here. The range is from 5 to 600 seconds. By default, this value is 5 seconds.
Shutdown Retries	Enter the shutdown retries value used here. The range is from 0 to 360. By default, this value is 3. Tick the Infinite option to disable this feature.

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

The following parameters can be configured in the **Storm Control 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.
Type	Select the type of storm attack that will be controlled here. Options to choose from are Broadcast , Multicast , and Unicast . When the Action is configured as Shutdown , the unicast refers to both known and unknown unicast packets; that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets.
Action	Select the action that will be taken here. Options to choose from are: <ul style="list-style-type: none"> • None - Specifies not to filter the storm packets. • Shutdown - Specifies to shut down the port when the value specified for rise threshold is reached. • Drop - Specifies to discard packets that exceed the risen threshold.
Level Type	Select the level type option here. Options to choose from are Packets Per Second (PPS), Kbps , and Level .
PPS Rise	Enter the PPS rise value here. This option specifies the rise threshold value in packets count per second. The range is from 1 to 255000 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.
PPS Low	Enter the PPS low value here. This option specifies the low threshold value in packets count per second. The range is from 1 to 255000 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.

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

Select **Kbps** as the **Level Type** to view the following window:

The screenshot shows the 'Storm Control Port Settings' window. The configuration is as follows:

- Unit:** 1
- From Port:** Gi1/0/1
- To Port:** Gi1/0/1
- Type:** Broadcast
- Action:** None
- Level Type:** Kbps
- Kbps Rise (0-2147483647):** (empty field)
- Kbps Low (0-2147483647):** (empty field)
- Buttons:** Apply

Figure 9-62 Storm Control (Level Type, Kbps)

The following additional parameters can be configured:

Parameter	Description
KBPS Rise	Enter the KBPS rise value here. This option specifies the rise threshold value as a rate of kilobits per second at which traffic is received on the port. The range is from 1 to 2147483647 Kbps.
KBPS Low	Enter the KBPS low value here. This option specifies the low threshold value as a rate of kilobits per second at which traffic is received on the port. The range is from 1 to 2147483647 Kbps. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.

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

Select **Level** as the **Level Type** to view the following window:

Figure 9-63 Storm Control (Level Type, Level)

The following additional parameters can be configured:

Parameter	Description
Level Rise	Enter the level rise value here. This option specifies the rise threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. The range is from 1 to 100 percent.
Level Low	Enter the level low value here. This option specifies the low threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. The range is from 1 to 100 percent. If the low level is not specified, the default value is 80% of the specified risen level.

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

9.16 SSH (Secure Shell)

9.16.1 SSH Global Settings

This window is used to configure and display the global settings associated with the SSH feature.

Click **Security > SSH > SSH Global Settings** to view the following window:

SSH Global Settings	
IP SSH Server State	Disabled
IP SSH Service Port (1-65535)	22
SSH Server Mode	V2
Authentication Timeout (30-600)	120 sec
Authentication Retries (1-32)	3 times
<button>Apply</button>	

Figure 9-64 SSH Global Settings

The following parameters can be configured in the **SSH Global Settings** section:

Parameter	Description
IP SSH Server State	Select to globally enable or disable the SSH server here.
IP SSH Service Port	Enter the SSH service port number used here. The range is from 1 to 65535. By default, this number is 22.
Authentication Timeout	Enter the authentication timeout value here. The range is from 30 to 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. The range is from 1 to 32. By default, this value is 3.

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

9.16.2 Host Key

This window is used to configure and display the SSH host key settings.

Click **Security > SSH > Host Key** to view the following window:

Figure 9-65 Host Key

The following parameters can be configured in the **Host Key Management** section:

Parameter	Description
Crypto Key Type	Select the cryptographic key type used here. Options to choose from are the Rivest Shamir Adleman (RSA) key type and the Digital Signature Algorithm (DSA) key type.
Key Modulus	Select the key modulus value here. Options to choose from are 360 , 512 , 768 , 1024 , and 2048 bit.

Click the **Generate** button to generate a host key based on the selections made.

Click the **Delete** button to remove a host key based on the selections made.

The following parameters can be configured in the **Host Key** section:

Parameter	Description
Crypto Key Type	Select the cryptographic key type used here. Options to choose from are RSA and DSA.

9.16.3 SSH Server Connection

This window is used to display the SSH server connection table and information.

Click **Security > SSH > SSH Server Connection** to view the following window:

A screenshot of the 'SSH Server Connection' window. The window has a title bar 'SSH Server Connection'. Inside, there is a section 'SSH Table' which contains a table. Above the table, it says 'Total Entries: 0'. The table has five columns: 'Session ID', 'Version', 'Cipher', 'User ID', and 'Client IP Address'.

Session ID	Version	Cipher	User ID	Client IP Address
------------	---------	--------	---------	-------------------

Figure 9-66 SH Server Connection

9.16.4 SSH User Settings

This window is used to configure and display the SSH user settings.

Click **Security > SSH > SSH User Settings** to view the following window:

Figure 9-67 SSH User Settings

The following parameters can be configured in the **SSH User Settings** section:

Parameter	Description
User Name	Enter the username for the SSH user account used here. This can be up to 32 characters long.
Authentication Method	Select the SSH authentication method here. Options to choose from are Password , Public Key , and Host-based .
Key File	After selecting Public Key or Host-based , enter the public key here. This can be up to 779 characters long.
Host Name	After selecting Host-based , enter the host name here. This can be up to 255 characters long.
IPv4 Address	After selecting Host-based , select and enter the IPv4 address of the SSH user account here.
IPv6 Address	After selecting Host-based , select and enter the IPv6 address of the SSH user account here.

Click the **Apply** button to add a new entry.

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

9.17 SSL (Secure Sockets Layer)

9.17.1 SSL Global Settings

This window is used to configure and display the global settings associated with the SSL feature.

Click **Security > SSL > SSL Global Settings** to view the following window:

Figure 9-68 SSL Global Settings

The following parameters can be configured in the **SSL Global Settings** section:

Parameter	Description
SSL Status	Select to globally enable or disable the SSL feature here.
Service Policy	Enter the service policy name here. This name can be up to 32 characters long.

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

The following parameters can be configured in the **Import File** section:

Parameter	Description
File Select	Select the file type that will be uploaded here. Options to choose from are Certificate and Private Key . After selecting the file type, browse to the file, located on the local computer, by pressing the Browse button.
Destination File Name	Enter the destination file name used here. This name can be up to 32 characters long.

Click the **Apply** button to import the SSL file.

9.17.2 Crypto PKI Trustpoint

This window is used to configure and display the SSL cryptographic Public Key Infrastructure (PKI) trust-point settings.

Click **Security > SSL > Crypto PKI Trustpoint** to view the following window:

Figure 9-69 Crypto PKI Trustpoint

The following parameters can be configured in the **Crypto PKI Trustpoint** section:

Parameter	Description
Trustpoint	Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.
File System Path	Enter the file system path for certificates and key pairs here.
Password	Enter the encrypted password phrase that is used to undo encryption when the private keys are imported here. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
TFTP Server Path	Enter the TFTP server path here.
Type	Select the type of certificate that will be imported here. Options to choose from are: <ul style="list-style-type: none"> • Both - Specifies to import the Certificate Authority (CA) certificate, local certificate and key pairs. • CA - Specifies to import the CA certificate only. • Local - Specifies to import local certificate and key pairs only.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

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

9.17.3 SSL Service Policy

This window is used to configure and display the SSL service policy settings.

Click **Security > SSL > SSL Service Policy** to view the following window:

Policy Name	Version	Cipher Suites	Session Cache Timeout (sec)	Secure Trustpoint	
Name	TLS 1.0, TLS 1.1...	DHE_DSS_WITH_3DES_ED...	600		Edit Delete

Figure 9-70 SSL Service Policy

The following parameters can be configured in the **SSL Service Policy** section:

Parameter	Description
Policy Name	Enter the SSL service policy name here. This name can be up to 32 characters long.
Version	Select the Transport Layer Security (TLS) version here. Options to choose from are TLS 1.0 , TLS 1.1 , and TLS 1.2 .
Session Cache Timeout	Enter the timeout value for session cache here. The range is from 60 to 86400 seconds. By default, this value is 600 seconds.
Secure Trustpoint	Enter the secure trust-point name here. This name can be up to 32 characters long.
Cipher Suites	Select the cipher suites that will be associated with this profile here.

Click the **Apply** button to add a new entry.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Edit** button to edit the settings of the specified entry.

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

10 OAM (Operations, Administration & Management)

10.1 Cable Diagnostics

This window is used to initiate and display the cable diagnostics test and results on the specified port(s).

Click **OAM > Cable Diagnostics** to view the following window:

The screenshot shows the 'Cable Diagnostics' window. At the top, there are dropdown menus for 'Unit' (set to 1), 'From Port' (set to Gi1/0/1), and 'To Port' (set to Gi1/0/1), along with a 'Test' button. Below this is the 'Unit 1 Settings' section, which contains a table with columns: Port, Type, Link Status, Test Result, Cable Length (M), and a 'Clear' button. The table lists ports Gi1/0/1 through Gi1/0/10. Port Gi1/0/1 is 'Link Up' and shows test results: Pair 1 Short at 1M, Pair 2 Ok at 2M, Pair 3 Ok at 2M, and Pair 4 Short at 1M. Ports Gi1/0/2 through Gi1/0/10 are 'Link Down' and show '-' for test results and cable length. A 'Clear All' button is located to the right of the table.

Port	Type	Link Status	Test Result	Cable Length (M)	
Gi1/0/1	1000BASE-T	Link Up	Pair 1 Short at 1M	-	Clear
			Pair 2 Ok at 2M	-	
			Pair 3 Ok at 2M	-	
			Pair 4 Short at 1M	-	
Gi1/0/2	1000BASE-T	Link Down	-	-	Clear
Gi1/0/3	1000BASE-T	Link Down	-	-	Clear
Gi1/0/4	1000BASE-T	Link Down	-	-	Clear
Gi1/0/5	1000BASE-T	Link Down	-	-	Clear
Gi1/0/6	1000BASE-T	Link Down	-	-	Clear
Gi1/0/7	1000BASE-T	Link Down	-	-	Clear
Gi1/0/8	1000BASE-T	Link Down	-	-	Clear
Gi1/0/9	1000BASE-T	Link Down	-	-	Clear
Gi1/0/10	1000BASE-T	Link Down	-	-	Clear

Figure 10-1 Cable Diagnostics

The following parameters can be configured in the **Cable Diagnostics** 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.

Click the **Test** button to start the cable diagnostics test on the specified port(s).

Click the **Clear All** button to clear all the cable diagnostics results.

Click the **Clear** button to clear the cable diagnostics results on the specified port.

10.2 1DDM (Digital Diagnostic Monitoring)

10.2.1 DDM Settings

This window is used to configure and display the global settings associated with the DDM feature and the DDM shutdown settings on the specified port(s).

Click **DDM > DDM Settings** to view the following window:

DDM Settings		
DDM Global Settings		
Transceiver Monitoring Traps Alarm	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	Apply
Transceiver Monitoring Traps Warning	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
DDM Shutdown Settings		
Unit	From Port	To Port
1	Gi1/0/1	Gi1/0/1
State		Shutdown
Disabled		Alarm
Apply		
Unit 1 Settings		
Port	State	Shutdown
Gi1/0/21	Enabled	None
Gi1/0/22	Enabled	None
Gi1/0/23	Enabled	None
Gi1/0/24	Enabled	None
Te1/0/25	Enabled	None
Te1/0/26	Enabled	None
Te1/0/27	Enabled	None
Te1/0/28	Enabled	None

Figure 10-2 DDM Settings

The following parameters can be configured in the **DDM Global Settings** section:

Parameter	Description
Transceiver Monitoring Traps Alarm	Select to enable or disable the sending of transceiver monitoring alarm traps here.
Transceiver Monitoring Traps Warning	Select to enable or disable the sending of transceiver monitoring warning traps here.

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

The following parameters can be configured in the **DDM Shutdown 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 DDM feature on the specified port(s) here.
Shutdown	Select the shutdown behavior here. Options to choose from are: <ul style="list-style-type: none">• Alarm - Specifies to shut down the port when the configured alarm threshold range is exceeded.• Warning - Specifies to shut down the port when the configured warning threshold range is exceeded.• None - Specifies that the port will never be shut down regardless if the threshold ranges were exceeded or not. This is the default option.

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

10.2.2 DDM Temperature Threshold Settings

This window is used to configure and display the DDM temperature threshold settings on the specified port(s).

Click **DDM > DDM Temperature Threshold Settings** to view the following window:

DDM Temperature Threshold Settings

DDM Temperature Threshold Settings

Unit: 1 Port: Gi1/0/1 Action: Add Type: Low Alarm Value: (-128-127.996) Celsius

Unit 1 Settings

Port	Current	High Alarm (Celsius)	High Warning (Celsius)	Low Warning (Celsius)	Low Alarm (Celsius)
Gi1/0/21	19.902	78.000	73.000	-8.000	-13.000
Gi1/0/22	18.557	78.000	73.000	-8.000	-13.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-3 DDM Temperature Threshold Settings

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

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of temperature threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold value. The range is from -128 to 127.996 °C.

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

10.2.3 DDM Voltage Threshold Settings

This window is used to configure and display the DDM voltage threshold settings on the specified port(s).

Click **DDM > DDM Voltage Threshold Settings** to view the following window:

Port	Current	High Alarm (V)	High Warning (V)	Low Warning (V)	Low Alarm (V)
Gi1/0/21	3.271	3.700	3.600	3.000	2.900
Gi1/0/22	3.295	3.700	3.600	3.000	2.900

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-4 DDM Voltage Threshold Settings

The following parameters can be configured in the **DDM Voltage Threshold Settings** section:

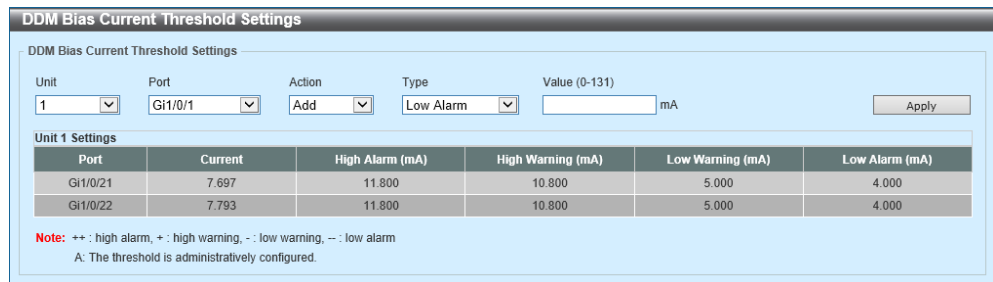
Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of voltage threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold value. The range is from 0 to 6.55 Volt.

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

10.2.4 DDM Bias Current Threshold Settings

This window is used to configure and display the DDM bias current threshold settings on the specified port(s).

Click **DDM > DDM Bias Current Threshold Settings** to view the following window:



DDM Bias Current Threshold Settings

DDM Bias Current Threshold Settings

Unit: 1 Port: Gi1/0/1 Action: Add Type: Low Alarm Value (0-131) mA

Apply

Unit 1 Settings

Port	Current	High Alarm (mA)	High Warning (mA)	Low Warning (mA)	Low Alarm (mA)
Gi1/0/21	7.697	11.800	10.800	5.000	4.000
Gi1/0/22	7.793	11.800	10.800	5.000	4.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-5 DDM Bias Current Threshold Settings

The following parameters can be configured in the **DDM Bias Current Threshold Settings** section:

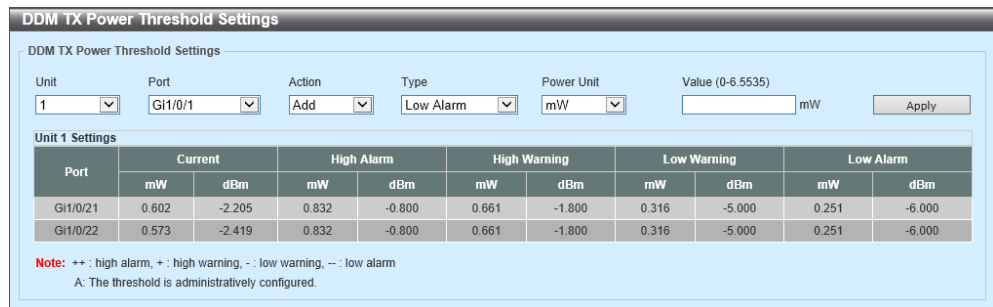
Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of bias current threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold value. The range is from 0 to 131 mA.

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

10.2.5 DDM TX Power Threshold Settings

This window is used to configure and display the DDM TX power threshold settings on the specified port(s).

Click **DDM > DDM TX Power Threshold Settings** to view the following window:



Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
Gi1/0/21	0.602	-2.205	0.832	-0.800	0.661	-1.800	0.316	-5.000	0.251	-6.000
Gi1/0/22	0.573	-2.419	0.832	-0.800	0.661	-1.800	0.316	-5.000	0.251	-6.000

Note: ++: high alarm, +: high warning, -: low warning, --: low alarm
A: The threshold is administratively configured.

Figure 10-6 DDM TX Power Threshold Settings

The following parameters can be configured in the **DDM TX Power Threshold Settings** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of TX power threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Power Unit	Select the power unit here. Options to choose from are mW and dBm .
Value	Enter the threshold value here. <ul style="list-style-type: none"> When selecting to specify the threshold value in mW, the range is from 0 to 6.5535 mW. When selecting to specify the threshold value in dBm, the range is from -40 to 8.1647 dBm.

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

10.2.6 DDM RX Power Threshold Settings

This window is used to configure and display the DDM RX power threshold settings on the specified port(s).

Click **DDM > DDM RX Power Threshold Settings** to view the following window:

DDM RX Power Threshold Settings

DDM RX Power Threshold Settings

Unit: 1 Port: Gi1/0/1 Action: Add Type: Low Alarm Power Unit: mW Value (0-6.5535): mW Apply

Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
Gi1/0/21	0.001	-29.331	1.000	0.000	0.794	-1.000	0.016	-18.013	0.010	-20.000
Gi1/0/22	0.000	-	1.000	0.000	0.794	-1.000	0.016	-18.013	0.010	-20.000

Note: ++: high alarm, +: high warning, -: low warning, --: low alarm
A: The threshold is administratively configured.

Figure 10-7 DDM RX Power Threshold Settings

The following parameters can be configured in the **DDM RX Power Threshold Settings** section:

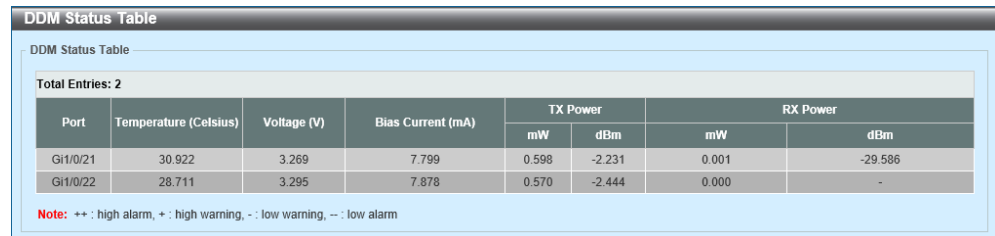
Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Port	Select the port that will be used here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of RX power threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Power Unit	Select the power unit here. Options to choose from are mW and dBm .
Value	Enter the threshold value here. <ul style="list-style-type: none"> When selecting to specify the threshold value in mW, the range is from 0 to 6.5535 mW. When selecting to specify the threshold value in dBm, the range is from -40 to 8.1647 dBm.

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

10.2.7 DDM Status Table

This window is used to display the DDM status table and information.

Click **DDM > DDM Status Table** to view the following window:



DDM Status Table

DDM Status Table

Total Entries: 2

Port	Temperature (Celsius)	Voltage (V)	Bias Current (mA)	TX Power		RX Power	
				mW	dBm	mW	dBm
Gi1/0/21	30.922	3.269	7.799	0.598	-2.231	0.001	-29.586
Gi1/0/22	28.711	3.295	7.878	0.570	-2.444	0.000	-

Note: ++ : high alarm, + : high warning, -: low warning, -- : low alarm

Figure 10-8 DDM Status Table

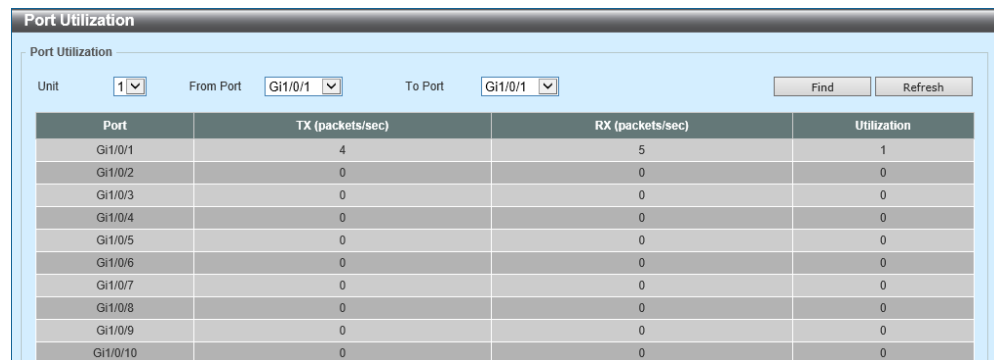
11 Monitoring

11.1 Utilization

11.1.1 Port Utilization

This window is used to display the port utilization table and information.

Click **Monitoring > Utilization > Port Utilization** to view the following window:



The screenshot shows the 'Port Utilization' window. At the top, there are dropdown menus for 'Unit' (set to 1), 'From Port' (set to Gi1/0/1), and 'To Port' (set to Gi1/0/1). There are 'Find' and 'Refresh' buttons. Below these is a table with four columns: Port, TX (packets/sec), RX (packets/sec), and Utilization. The table lists ports Gi1/0/1 through Gi1/0/10. Port Gi1/0/1 shows TX: 4, RX: 5, and Utilization: 1. All other ports show TX: 0, RX: 0, and Utilization: 0.

Port	TX (packets/sec)	RX (packets/sec)	Utilization
Gi1/0/1	4	5	1
Gi1/0/2	0	0	0
Gi1/0/3	0	0	0
Gi1/0/4	0	0	0
Gi1/0/5	0	0	0
Gi1/0/6	0	0	0
Gi1/0/7	0	0	0
Gi1/0/8	0	0	0
Gi1/0/9	0	0	0
Gi1/0/10	0	0	0

Figure 11-1 Port Utilization

The following parameters can be configured in the **Port Utilization** 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.

Click the **Find** button to display the port utilization information related to the specified port(s).

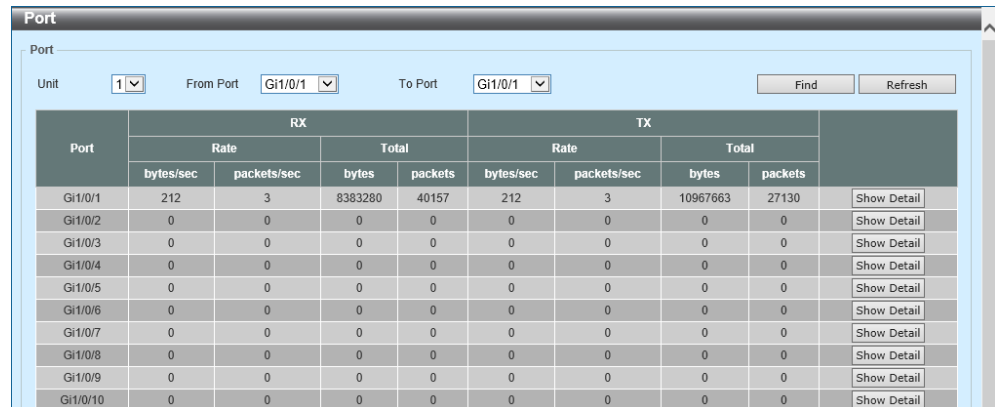
Click the **Refresh** button to refresh the information displayed in the table.

11.2 Statistics

11.2.1 Port

This window is used to display the port RX/TX statistics and information.

Click **Monitoring > Statistics > Port** to view the following window:



The screenshot shows a window titled "Port" with a search bar and a table of statistics. The search bar includes a "Unit" dropdown set to "1", "From Port" and "To Port" dropdowns both set to "Gi1/0/1", and "Find" and "Refresh" buttons. The table has columns for Port, RX Rate (bytes/sec, packets/sec), RX Total (bytes, packets), TX Rate (bytes/sec, packets/sec), TX Total (bytes, packets), and a "Show Detail" button for each row.

Port	RX				TX				Show Detail
	Rate		Total		Rate		Total		
	bytes/sec	packets/sec	bytes	packets	bytes/sec	packets/sec	bytes	packets	
Gi1/0/1	212	3	8383280	40157	212	3	10967663	27130	Show Detail
Gi1/0/2	0	0	0	0	0	0	0	0	Show Detail
Gi1/0/3	0	0	0	0	0	0	0	0	Show Detail
Gi1/0/4	0	0	0	0	0	0	0	0	Show Detail
Gi1/0/5	0	0	0	0	0	0	0	0	Show Detail
Gi1/0/6	0	0	0	0	0	0	0	0	Show Detail
Gi1/0/7	0	0	0	0	0	0	0	0	Show Detail
Gi1/0/8	0	0	0	0	0	0	0	0	Show Detail
Gi1/0/9	0	0	0	0	0	0	0	0	Show Detail
Gi1/0/10	0	0	0	0	0	0	0	0	Show Detail

Figure 11-2 Port

The following parameters can be configured in the **Port** section:

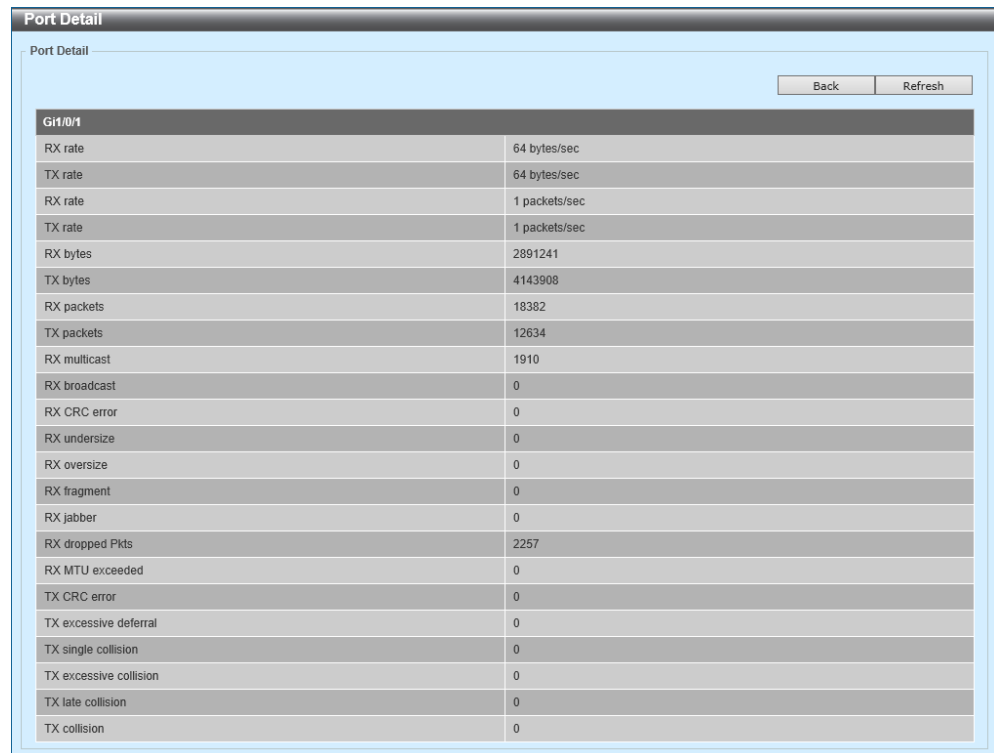
Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
From Port - To Port	Select the port(s) that will be used here.

Click the **Find** button to display the port statistics information related to the specified port(s).

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:



Gi1/0/1	
RX rate	64 bytes/sec
TX rate	64 bytes/sec
RX rate	1 packets/sec
TX rate	1 packets/sec
RX bytes	2891241
TX bytes	4143908
RX packets	18382
TX packets	12634
RX multicast	1910
RX broadcast	0
RX CRC error	0
RX undersize	0
RX oversize	0
RX fragment	0
RX jabber	0
RX dropped Pkts	2257
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 the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

11.2.2 Interface Counters

This window is used to display the interface counters statistics and information.

Click **Monitoring > Statistics > Interface Counters** to view the following window:

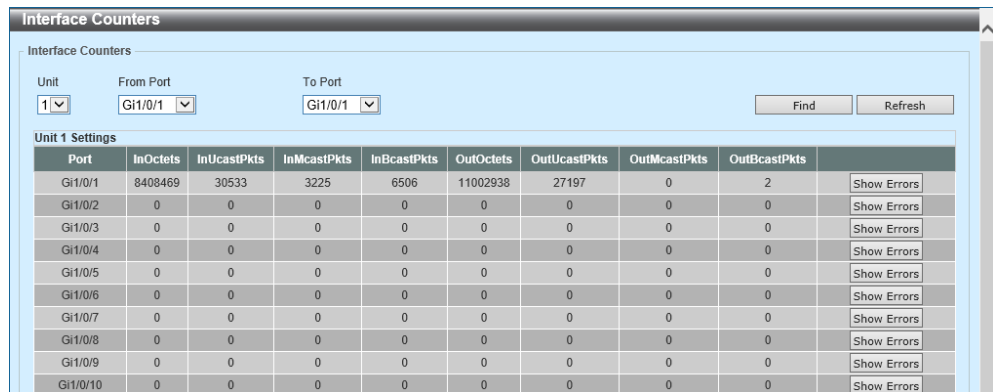


Figure 11-4 Interface Counters

The following parameters can be configured in the **Interface Counters** 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.

Click the **Find** button to display the interface counters related to the specified port(s).

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Errors** button to display detailed error information related to the entry.

Click the **Show Errors** button to view the following window:

Counters Errors	
Counters Errors	
<div>Back Refresh</div>	
Gi1/0/1 Counters Errors	
Undersize	0
Fcs-Err	0
Rcv-Err	0
InDiscard	2261
Xmit-Err	0
OutDiscard	0
Single-Col	0
Excess-Col	0
Multi-Col	0
Late-Col	0
DeferredTx	0
Symbol-Err	0

Figure 11-5 Interface Counters (Show Errors)

Click the **Back** button to return to the previous window.
Click the **Refresh** button to refresh the information displayed in the table.

11.2.3 Counters

This window is used to display and clear the link-change counters on the specified port(s).

Click **Monitoring > Statistics > Counters** to view the following window:

The screenshot shows the 'Counters' window with the following settings:

- Unit: 1
- From Port: Gi1/0/1
- To Port: Gi1/0/1

Buttons: Find, Refresh, Clear, Clear All

Unit 1 Settings

Port	linkChange	
Gi1/0/1	3	Show Detail
Gi1/0/2	0	Show Detail
Gi1/0/3	0	Show Detail
Gi1/0/4	0	Show Detail
Gi1/0/5	0	Show Detail
Gi1/0/6	0	Show Detail
Gi1/0/7	0	Show Detail
Gi1/0/8	0	Show Detail
Gi1/0/9	0	Show Detail
Gi1/0/10	0	Show Detail

Figure 11-6 Counters

The following parameters can be configured in the **Counters** 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.

Click the **Find** button to display the link-change counter information related to the specified port(s).

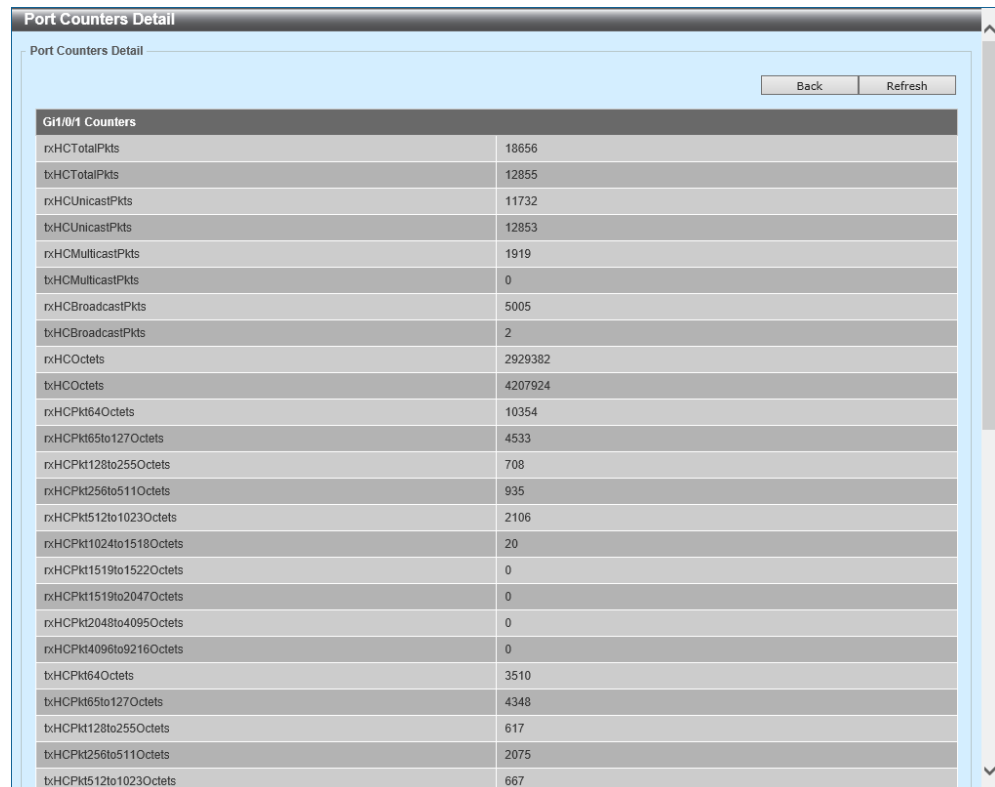
Click the **Refresh** button to refresh the information displayed in the table.

Click the **Clear** button to clear the link-change counter information related to the specified port(s).

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

Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:



Gi1/0/1 Counters	
rxHCTotalPkts	18656
txHCTotalPkts	12855
rxHCUnicastPkts	11732
txHCUnicastPkts	12853
rxHCMulticastPkts	1919
txHCMulticastPkts	0
rxHCBroadcastPkts	5005
txHCBroadcastPkts	2
rxHCOctets	2929382
txHCOctets	4207924
rxHCPkt64Octets	10354
rxHCPkt65to127Octets	4533
rxHCPkt128to255Octets	708
rxHCPkt256to511Octets	935
rxHCPkt512to1023Octets	2106
rxHCPkt1024to1518Octets	20
rxHCPkt1519to1522Octets	0
rxHCPkt1519to2047Octets	0
rxHCPkt2048to4095Octets	0
rxHCPkt4096to9216Octets	0
txHCPkt64Octets	3510
txHCPkt65to127Octets	4348
txHCPkt128to255Octets	617
txHCPkt256to511Octets	2075
txHCPkt512to1023Octets	667

Figure 11-7 Counters (Show Detail)

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

Click the **Refresh** button to refresh the information displayed in the table.

11.3 Mirror Settings

This window is used to configure and display the port mirror settings.

Click **Monitoring > Mirror Settings** to view the following window:

Mirror Settings

RSPAN VLAN Settings

VID List (2-4094)

Mirror Settings

Session Number

Destination ☐ Port Unit Port

Source ☐ Port Unit From Port To Port Frame Type

☐ CPU RX

Mirror Session Table

Session Number	Session Type	Show Detail
1	Local Session	<input type="button" value="Show Detail"/>

Figure 11-8 Mirror Settings

The following parameters can be configured in the **RSPAN VLAN Settings** section:

Parameter	Description
VID List	Enter the RSPAN VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 2 to 4094.

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

The following parameters can be configured in the **Mirror Settings** section:

Parameter	Description
Session Number	Select the mirror session number for this entry here. This number is between 1 and 4.
Destination	<p>Select and configure the destination settings for this port mirror entry here.</p> <p>Select the destination Port or Remote VLAN.</p> <ul style="list-style-type: none"> • Port - Select the Switch Unit ID and Destination Port number. • Remote VLAN - Select the Switch Unit ID and Destination Port number. Enter the VID in the space provided. The VID range is from 2 to 4094.
Source	<p>Select and configure the source settings for this port mirror entry here.</p> <p>Select the source Port, ACL or Remote VLAN.</p> <ul style="list-style-type: none"> • Port - Select the Switch Unit ID, From Port and To Port numbers. Select the Frame Type. Frame type options to choose from are: <ul style="list-style-type: none"> oBoth - Specifies that traffic in both the incoming and outgoing directions will be mirrored. oRX - Specifies that traffic in only the incoming direction will be mirrored. oTX - Specifies that traffic in only the outgoing direction will be mirrored. oCPU RX - Specifies to monitor CPU RX traffic. • ACL - Enter the ACL Name in the space provided. This can be up to 32 characters long. • Remote VLAN - Enter the remote VID in the space provided. The range is from 2 to 4094.

Click the **Apply** button to add a new entry.

Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Mirror Session Table** section:

Parameter	Description
Mirror Session Type	Select the mirror session type of information that will be displayed here. Options to choose from are All Session , Session Number , Remote Session , and Local Session . After selecting the Session Number option, select the session number from the drop-down menu. The range is from 1 to 4.

Click the **Find** button to find and display entries based on the search criteria specified.

Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:

The screenshot shows a window titled "Mirror Session Detail". Inside, there is a table with the following data:

Session Number	1
Session Type	Local Session
Both Port	Gi1/0/8-Gi1/0/9
RX Port	
TX Port	
CPU RX	
Flow Based Source	
Destination Port	Gi1/0/10

A "Back" button is located at the bottom right of the window.

Figure 11-9 Mirror Settings (Show Detail)

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

11.4 Device Environment

This window is used to display the current temperature reading, fan status and power module status of the switch.

Click **Monitoring > Device Environment** to view the following window:

Device Environment		
Detail Temperature Status		
Unit	Temperature Description/ID	Current/Threshold Range
1	Central Temperature /1	27C/11~79C
Status code: * temperature is out of threshold range		
Detail Fan Status		
Unit	Items	Status
1	Back Fan 1	Speed Low
	Back Fan 2	Speed Low
	Fan High Temperature Threshold(Celsius)	36
	Fan Low Temperature Threshold(Celsius)	33
Detail Power Status		
Unit	Power Module	Power Status
1	Power 1	In-operation
	Power 2	Empty

Figure 11-10 Device Environment

12 Eco Mode

12.1 Power Saving

This window is used to configure and display the power saving settings on the specified port(s).

Click **Eco Mode > Power Saving** to view the following window:

Port	Link	Type	Mode	Power Saving Mode
Gi1/0/1	Up	1000T	Auto(100F)	Disabled
Gi1/0/2	Down	1000T	Auto	Disabled
Gi1/0/3	Down	1000T	Auto	Disabled
Gi1/0/4	Down	1000T	Auto	Disabled
Gi1/0/5	Down	1000T	Auto	Disabled
Gi1/0/6	Down	1000T	Auto	Disabled
Gi1/0/7	Down	1000T	Auto	Disabled
Gi1/0/8	Down	1000T	Auto	Disabled
Gi1/0/9	Down	1000T	Auto	Disabled
Gi1/0/10	Down	1000T	Auto	Disabled

Figure 12-1 Power Saving

The following parameters can be configured in the **Power Saving 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.
Power Saving Mode	Select the power saving mode that will be used on the specified port(s). Options to choose from are: <ul style="list-style-type: none">• Disabled - Specifies to disable the power saving function.• Full - Specifies to use the power saving function to its full capacity.• Half - Specifies to use half of the power saving function capacity only. This is generally anything between zero and full capacity.

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

12.2 EEE (Energy Efficient Ethernet)

This window is used to configure and display the EEE settings on the specified port(s).

Click **Eco Mode > EEE** to view the following window:

EEE Settings			
Unit	From Port	To Port	State
1	Gi1/0/1	Gi1/0/1	Disabled
Apply			
Unit 1 Settings			
Port	State		
Gi1/0/1	Disabled		
Gi1/0/2	Disabled		
Gi1/0/3	Disabled		
Gi1/0/4	Disabled		
Gi1/0/5	Disabled		
Gi1/0/6	Disabled		
Gi1/0/7	Disabled		
Gi1/0/8	Disabled		
Gi1/0/9	Disabled		
Gi1/0/10	Disabled		

Figure 12-2 EEE

The following parameters can be configured in the **EEE 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 EEE feature on the specified port(s).

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

13 Toolbar

13.1 Save

13.1.1 Save Configuration

This window is used to save the running configuration as the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

Click **Save > Save Configuration** in the toolbar to view the following window:

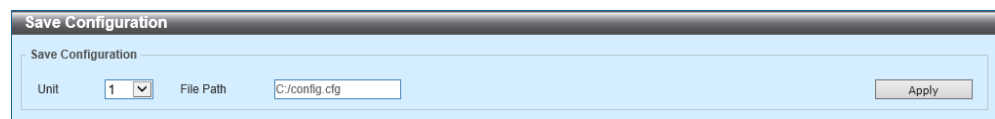


Figure 13-1 Save Configuration

The following parameters can be configured in the **Save Configuration** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
File Path	Enter the filename and path in the space provided.

Click the **Apply** button to save the configuration.

13.2 Tools

13.2.1 Firmware Upgrade & Backup

13.2.1.1 Firmware Upgrade from HTTP

This window is used to upgrade the firmware on the switch from a local PC using HTTP.

Click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP** in the toolbar to view the following window:

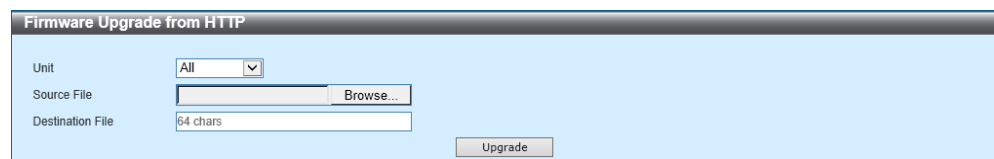


Figure 13-2 Firmware Upgrade from HTTP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Source File	Click the Browse button and navigate to the firmware file (on the local PC) that will be used in this upgrade.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to start the upgrade.

13.2.1.2 Firmware Upgrade from TFTP

This window is used to upgrade the firmware on the switch from a TFTP server.

Click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP** in the toolbar to view the following window:

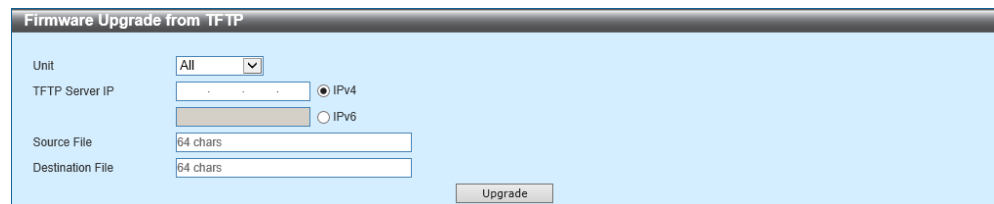


Figure 13-3 Firmware Upgrade from TFTP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
TFTP Server IP	Enter the IP address of the TFTP server here. <ul style="list-style-type: none">• IPv4 - Select and enter the IPv4 address of the TFTP server here.• IPv6 - Select and enter the IPv6 address of the TFTP server here.
Source File	Enter the source filename and path of the firmware file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to start the upgrade.

13.2.1.3 Firmware Upgrade from RCP

This window is used to upgrade the firmware on the switch from an RCP server.

Click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from RCP** in the toolbar to view the following window:

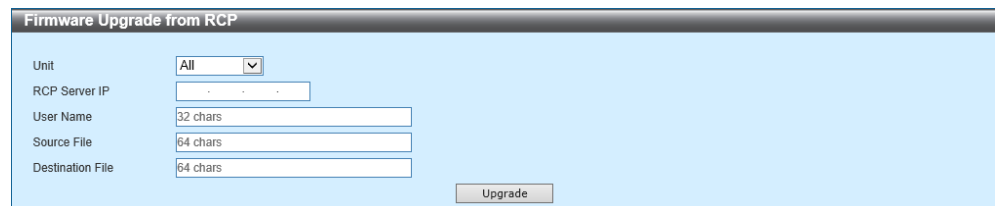


Figure 13-4 Firmware Upgrade from RCP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the firmware file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to start the upgrade.

13.2.1.4 Firmware Backup to HTTP

This window is used to save a backup copy of the firmware on the switch to a local PC using HTTP.

Click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP** in the toolbar to view the following window:

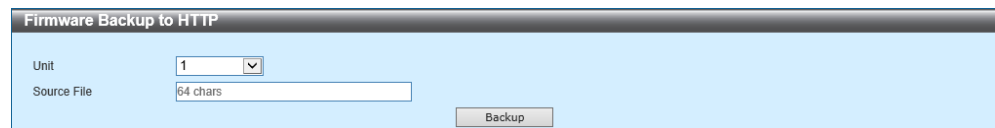


Figure 13-5 Firmware Backup to HTTP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.1.5 Firmware Backup to TFTP

This window is used to save a backup copy of the firmware on the switch to a TFTP server.

Click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP** in the toolbar to view the following window:

Figure 13-6 Firmware Backup to TFTP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
TFTP Server IP	Enter the IP address of the TFTP server here. <ul style="list-style-type: none"> IPv4 - Select and enter the IPv4 address of the TFTP server here. IPv6 - Select and enter the IPv6 address of the TFTP server here.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the TFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.1.6 Firmware Backup to RCP

This window is used to save a backup copy of the firmware on the switch to an RCP server.

Click **Tools > Firmware Upgrade & Backup > Firmware Backup to RCP** in the toolbar to view the following window:

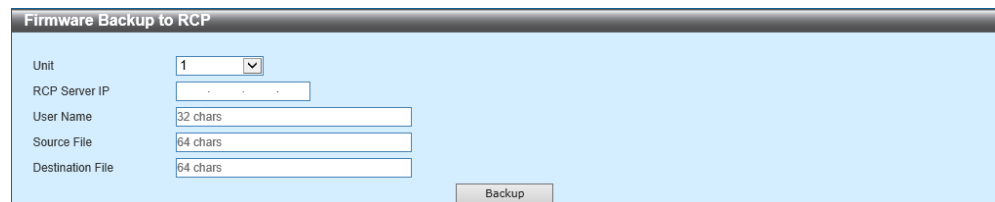


Figure 13-7 Firmware Backup to RCP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the RCP server here. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.2 Configuration Restore & Backup

13.2.2.1 Configuration Restore from HTTP

This window is used to restore the configuration on the switch from the local PC using HTTP.

Click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP** in the toolbar to view the following window:

Figure 13-8 Configuration Restore from HTTP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Source File	Click the Browse button and navigate to the configuration file (on the local PC) that will be used in this restore.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to restore and overwrite the running configuration file on the Switch. Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to start the restore.

13.2.2.2 Configuration Restore from TFTP

This window is used to restore the configuration on the switch from a TFTP server.

Click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP** in the toolbar to view the following window:

Figure 13-9 Configuration Restore from TFTP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
TFTP Server IP	Enter the IP address of the TFTP server here. <ul style="list-style-type: none"> • IPv4 - Select and enter the IPv4 address of the TFTP server here. • IPv6 - Select and enter the IPv6 address of the TFTP server here.
Source File	Enter the source filename and path of the configuration file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. <ul style="list-style-type: none"> • Select the running-config option to restore and overwrite the running configuration file on the Switch. • Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to start the restore.

13.2.2.3 Configuration Restore from RCP

This window is used to restore the configuration on the switch from an RCP server.

Click **Tools > Configuration Restore & Backup > Configuration Restore from RCP** in the toolbar to view the following window:

Figure 13-10 Configuration Restore from RCP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the configuration file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to restore and overwrite the running configuration file on the Switch. Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to start the restore.

13.2.2.4 Configuration Backup to HTTP

This window is used to save a backup copy of the configuration on the switch to a local PC using HTTP.

Click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP** in the toolbar to view the following window:

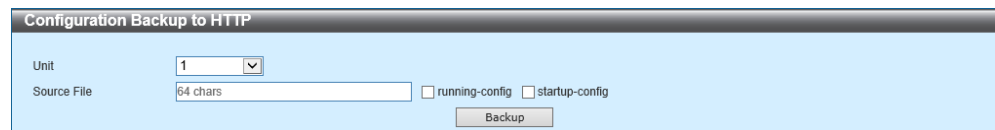


Figure 13-11 Configuration Backup to HTTP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. <ul style="list-style-type: none">• Select the running-config option to back up the running configuration file from the Switch.• Select the startup-config option to back up the start-up configuration file from the Switch.

Click the **Backup** button to start the backup.

13.2.2.5 Configuration Backup to TFTP

This window is used to save a backup copy of the configuration on the switch to a TFTP server.

Click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP** in the toolbar to view the following window:

Figure 13-12 Configuration Backup to TFTP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
TFTP Server IP	Enter the IP address of the TFTP server here. <ul style="list-style-type: none"> • IPv4 - Select and enter the IPv4 address of the TFTP server here. • IPv6 - Select and enter the IPv6 address of the TFTP server here.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. <ul style="list-style-type: none"> • Select the running-config option to back up the running configuration file from the Switch. • Select the startup-config option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.2.6 Configuration Backup to RCP

This window is used to save a backup copy of the configuration on the switch to an RCP server.

Click **Tools > Configuration Restore & Backup > Configuration Backup to RCP** in the toolbar to view the following window:

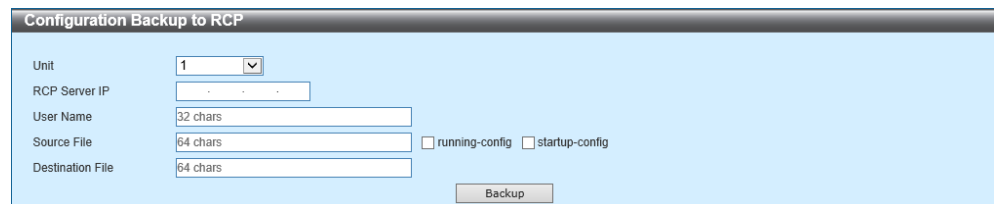


Figure 13-13 Configuration Backup to RCP

The following parameters can be configured:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. <ul style="list-style-type: none">• Select the running-config option to back up the running configuration file from the Switch.• Select the startup-config option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the RCP server. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.3 Log Backup

13.2.3.1 Log Backup to HTTP

This window is used to save a copy of the system log or the attack log on the switch to a local PC using HTTP.

Click **Tools > Log Backup > Log Backup to HTTP** in the toolbar to view the following window:

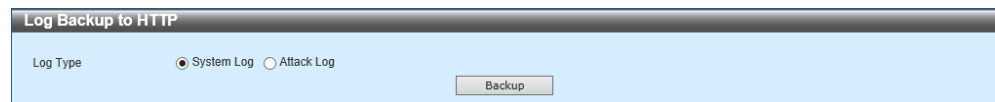


Figure 13-14 Log Backup to HTTP

The following parameters can be configured:

Parameter	Description
Log Type	Select the log type that will be backed up to the local PC using HTTP. <ul style="list-style-type: none">• System Log - Specifies that the system log will be backed up.• Attack Log - Specifies that the attack log will be backed up.

Click the **Backup** button to start the backup.

13.2.3.2 Log Backup to TFTP

This window is used to save a copy of the system log or the attack log on the switch to a TFTP server.

Click **Tools > Log Backup > Log Backup to TFTP** in the toolbar to view the following window:

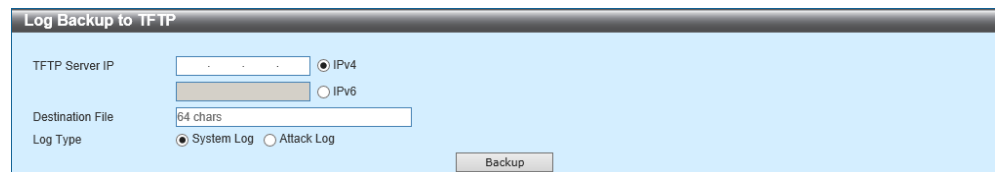


Figure 13-15 Log Backup to TFTP

The following parameters can be configured:

Parameter	Description
TFTP Server IP	Enter the IP address of the TFTP server here. <ul style="list-style-type: none">• IPv4 - Select and enter the IPv4 address of the TFTP server here.• IPv6 - Select and enter the IPv6 address of the TFTP server here.
Destination File	Enter the destination path and location where the log file should be stored on the TFTP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the TFTP server. <ul style="list-style-type: none">• System Log - Specifies that the system log will be backed up.• Attack Log - Specifies that the attack log will be backed up.

Click the **Backup** button to start the backup.

13.2.3.3 Log Backup to RCP

This window is used to save a copy of the system log or the attack log on the switch to an RCP server.

Click **Tools > Log Backup > Log Backup to RCP** in the toolbar to view the following window:

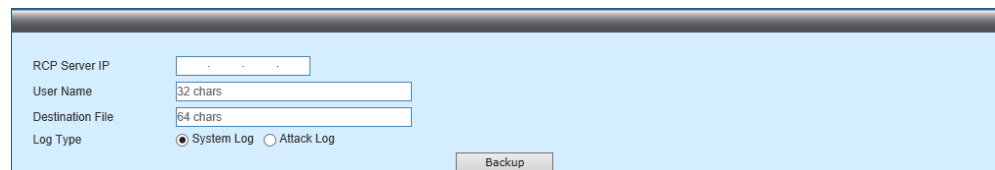


Figure 13-16 Log Backup to RCP

The following parameters can be configured:

Parameter	Description
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Destination File	Enter the destination path and location where the log file should be stored on the RCP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the RCP server. <ul style="list-style-type: none">• System Log - Specifies that the system log will be backed up.• Attack Log - Specifies that the attack log will be backed up.

Click the **Backup** button to start the backup.

13.2.4 Ping

This window is used to ping a destination IPv4/IPv6 address or domain name to test network connectivity. An access list can be applied to the ping request.

Click **Tools > Ping** in the toolbar to view the following window:

The screenshot shows the 'Ping' window with the following sections:

- Ping Access Class:** Includes an 'ACL Name' field with a 'Please Select' button, an 'Action' dropdown menu set to 'Add', and an 'Apply' button. Below this is a table showing 'Added Access Class' with one entry: 'S-IP-ACL'.
- IPv4 Ping:** Includes radio buttons for 'Target IPv4 Address' (selected) and 'Domain Name'. Fields for 'Ping Times (1-255)' (set to 255), 'Timeout (1-99)' (set to 1), and 'Source IPv4 Address'. A checkbox for 'Infinite' is checked. A 'Start' button is at the bottom right.
- IPv6 Ping:** Includes radio buttons for 'Target IPv6 Address' (selected) and 'Domain Name'. Fields for 'Ping Times (1-255)' (set to 255), 'Timeout (1-99)' (set to 1), and 'Source IPv6 Address'. A checkbox for 'Infinite' is checked. A 'Start' button is at the bottom right.

Figure 13-17 Ping

The following parameters can be configured in the **Ping Access Class** section:

Parameter	Description
ACL Name	Enter the name of the ACL that will be used here. This name can be up to 32 characters long. Click the Please Select button to select an existing ACL from the list.
Action	Select the action to be taken here. Options to choose from are Add and Clear .

Click the **Apply** button to use the selected access control list.

The following parameters can be configured in the **IPv4 Ping** section:

Parameter	Description
Target IPv4 Address	Select and enter the destination IPv4 address here.
Domain Name	Select and enter the destination domain name here. This can be up to 255 characters long.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. The range is from 1 to 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IPv4 address until the program is stopped.
Timeout	Enter the timeout period for Ping messages. If the packet fails to find the IPv4 address in this specified time, the Ping packet will be dropped. The range is from 1 to 99 seconds.
Source IPv4 Address	Enter the source IPv4 address. If the Switch has more than one IPv4 address, one of them can be entered here. When entered, this IPv4 address will be used as the source IPv4 address of the packets sent to the remote host.

Click the **Start** button to start the IPv4 ping.

The following parameters can be configured in the **IPv6 Ping** section:

Parameter	Description
Target IPv6 Address	Select and enter the destination IPv6 address here.
Domain Name	Select and enter the destination domain name here. This can be up to 255 characters long.
Ping Times	Enter the number of times desired to attempt to Ping the IPv6 address configured in this window. The range is from 1 to 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IPv6 address until the program is stopped.
Timeout	Enter the timeout period for Ping messages. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped. The range is from 1 to 99 seconds.
Source IPv6 Address	Enter the source IPv6 address. If the Switch has more than one IPv6 address, one of them can be entered here. When entered, this IPv6 address will be used as the source IPv6 address of the packets sent to the remote host.

Click the **Start** button to start the IPv6 ping.

Select and enter the **IPv4 Ping** parameters and click the **Start** button to view the following window:

The screenshot shows the 'Ping' window with the following sections:

- Ping Access Class:** Includes an 'ACL Name' field with a 'Please Select' button, an 'Action' dropdown menu set to 'Add', and an 'Apply' button. Below this is a table titled 'Added Access Class' with one entry: 'S-IP-ACL'.
- IPv4 Ping Result:** A text area displaying the following output:

```
[1] Reply from 192.168.70.1, time=10ms
[2] Reply from 192.168.70.1, time<10ms
[3] Reply from 192.168.70.1, time<10ms
[4] Reply from 192.168.70.1, time<10ms
Ping Statistics for 192.168.70.1
Packets: Sent = 4, Received = 4, Lost = 0
```

Below the text area are 'Stop' and 'Back' buttons.
- IPv6 Ping:** Includes radio buttons for 'Target IPv6 Address' (selected) and 'Domain Name'. The 'Target IPv6 Address' field contains '2233::1'. The 'Domain Name' field contains '255 chars'. There are fields for 'Ping Times (1-255)' (set to 'Infinite') and 'Timeout (1-99)' (set to '1' sec). There is also a 'Source IPv6 Address' field. A 'Start' button is at the bottom right.

Figure 13-18 Ping (Results)

Click the **Stop** button to stop the pinging process.
Click the **Back** button to return to the original Ping window.

Click the **Please Select** button to view the following window:

The screenshot shows the 'ACL Access List' window with a table of ACL entries:

Total Entries: 2			
	ID	ACL Name	ACL Type
<input type="radio"/>	1	S-IP-ACL	Standard IP ACL
<input type="radio"/>	11000	S-IP6-ACL	Standard IPv6 ACL

At the bottom right, there is a pagination control showing '1/1' and a 'Go' button. An 'OK' button is at the bottom right of the window.

Figure 13-19 Ping (Please Select)

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.
Click the **OK** button to use the selected access control list.

13.2.5 Trace Route

This window is used to trace a route to a destination IPv4/IPv6 address or domain name to test network connectivity.

Click **Tools > Trace Route** in the toolbar to view the following window:

The screenshot shows the 'Trace Route' window with two sections: 'IPv4 Trace Route' and 'IPv6 Trace Route'. Both sections have a 'Start' button. The 'IPv4 Trace Route' section has the following fields: 'IPv4 Address' (radio button selected), 'Domain Name' (radio button), 'Max TTL (1-255)' (30), 'Port (1-65535)' (33434), 'Timeout (1-65535)' (5 sec), and 'Probe Number (1-1000)' (1). The 'IPv6 Trace Route' section has the following fields: 'IPv6 Address' (radio button selected), 'Domain Name' (radio button), 'Max TTL (1-255)' (30), 'Port (1-65535)' (33434), 'Timeout (1-65535)' (5 sec), and 'Probe Number (1-1000)' (1).

Figure 13-20 Trace Route

The following parameters can be configured in the **IPv4 Trace Route** section:

Parameter	Description
IPv4 Address	Select and enter the destination IPv4 address here.
Domain Name	Select and enter the destination domain name here. This can be up to 255 characters long.
Max TTL	Enter the maximum Time-To-Live (TTL) value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range is from 1 to 255 hops.
Port	Enter the port number here. The range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. The range is from 1 to 65535 seconds. The default is 5 seconds.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. The default value is 1.

Click the **Start** button to start the IPv4 trace route.

The following parameters can be configured in the **IPv6 Trace Route** section:

Parameter	Description
IPv6 Address	Select and enter the destination IPv6 address here.
Domain Name	Select and enter the destination domain name here. This can be up to 255 characters long.
Max TTL	Enter the maximum TTL value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range is from 1 to 255 hops.
Port	Enter the port number here. The range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. The range is from 1 to 65535 seconds. The default is 5 seconds.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. The default value is 1.

Click the **Start** button to start the IPv6 trace route.

Select and enter the **IPv4 Trace Route** parameters and click the **Start** button to view the following window:

The screenshot shows a window titled "Trace Route". It is divided into two main sections. The top section, "IPv4 Trace Route Result", displays a list of four hops with their respective IP addresses and round-trip times: [1] <10 ms 192.168.249.134, [2] 20 ms 10.1.1.254, [3] <10 ms 192.168.249.134, and [4] <10 ms [172.19.10.38]. Below this list is a "Back" button. The bottom section, "IPv6 Trace Route", contains configuration fields for various parameters: "IPv6 Address" (set to 2233::1), "Domain Name" (set to 255 chars), "Max TTL (1-255)" (set to 30), "Port (1-65535)" (set to 33434), "Timeout (1-65535)" (set to 5 sec), and "Probe Number (1-1000)" (set to 1). A "Start" button is located at the bottom right of this section.

Figure 13-21 Trace Route (Results)

Click the **Back** button to return to the original Trace Route window.

13.2.6 Reset

This window is used to initiate a factory reset of the software configuration on the switch.

Click **Tools > Reset** in the toolbar to view the following window:

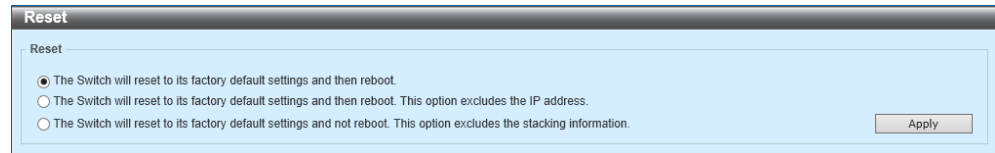


Figure 13-22 Reset

The following parameters can be configured:

Parameter	Description
Reset	<p>Select one of the following reset options:</p> <ul style="list-style-type: none"> • The Switch will reset to its factory default settings and then reboot. • The Switch will reset to its factory default settings and then reboot. This option excludes the IP address. • The Switch will reset to its factory default settings and not reboot. This option excludes the stacking information.

Click the **Apply** button to start the factory reset.

13.2.7 Reboot System

This window is used to initiate a reboot of the switch. Any new configuration changes made since the last reboot or power-up will be lost if the changes were not saved.

Click **Tools > Reboot System** in the toolbar to view the following window:

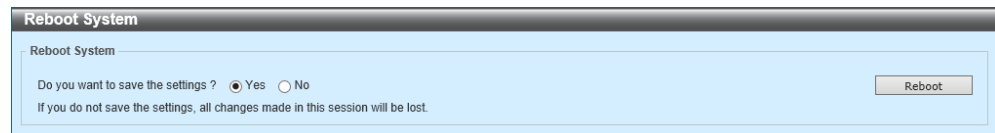


Figure 13-23 Reboot System

Select the **Yes** option to save the new configurations made before the reboot.

Select the **No** option to discard the new configurations made before the reboot.

Click the **Reboot** button to start the reboot.

13.3 Language

Select the language of the Web UI here. By default, English and Japanese can be selected.

Select the language in the toolbar as illustrated below:



Figure 13-24 Language

13.4 Logout

Click the **Logout** option, in the toolbar, to log out of the Web UI of the switch.



Figure 13-25 Logout

14 Appendix - System Log Entries

14.1 802.1X

ID	Log Description	Severity
1.	<p>Event Description: 802.1X Authentication successful.</p> <p>Log Message: [802.1X](<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid></p> <p>Parameters Description:</p> <p>method: Indicates local or RADIUS.</p> <p>username: The user that is being authenticated.</p> <p>macaddr: The MAC address of the authenticated device.</p> <p>portNum: The switch port number.</p> <p>vid: The authorized VLAN ID.</p>	Informational
2.	<p>Event Description: 802.1X Authentication failure.</p> <p>Log Message: [802.1X](<method>)Rejected user <username> (<macaddr>) on Port <portNum></p> <p>Parameters Description:</p> <p>method: local or RADIUS.</p> <p>username: TIndicateshe user that is being authenticated.</p> <p>macaddr: The MAC address of the authenticated device.</p> <p>portNum: The switch port number.</p>	Notice
3.	<p>Event Description: The 802.1X authentication table full, cannot authenticate new address.</p> <p>Log Message: [802.1X]Rejected <macaddr> on Port <portNum> (auth table was full)</p> <p>Parameters Description:</p> <p>macaddr: The MAC address of the authenticated device.</p> <p>portNum: The switch port number.</p>	Notice

14.2 AAA

ID	Log Description	Severity
1.	Event Description: Successful login. Log Message: Successful login through <Console Telnet SSH>(Username: <username>, IP: <ipaddr ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Informational
2.	Event Description: Login failed. Log Message: Login failed through <Console Telnet SSH> (Username: <username>, IP: <ipaddr ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Warning
3.	Event Description: Logout. Log Message: Logout through <Console Telnet SSH> (Username: <username>, IP: <ipaddr ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Informational
4.	Event Description: Session timed out. Log Message: <Console Telnet > session timed out (Username: <username>, IP: <ipaddr ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Informational
5.	Event Description: SSH server is enabled. Log Message: SSH server is enabled	Informational
6.	Event Description: SSH server is disabled. Log Message: SSH server is disabled	Informational
7.	Event Description: Authentication Policy is enabled. Log Message: Authentication Policy is enabled (Module: AAA)	Informational
8.	Event Description: Authentication Policy is disabled. Log Message: Authentication Policy is disabled (Module: AAA)	Informational
9.	Event Description: Login failed due to AAA server timeout or improper configuration. Log Message: Login failed through <Console Telnet SSH> from <ipaddr ipv6address> due to AAA server <ipaddr ipv6address> timeout or improper configuration (Username: <username>) Parameters Description: ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Warning

ID	Log Description	Severity
10.	<p>Event Description: Successful Enable Admin authenticated by AAA local or none or server.</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>Parameters Description:</p> <p>local: Enable admin by AAA local method.</p> <p>none: Enable admin by AAA none method.</p> <p>server: Enable admin by AAA server method.</p> <p>ipaddr: The IP address.</p> <p>ipv6address: The IPv6 address.</p> <p>username: The user name.</p>	Informational
11.	<p>Event Description: Enable Admin failed due to AAA server timeout 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>Parameters Description:</p> <p>ipaddr: The IP address.</p> <p>ipv6address: The IPv6 address.</p> <p>username: The user name.</p>	Warning
12.	<p>Event Description: Enable Admin failed authenticated by AAA local or server.</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>Parameters Description:</p> <p>local: Enable admin by AAA local method.</p> <p>server: Enable admin by AAA server method.</p> <p>ipaddr: The IP address.</p> <p>ipv6address: The IPv6 address.</p> <p>username: The user name.</p>	Warning
13.	<p>Event Description: Successful login authenticated by AAA local or none or server.</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>Parameters Description:</p> <p>local: Specify AAA local method.</p> <p>none: Specify none method.</p> <p>server: Specify AAA server method.</p> <p>ipaddr: The IP address.</p> <p>ipv6address: The IPv6 address.</p> <p>username: The user name.</p>	Informational
14.	<p>Event Description: Login failed authenticated by AAA local or server.</p> <p>Log Message: Login failed through <Console Telnet SSH> from <ipaddr ipv6address> authenticated by AAA <local server <ipaddr ipv6address>> (Username: <username>)</p> <p>Parameters Description:</p> <p>local: Specify AAA local method.</p> <p>server: Specify AAA server method.</p> <p>ipaddr: The IP address.</p> <p>ipv6address: The IPv6 address.</p> <p>username: The user name.</p>	Warning

14.3 ARP

ID	Log Description	Severity
1.	<p>Event Description: Gratuitous ARP detected duplicate IP. Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>) Parameters Description: ipaddr: The IP address which is duplicated with our device. macaddr: The MAC address of the device that has duplicated IP address as our device. unitID: 1.Interger value; 2.Represent the id of the device in the stacking system. portNum: 1.Interger value; 2.Represent the logic port number of the device. ipif_name: The name of the interface of the switch which has the conflict IP address.</p>	Warning

14.4 Authentication (2-step)

ID	Log Description	Severity
1.	<p>Event Description: 2-step Authentication successful.</p> <p>Log Message: [<step-mode>] (<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid></p> <p>Parameters Description:</p> <p>step-mode: Indicates 2-step authentication mode.</p> <p>method: Indicates local or RADIUS.</p> <p>username: The user that is being authenticated.</p> <p>macaddr: The MAC address of the authenticated device.</p> <p>portNum: The switch port number.</p> <p>vid: The authorized VLAN ID.</p>	Informational
2.	<p>Event Description: MAC-WEB Authentication failures.</p> <p>Log Message: [MAC-WEB] (<method>) Rejected at MAC auth <macaddr> on Port <portNum></p> <p>Parameters Description:</p> <p>method: Indicates local or RADIUS.</p> <p>macaddr: The MAC address of the authenticated device.</p> <p>portNum: The switch port number.</p>	Notice
3.	<p>Event Description: MAC-WEB Authentication failures.</p> <p>Log Message: [MAC-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum></p> <p>Parameters Description:</p> <p>method: Indicates local or RADIUS.</p> <p>username: The user that is being rejected.</p> <p>macaddr: The MAC address of the authenticated device.</p> <p>portNum: The switch port number.</p>	Notice
4.	<p>Event Description: MAC-802.1X Authentication failures.</p> <p>Log Message: [MAC-802.1X] (<method>) Rejected at MAC auth <macaddr> on Port <portNum></p> <p>Parameters Description:</p> <p>method: Indicates local or RADIUS.</p> <p>macaddr: The MAC address of the authenticated device.</p> <p>portNum: The switch port number.</p>	Notice
5.	<p>Event Description: MAC-802.1X Authentication failures.</p> <p>Log Message: [MAC-802.1X] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum></p> <p>Parameters Description:</p> <p>method: Indicates local or RADIUS.</p> <p>username: The user that is being rejected.</p> <p>macaddr: The MAC address of the authenticated device.</p> <p>portNum: The switch port number.</p>	Notice
6.	<p>Event Description: 802.1X-WEB Authentication failures.</p> <p>Log Message: [802.1X-WEB] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum></p> <p>Parameters Description:</p> <p>method: Indicates local or RADIUS.</p> <p>username: The user that is being rejected.</p> <p>macaddr: The MAC address of the authenticated device.</p> <p>portNum: The switch port number.</p>	Notice

ID	Log Description	Severity
7.	Event Description: 802.1 X-WEB Authentication failures. Log Message: [802.1X-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. username: The user that is being rejected. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

14.5 BPDU Guard

ID	Log Description	Severity
1.	Event Description: BPDU attack happened. Log Message: Port<portNum> enter BPDU under attacking state (mode: drop / block / shutdown) Parameters Description: portNum: The port number. mode: The BPDU current state.	Informational
2.	Event Description: BPDU attack automatically recover. Log Message: Port <portNum> recover from BPDU under attacking state automatically Parameters Description: portNum: The port number.	Informational
3.	Event Description: BPDU attack manually recover. Log Message: Port<portNum> recover from BPDU under attacking state manually Parameters Description: portNum: The port number.	Informational

14.6 Command

ID	Log Description	Severity
1.	<p>Event Description: Command Logging</p> <p>Log Message: "<command-str>" executed by <username> from <line>[, IP: <ip-address>]</p> <p>Parameters Description:</p> <p>username: The account name which executed this command.</p> <p>command-str: The command string which was executed successfully and cause a change in switch configuration.</p> <p>line: This parameter indicates the line mode which this command is executed from. (e.g. console, telnet, SSH)</p> <p>ip-address: (Optional) If the command is inputted from remote terminal (e.g. telnet, SSH), this parameter is needed.</p>	Informational

14.7 Configuration/Firmware

ID	Log Description	Severity
1.	<p>Event description: Firmware upgraded successfully.</p> <p>Log Message: [Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Informational
2.	<p>Event description: Firmware upgraded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning
3.	<p>Event description: Firmware uploaded successfully.</p> <p>Log Message: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Informational
4.	<p>Event description: Firmware uploaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning

ID	Log Description	Severity
5.	<p>Event description: Configuration downloaded successfully.</p> <p>Log Message: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Informational
6.	<p>Event description: Configuration downloaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning
7.	<p>Event description: Configuration uploaded successfully.</p> <p>Log Message: [Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Informational
8.	<p>Event description: Configuration uploaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning

ID	Log Description	Severity
9.	<p>Event description: Unknown type files downloaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning
10.	<p>Event description: Log message uploaded successfully.</p> <p>Log Message: Log message uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description:</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p>	Informational
11.	<p>Event description: Log message uploaded unsuccessfully.</p> <p>Log Message: Log message uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters description:</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p>	Informational

14.8 DAD

ID	Log Description	Severity
1.	Event description: When DUT receives Neighbor Solicitation (NS) message with reduplicated address in the DAD duration, DUT will add a log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages Parameters description: ipv6address : ipv6 address in Neighbor Solicitation Messages. interface-id : port interface ID.	Warning
2.	Event description: When DUT receives Neighbor Advertisement (NA) message with reduplicated address in the DAD duration, DUT will add a log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages Parameters description: ipv6address : ipv6 address in Neighbor Advertisement Messages. interface-id : port interface ID.	Warning

14.9 DDM

ID	Log Description	Severity
1.	<p>Event description: when the any of SFP parameters exceeds from the warning threshold.</p> <p>Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded</p> <p>Parameters description:</p> <p>interface-id: port interface ID.</p> <p>component: DDM threshold type. It can be one of the following types:</p> <p>temperature</p> <p>supply voltage</p> <p>bias current</p> <p>TX power</p> <p>RX power</p> <p>high-low: High or low threshold.</p>	Warning
2.	<p>Event description: when the any of SFP parameters exceeds from the alarm threshold.</p> <p>Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded</p> <p>Parameters description:</p> <p>interface-id: port interface ID.</p> <p>component: DDM threshold type. It can be one of the following types:</p> <p>temperature</p> <p>supply voltage</p> <p>bias current</p> <p>TX power</p> <p>RX power</p> <p>high-low: High or low threshold.</p>	Critical
3.	<p>Event description: when the any of SFP parameters recovers from the warning threshold.</p> <p>Log Message: Optical transceiver <interface-id> <component> back to normal</p> <p>Parameters description:</p> <p>interface-id: port interface ID.</p> <p>component: DDM threshold type. It can be one of the following types:</p> <p>temperature</p> <p>supply voltage</p> <p>bias current</p> <p>TX power</p> <p>RX power</p>	Warning

14.10 Debug Error

ID	Log Description	Severity
1.	Event description: system fatal error lead to reboot system. Log Message: [Uint <unitID>] System re-start reason: system fatal error Parameters description: unitID: The unit ID.	Emergencies
2.	Event description: CPU exception lead to reboot system. Log Message: [Uint <unitID>] System re-start reason: CPU exception Parameters description: unitID: The unit ID.	Emergencies

14.11 DHCPv6 Client

ID	Log Description	Severity
1.	Event description: DHCPv6 client interface administrator state changed. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled disabled] Parameters description: <ipif-name>: Name of the DHCPv6 client interface.	Informational
2.	Event description: DHCPv6 client obtains an ipv6 address from a DHCPv6 server. Log Message: DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name> Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
3.	Event description: The ipv6 address obtained from a DHCPv6 server starts renewing. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts renewing Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
4.	Event description: The ipv6 address obtained from a DHCPv6 server renews success. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> renews success Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
5.	Event description: The ipv6 address obtained from a DHCPv6 server starts rebinding. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
6.	Event description: The ipv6 address obtained from a DHCPv6 server rebinds success. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> rebinds success Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
7.	Event description: The ipv6 address from a DHCPv6 server was deleted. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> was deleted Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational

ID	Log Description	Severity
8.	Event description: DHCPv6 client PD interface administrator state changed. Log Message: DHCPv6 client PD on interface <intf-name> changed state to <enabled disabled> Parameters description: intf-name: Name of the DHCPv6 client PD interface.	Informational
9.	Event description: DHCPv6 client PD obtains an IPv6 prefix from a delegation router. Log Message: DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> Parameters description: ipv6networkaddr: ipv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
10.	Event description: The IPv6 prefix obtained from a delegation router starts renewing. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing Parameters description: ipv6networkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
11.	Event description: The IPv6 prefix obtained from a delegation router renews success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success Parameters description: ipv6networkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
12.	Event description: The IPv6 prefix obtained from a delegation router starts rebinding. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
13.	Event description: The IPv6 prefix obtained from a delegation router rebinds success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
14.	Event description: The IPv6 prefix from a delegation router was deleted. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational

14.12 DHCPv6 Relay

ID	Log Description	Severity
1.	Event description: DHCPv6 relay on a specify interface's administrator state changed. Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled disabled] Parameters description: <ipif-name>: Name of the DHCPv6 relay agent interface.	Informational

14.13 DHCPv6 Server

ID	Log Description	Severity
1.	Event description: The address of the DHCPv6 Server pool is used up. Log Message: The address of the DHCPv6 Server pool <pool-name> is used up Parameters description: <pool-name>: Name of the DHCPv6 Server pool.	Informational
2.	Event description: The number of allocated ipv6 addresses is equal to MAX-NUM (4096). Log Message: The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to MAX-NUM	

14.14 DNS Resolver

ID	Log Description	Severity
1.	Event description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted Log Message: DUPLICATEDDOMAIN: Duplicate Domain name case name: <domain name>, static IP: <static- ip>, dynamic IP:<dynamic-ip > Parameters description: domain name: the domain name string. ipaddr: IP address.	Informational

14.15 Dynamic ARP

ID	Log Description	Severity
1.	<p>Event description: This log will be generated when DAI detect invalid ARP packet.</p> <p>Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)</p> <p>Parameters description:</p> <p>type: The type of ARP packet, it indicates that ARP packet is request or ARP response.</p> <p>ip-address: IP address.</p> <p>mac-address: MAC address.</p> <p>vlan-id: VLAN ID.</p> <p>interface-id : The interface number.</p>	Warning
2.	<p>Event description: This log will be generated when DAI detect valid ARP packet.</p> <p>Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)</p> <p>Parameters description:</p> <p>type: The type of ARP packet, it indicates that ARP packet is request or ARP response.</p> <p>ip-address: IP address.</p> <p>mac-address: MAC address.</p> <p>vlan-id: VLAN ID.</p> <p>interface-id : The interface number.</p>	Informational

14.16 Fan

ID	Log Description	Severity
1.	Event description: Back Fan failed. Log Message: Unit <unitID>, Back Fan <value> failed Parameters description: unitID: The unit ID. value : Fans ID.	Critical
2.	Event description: Back Fan recovered. Log Message: Unit <unitID>, Back Fan <value> back to normal Parameters description: unitID: The unit ID. value : Fans ID.	Critical

14.17 Interface

ID	Log Description	Severity
1.	Event description: Port link up. Log Message: Port <port> link up, <nway> Parameters description: port: Represents the logical port number. nway: Represents the speed and duplex of link.	Informational
2.	Event description: Port link down. Log Message: Port <port> link down Parameters description: port: Represents the logical port number.	Informational

14.18 IP-Directed Broadcast

ID	Log Description	Severity
1.	Event description: IP Directed-broadcast rate exceed 50 packets per second on a certain subnet. Log Message: IP Directed Broadcast packet rate is high on subnet. [(IP: %s)] Parameters description: IP: The broadcast IP destination address.	Informational
2.	Event description: IP Directed-broadcast rate exceed 100 packets per second. Log Message: IP Directed Broadcast rate is high	Informational

14.19 IP Source Guard Verify

ID	Log Description	Severity
1.	<p>Event description: This message indicates that no hardware rule resource to set DHCP Snooping entry into IPSG table.</p> <p>Log Message: Failed to set IPSG entry due to no hardware rule resource. (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Interface <INTERFACE-ID>)</p> <p>Parameters description:</p> <p>IPADDR: IP address</p> <p>MACADDR: MAC address</p> <p>VLANID: The VLAN VID</p> <p>INTERFACE-ID : The interface number</p>	Warning

14.20 LACP

ID	Log Description	Severity
1.	Event description: Link Aggregation Group link up. Log Message: Link Aggregation Group < group_id > link up Parameters description: group_id: The group id of the link up aggregation group.	Informational
2.	Event description: Link Aggregation Group link down. Log Message: Link Aggregation Group < group_id > link down Parameters description: group_id: The group id of the link down aggregation group.	Informational
3.	Event description: Member port attach to Link Aggregation Group. Log Message: <ifname> attach to Link Aggregation Group <group_id> Parameters description: ifname: The interface name of the port that attach to aggregation group. group_id: The group id of the aggregation group that port attach to.	Informational
4.	Event description: Member port detach from Link Aggregation Group. Log Message: <ifname> detach from Link Aggregation Group <group_id> Parameters description: ifname: The interface name of the port that detach from aggregation group. group_id: The group id of the aggregation group that port detach from.	Informational

14.21 LLDP-MED

ID	Log Description	Severity
1.	<p>Event description: LLDP-MED topology change detected.</p> <p>Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters description:</p> <p>portNum: The port number.</p> <p>chassisType: chassis ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none">1. chassisComponent(1)2. interfaceAlias(2)3. portComponent(3)4. macAddress(4)5. networkAddress(5)6. interfaceName(6)7. local(7) <p>chassisID: chassis ID.</p> <p>portType: port ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none">1. interfaceAlias(1)2. portComponent(2)3. macAddress(3)4. networkAddress(4)5. interfaceName(5)6. agentCircuitId(6)7. local(7) <p>portID: port ID.</p> <p>deviceClass: LLDP-MED device type.</p>	Notice

ID	Log Description	Severity
2.	<p>Event description: Conflict LLDP-MED device type detected.</p> <p>Log Message: Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters description:</p> <p>portNum: The port number.</p> <p>chassisType: chassis ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) <p>chassisID: chassis ID.</p> <p>portType: port ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) <p>portID: port ID.</p> <p>deviceClass: LLDP-MED device type.</p>	Notice
3.	<p>Event description: Incompatible LLDP-MED TLV set detected.</p> <p>Log Message: Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters description:</p> <p>portNum: The port number.</p> <p>chassisType: chassis ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) <p>chassisID: chassis ID.</p> <p>portType: port ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) <p>portID: port ID.</p> <p>deviceClass: LLDP-MED device type.</p>	Notice

14.22 Loop Detection

ID	Log Description	Severity
1.	Event description: The loop detected between 2 ports or 2 LACP interfaces. Log Message: The loop detected between port/port-channel <portNum> and <portNum> Parameters description: portNum: The port number or LACP interface id.	Warning
2.	Event description: The loop detected on 1 port or 1 LACP interface. Log Message: The loop detected on port/port-channel <portNum> Parameters description: portNum: The port number or LACP interface id.	Warning
3.	Event description: The loop detected between 1 port and 1 LACP interface. Log Message: The loop detected between port/port-channel <portNum> and port/port-channel <portNum> Parameters description: portNum: The port number or port-channel number.	Warning
4.	Event description: Looped port or LACP interface auto recovery. Log Message: Port/Port-channel <portNum> auto recovery Parameters description: portNum: The port number or LACP interface id.	Informational

14.23 MAC-based Access Control

ID	Log Description	Severity
1.	Event description: MAC authentication successful. Log Message: [MAC](<method>)Authorized <macaddr> on Port <portNum> to VLAN <vid> Parameters description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number. vid: The authorized VLAN ID.	Informational
2.	Event description: MAC authentication failure. Log Message: [MAC](<method>)Rejected <macaddr> on Port <portNum> Parameters description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
3.	Event description: The MAC authentication table full, cannot authenticate new address. Log Message: [MAC]Rejected <macaddr> on Port <portNum> (auth table was full) Parameters description: macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

14.24 MSTP Debug Enhancement

ID	Log Description	Severity
1.	Event description: Topology changed. Log Message: Topology changed (Instance : <Instance-id>,<interface-id>, MAC:<macaddr>) Parameters description: Instance-id: Instance ID. interface-id: Port ID. macaddr: MAC address.	Notice
2.	Event description: Spanning Tree new Root Bridge. Log Message: [CIST CIST Regional MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :< priority>) Parameters description: Instance-id : Instance ID. macaddr: MAC address. priority: Priority value.	Notice
3.	Event description: Spanning Tree new Root Bridge. Log Message: [CIST CIST Regional MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :< priority>) Parameters description: Instance-id : Instance ID. macaddr: MAC address. priority: Priority value.	Informational
4.	Event description: Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
5.	Event description: New root port. Log Message: New root port selected (Instance:<instance-id>, <interface-id >) Parameters description: instance-id: Instance ID. interface-id: Port ID.	Notice
6.	Event description: Spanning Tree port status changed. Log Message: Spanning Tree port status change (Instance :< instance-id>, <interface-id>) <old-status> -> <new-status> Parameters description: instance-id: Instance ID. interface-id: Port ID. old_status: Old status. new_status: New status.	Notice
7.	Event description: Spanning Tree port role changed. Log Message: Spanning Tree port role change (Instance :< instance-id>, <interface-id>) <old-role> -> <new-role> Parameters description: instance-id: Instance ID. interface-id: Port ID. old_role: Old role. new_status: New role.	Informational
8.	Event description: Spanning Tree instance created. Log Message: Spanning Tree instance created. (Instance :< instance-id>) Parameters description: instance-id: Instance ID.	Informational

ID	Log Description	Severity
9.	Event description: Spanning Tree instance deleted. Log Message: Spanning Tree instance deleted. (Instance :< instance-id >) Parameters description: instance-id: Instance ID.	Informational
10.	Event description: Spanning Tree Version changed. Log Message: Spanning Tree version change (new version :< new-version>) Parameters description: new_version: New STP version.	Informational
11.	Event description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level change (name :< name>, revision level <revision-level>) Parameters description: name : New name. revision_level: New revision level.	Informational
12.	Event description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: < instance-id > delete vlan <startvlanid> [- <endvlanid>]) Parameters description: instance-id: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
13.	Event description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: < instance-id > add vlan <startvlanid> [- <endvlanid>]) Parameters description: instance-id: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
14.	Event description: Spanning Tree role 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 Parameters description: instance-id: Instance ID. interface-id: Port ID.	Informational

14.25 OSPF[ZEQUO6700RE/6600RE]

ID	Log Description	Severity
1.	Event description: OSPF interface link state changed. Log Message: OSPF-6-INTFSTATECHANGE: OSPF interface <intf-name> changed state to <status> Parameters description: intf-name: Name of OSPF interface. Status: Up or down.	Informational
2.	Event description: OSPF interface administrator state changed. Log Message: OSPF-6-INTFADMINCHANGE: OSPF protocol on interface <intf-name> changed state to <status> Parameters description: intf-name: Name of OSPF interface. Status: Enabled or disabled.	Informational
3.	Event description: One OSPF interface changed from one area to another. Log Message: OSPF-6-INTFAREACHANGE: OSPF interface <intf-name> changed from area <area-id> to area <area-id> Parameters description: intf-name: Name of OSPF interface. area-id: OSPF area ID.	Informational
4.	Event description: One OSPF neighbor state changed from Loading to Full. Log Message: OSPF-5-NBRLOADINGTOFULL: OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice
5.	Event description: One OSPF neighbor state changed from Full to Down. Log Message: OSPF-5-NBRFULLTODOWN: OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice
6.	Event description: One OSPF neighbor state's dead timer expired. Log Message: OSPF-5-DTIMEXPIRED: OSPF nbr <nbr-id> on interface <intf-name> dead timer expired Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice
7.	Event description: One OSPF virtual neighbor state changed from Loading to Full. Log Message: OSPF-5-VNBRLOADINGTOFULL: OSPF nbr <nbr-id> on virtual link changed state from Loading to Full Parameters description: nbr-id: Neighbor's router ID.	Notice
8.	Event description: One OSPF virtual neighbor state changed from Full to Down. Log Message: OSPF-5-VNBRFULLTODOWN: OSPF nbr <nbr-id> on virtual link changed state from Full to Down Parameters description: nbr-id: Neighbor's router ID.	Notice

ID	Log Description	Severity
9.	Event description: OSPF router ID was changed. Log Message: OSPF-6-RIDCHANGE: OSPF router ID changed to <router-id> Parameters description: router-id: OSPF router ID.	Informational
10.	Event description: OSPF state change. Log Message: OSPF-6-STATECHANGE: OSPF state changed to <state> Parameters description: state: Enabled or disabled.	Informational

14.26 Port Security

ID	Log Description	Severity
1.	Event description: Address full on a port Log Message: MAC address <mac-address> causes port security violation on <interface-id> Parameters description: macaddr: The violation MAC address. interface-id: The interface on which the violation occur.	Warning
2.	Event description: Address full on system. Log Message : Limit on system entry number has been exceeded	Warning

14.27 RADIUS

ID	Log Description	Severity
1.	<p>Event description: This log will be generated when RADIUS assigned a valid VLAN ID attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>)</p> <p>Parameters description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>vid: The assign VLAN ID that authorized by from RADIUS server.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>username: It indicates the username for authentication.</p>	Informational
2.	<p>Event description: This log will be generated when RADIUS assigned a valid bandwidth attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface-id> (Username: <username>)</p> <p>Parameters description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>direction: It indicates the direction for bandwidth control, e.g.: ingress or egress.</p> <p>threshold: The assign threshold of bandwidth that authorized by from RADIUS server.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>username: It indicates the username for authentication.</p>	Informational
3.	<p>Event description: This log will be generated when RADIUS assigned a valid priority attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port < interface-id> (Username: <username>)</p> <p>Parameters description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>priority: The assign priority that authorized by from RADIUS server.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>username: It indicates the username for authentication.</p>	Informational
4.	<p>Event description: This log will be generated when RADIUS assigned ACL script but fails to apply to the system due to insufficient resource.</p> <p>Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port < interface-id> (<acl-script>)</p> <p>Parameters description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>username: It indicates the username for authentication.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>acl-script: The assign ACL script that authorized by from RADIUS server.</p>	Warning
5.	<p>Event description: This log will be generated when fail to assign access-list number.</p> <p>Log Message: Local assigns [USERNAME] filter-id ID failure at port INTERFACE-ID</p> <p>Parameters description:</p> <p>username: It indicates the username for authentication.</p> <p>filter-id: It indicates access-list number.</p> <p>interface-id: It indicates the port number of the client authenticated.</p>	Warning

14.28 RRP

ID	Log Description	Severity
1.	Event description: The status in "Master Node" changes from "Failed" to "Complete." Log Message: Ring topology was recovered to complete	Notice
2.	Event description: The status in "Master Node" changes from "Complete" to "Failed." Log Message: Ring topology was failed	Warning
3.	Event description: Master or Transit node flush its Forwarding Database based on RRP packets or state machine. Log Message: FDB was flushed	Informational
4.	Event description: The RRP status in "Transit Node" changes to "Link-Up." Log Message: RRP ring status was changed to Link-Up	Warning
5.	Event description: The RRP status in "Transit Node" changes to "Link-Down." Log Message: RRP ring status was changed to Link-Down	Notice
6.	Event description: The RRP status in "Transit Node" changes to "Pre-Forwarding". Log Message: RRP ring status was changed to Pre-Forwarding	Informational
7.	Event description: Worked ring guard function at the specific domain and port. Log Message: Ring Guard was activated on "<domain-name>" domain at port <port> Parameters description: <domain name>: target domain name. <port num>: target port number worked ring guard function.	Informational

14.29 SNMP

ID	Log Description	Severity
1.	Event Description: SNMP request received with invalid community string. Log Message: SNMP request received from <ipaddr> with invalid community string Parameters Description: ipaddr: The IP address.	Informational

14.30 Stacking

ID	Log Description	Severity
1.	Event description: Hot insertion. Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
2.	Event description: Hot removal. Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
3.	Event description: Stacking topology change. Log Message: Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>) Parameters description: Stack_TP_TYPE: The stacking topology type is one of the following: 1. Ring, 2. Chain. unitID: Box ID. Macaddr: MAC address.	Informational
4.	Event description: Backup master changed to master. Log Message: Backup master changed to master. Master (Unit: <unitID>) Parameters description: unitID: Box ID.	Informational
5.	Event description: Slave changed to master. Log Message: Slave changed to master. Master (Unit: <unitID>) Parameters description: unitID: Box ID.	Informational
6.	Event description: Box ID conflict. Log Message: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>) Parameters description: unitID: Box ID. macaddr: The MAC addresses of the conflicting boxes.	Critical

14.31 System

ID	Log Description	Severity
1.	Event description: System start up. Log Message: [Unit <unitID>] System started up Parameters description: unitID: The unit ID.	Critical
2.	Event description: Save current configuration to flash. Log Message: [Unit <unitID>] Configuration saved to flash by console (Username: <username>) Parameters description: unitID: The unit ID. username: The user name.	Informational
3.	Event description: Power fail. Log Message: Unit <unitID> Power <powerID> failed Parameters description: unitID: The unit ID. powerID: The power ID.	Critical
4.	Event description: Power is recovered. Log Message: Unit <unitID> Power <powerID> back to normal Parameters description: unitID: The unit ID. powerID: The power ID.	Critical
5.	Event description: Save system configuration from remote. Log Message: [Unit <unitID>] Configuration saved to flash (Username: <username>, IP: <ipaddr>) Parameters description: unitID: The unit ID. username: The user name. ipaddr: The ip address.	Informational
6.	Event description: System power up and start up. Log Message: [Unit <unitID>] System cold start Parameters description: unitID: The unit ID.	Critical
7.	Event description: System reboot and start up. Log Message: [Unit <unitID>] System warm start Parameters description: unitID: The unit ID.	Critical

14.32 Telnet

ID	Log Description	Severity
1.	Event description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
2.	Event description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Warning
3.	Event description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
4.	Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational

14.33 Temperature

ID	Log Description	Severity
1.	Event description: Temperature sensor enters alarm state. Log Message: Uint <unitID> Sensor:<sensorID> detects abnormal temperature <temperature> Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The current temperature of the sensor.	Critical
2.	Event description: Temperature recovers to normal. Log Message: Uint <unitID> Sensor:<sensorID> temperature back to normal Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The temperature.	Critical

14.34 Traffic Control

ID	Log Description	Severity
1.	Event description: Broadcast, Multicast or Unicast storm occurrence. Log Message: Broadcast Multicast Unicast> storm is occurring on <interface-id> Parameters description: interface-id: The interface ID on which a storm is occurring.	Warning
2.	Event description: Broadcast, Multicast or Unicast storm cleared. Log Message: <Broadcast Multicast Unicast> storm is cleared on <interface-id> Parameters description: interface-id: The interface ID on which a storm is cleared.	Informational
3.	Event description: Port shut down due to a packet storm. Log Message: <interface-id> is currently shut down due to the <Broadcast Multicast Unicast> storm Parameters description: Interface-id: The interface ID on which is error-disabled by storm.	Warning

14.35 UDLD

ID	Log Description	Severity
1.	Event description: A unidirectional link is detected on this port. Log Message: Unidirectional link detection on <INTERFACE-ID> Parameters description: INTERFACE-ID: The interface name.	Warning

14.36 Voice VLAN

ID	Log Description	Severity
1.	Event description: When a new voice device is detected on an interface. Log Message: New voice device detected (<interface-id>, MAC: < mac-address >) Parameters description: interface-id: Interface name. mac-address: Voice device MAC address	Informational
2.	Event description: When an interface which is in auto voice VLAN mode joins the voice VLAN. Log Message: < interface-id > add into voice VLAN <vid > Parameters description: interface-id: Interface name.s vid: VLAN ID.	Informational
3.	Event description: When an interface leaves the Voice VLAN and at the same time, no voice device is detected in the aging interval for that interface, the log message will be sent. Log Message: < interface-id > remove from voice VLAN <vid > Parameters description: interface-id: Interface name. vid: LAN ID.	Informational

14.37 VRRP

ID	Log Description	Severity
1.	Event description: One virtual router state becomes Master. Log Message: VRRP-6-STATEMASTER: VR <vr-id> at interface <intf-name> switch to Master role Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational
2.	Event description: One virtual router state becomes Backup. Log Message: VRRP-6-STATEBACKUP: VR <vr-id> at interface <intf-name> switch to Backup state Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational
3.	Event description: One virtual router state becomes Init. Log Message: VRRP-6-STATEINIT: VR <vr-id> at interface <intf-name> switch to Init state Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational
4.	Event description: Authentication type mismatch of one received VRRP advertisement message. Log Message: VRRP-4-AUTHYPEMIS: Authentication type mismatch on VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning
5.	Event description: Authentication checking fail of one received VRRP advertisement message. Log Message: VRRP-4-AUTHFAIL: Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based. Auth-type: VRRP interface authentication type.	Warning
6.	Event description: Checksum error of one received VRRP advertisement message. Log Message: VRRP-4-BADCHK: Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning
7.	Event description: Virtual router ID mismatch of one received VRRP advertisement message. Log Message: VRRP-4-VRIDMIS: Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning

ID	Log Description	Severity
8.	Event description: Advertisement interval mismatch of one received VRRP advertisement message. Log Message: VRRP-4-ADVMIS: Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning
9.	Event description: A virtual MAC address is added into switch L2 table. Log Message: VRRP-5-MACADD: Added a virtual MAC <vrrp-mac-addr> into L2 table Parameters description: vrrp-mac-addr: VRRP virtual MAC address.	Notice
10.	Event description: A virtual MAC address is deleted from switch L2 table. Log Message: VRRP-5-MACDEL: Deleted a virtual MAC <vrrp-mac-addr> from L2 table Parameters description: vrrp-mac-addr: VRRP virtual MAC address.	Notice
11.	Event description: A virtual MAC address is adding into switch L3 table. Log Message: VRRP-5-MACL3ADD: Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table Parameters description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address	Notice
12.	Event description: A virtual MAC address is deleting from switch L3 table. Log Message: VRRP-5-MACL3DEL: Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table. Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Notice
13.	Event description: Failed when adding a virtual MAC into switch chip L2 table. Log Message: VRRP-3-MACADDFAIL: Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode> Parameters description: vrrp-mac-addr: VRRP virtual MAC address. vrrp-errcode: Errcode of VRRP protocol behavior.	Error
14.	Event description: Failed when deleting a virtual MAC from switch chip L2 table. Log Message: VRRP-3-MACDELFAIL: Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode> Parameters description: vrrp-mac-addr: VRRP virtual MAC address. vrrp-errcode: Errcode of VRRP protocol behavior.	Error
15.	Event description: Failed when adding a virtual MAC into switch L3 table. The L3 table is full. Log Message: VRRP-3-MACL3FULL: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full Parameters description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address.	Error

ID	Log Description	Severity
16.	<p>Event description: Failed when adding a virtual MAC into switch L3 table. The port where the MAC is learned from is invalid.</p> <p>Log Message: VRRP-3-BADMAC: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid</p> <p>Parameters description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address. mac-port: port number of VRRP virtual MAC.</p>	Error
17.	<p>Event description: Failed when adding a virtual MAC into switch L3 table. The interface where the MAC is learned from is invalid.</p> <p>Log Message: VRRP-3-BADINTF: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid</p> <p>Parameters description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address. mac-intf: interface id on which VRRP virtual MAC address is based.</p>	Error
18.	<p>Event description: Failed when adding a virtual MAC into switch L3 table. The box where the MAC is learned from is invalid.</p> <p>Log Message: VRRP-3-BADUNIT: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid</p> <p>Parameters description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address. mac-box: stacking box number of VRRP virtual MAC.</p>	Error
19.	<p>Event description: Failed when adding a virtual MAC into switch chip's L3 table.</p> <p>Log Message: VRRP-3-MACL3ADDFAIL: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode></p> <p>Parameters description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address. vrrp-errcode: Err code of VRRP protocol behavior.</p>	Error
20.	<p>Event description: Failed when deleting a virtual MAC from switch chip's L3 table.</p> <p>Log Message: VRRP-3-MACL3DELFAIL: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode></p> <p>Parameters description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address. vrrp-errcode: Err code of VRRP protocol behavior.</p>	Error

14.38 WAC

ID	Log Description	Severity
1.	Event description: When a client host fails to authenticate. Log Message: [WEB](RADIUS/Local) Rejected user <string> (<macaddr>) on Port <portNum> Parameters description: string: User name. macaddr: MAC address. portNum : The port number.	Warning
2.	Event description: When a client host authenticated successful. Log Message: [WEB](RADIUS/Local)Authorized user <string> (<macaddr>) on Port <portNum> to VLAN <vlanNum> Parameters description: string: User name. macaddr: MAC address. portNum : The port number. vlanNum : The VLAN number.	Informational
3.	Event description: When client table full. Log Message: [WEB]Rejected <macaddr> on Port <portNum> (auth table was full) Parameters description: macaddr: MAC address. portNum : The port number.	Notice

14.39 Web

ID	Log Description	Severity
1.	Event description: Successful login via web. Log Message: "Successful login through Web (Username: <username>, IP: <ipaddr>)" Parameters description: username: user name. ipaddr: IP address from where user access the switch via web.	Informational
2.	Event description: Login failed via web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>)" Parameters description: username: user name. ipaddr: IP address from where user access the switch via web.	Warning
3.	Event description: Successful login from HTTPS. Log Message: Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters description: username: user name. ipaddr: IP address from where user access the switch via secure web.	Informational
4.	Event description: login failed via secure web. Log Message: Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters description: username: user name. ipaddr: IP address from where user access the switch via secure web.	Warningsssss ssss
5.	Event description: Log upload successfully. Log Message: Log message uploaded by WEB successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <ipaddr>, File Name: <filename>) Parameters description: username: user name. ipaddr: IP address from where user access the switch. macaddr: MAC address of client. server IP: TFTP server IP address. filename: the log file name.	Informational
6.	Event description: Log upload unsuccessfully. Log Message: Log message uploaded by WEB unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <ipaddr>, File Name: <filename>) Parameters description: username: user name. ipaddr: IP address from where user access the switch. macaddr: MAC address of client. server IP: TFTP server IP address. filename: the log file name.	Informational

15 Appendix - System Trap Entries

15.1 BPDU Guard

ID	Trap Name	Trap Description	OID
1.	mnoBpduProtectionUnderAttackingTrap	BPDU attack happened, enter drop / block / shutdown mode. Binding objects: mnoBpduProtectionPortIndex The port interface. (2) mnoBpduProtectionPortMode Drop / block / shutdown mode.	1.3.6.1.4.1.396.5.5.3.4.0.1
2.	mnoBpduProtectionRecoveryTrap	BPDU attack automatically recover. Binding objects: mnoBpduProtectionPortIndex The port interface. mnoBpduProtectionRecoveryMethod Auto/manual recovers.	1.3.6.1.4.1.396.5.5.3.4.0.2

15.2 DDM

ID	Trap Name	Trap Description	OID
1.	mnoDdmAlarmTrap	<p>The trap is sent when any parameter value exceeds the alarm threshold value or recovers to normal status depending on the configuration of the trap action.</p> <p>Binding objects:</p> <p>mnoDdmPort The port number</p> <p>mnoDdmThresholdType The ddm threshold type</p> <p>temperature/voltage/bias/txpower/rxpower</p> <p>mnoDdmThresholdExceedType The threshold that was exceeded was a high alarm threshold or a low alarm threshold</p> <p>(4) mnoDdmThresholdExceedOrRecover The GBIC is exceeding its ddm threshold or recover to normal status</p>	1.3.6.1.4.1.396.5.5.1.4.0.1
2.	mnoDdmWarningTrap	<p>The trap is sent when any parameter value exceeds the warning threshold value or recovers to normal status depending on the configuration of the trap action.</p> <p>Binding objects:</p> <p>mnoDdmPort The port number</p> <p>mnoDdmThresholdType The ddm threshold type</p> <p>temperature/voltage/bias/txpower/rxpower</p> <p>mnoDdmThresholdExceedType The threshold that was exceeded was a high warning threshold or a low warning threshold</p> <p>(4) mnoDdmThresholdExceedOrRecover The GBIC is exceeding its ddm threshold or recover to normal status</p>	1.3.6.1.4.1.396.5.5.1.4.0.2

15.3 DHCP Server Protect

ID	Trap Name	Trap Description	OID
1.	mnoFilterDetectedTrap	Send trap when an illegal DHCP server is detected. The same illegal DHCP server IP address detected is just sent once to the trap receivers within the log ceasing unauthorized duration. Binding objects: mnoFilterDetectedIP The illegal DHCP server IP address. mnoFilterDetectedport The port interface.	1.3.6.1.4.1.396. 5.5.3.7.0.1

15.4 Fan

ID	Trap Name	Trap Description	OID
1.	mnoFanFailure	This notification will send out when the fan failure.	1.3.6.1.4.1.396.5.5.1.1
2.	mnoFanRecovery	This notification will send out when the fan recovery.	1.3.6.1.4.1.396.5.5.1.5

15.5 Gratuitous ARP

ID	Trap Name	Trap Description	OID
1.	mnoAgentGratuitousARPTrap	<p>The trap is sent when IP address conflicted.</p> <p>Binding objects:</p> <p>agentGratuitousARPIpAddr The conflicted IP address received in the gratuitous ARP packet.</p> <p>agentGratuitousARPMacAddr The sender's MAC address in the gratuitous ARP packet.</p> <p>agentGratuitousARPPortNumber The switch's port number who received the gratuitous ARP packet.</p> <p>agentGratuitousARPInterfaceName The switch's IP interface name who received the gratuitous ARP.</p>	1.3.6.1.4.1.396.5.5.3.6.0.1

15.6 LLDP-MED

ID	Trap Name	Trap Description	OID
1.	IldpRemTablesChange	A IldpRemTablesChange notification is sent when the value of IldpStatsRemTableLastChangeTime changes. Binding objects: (1) IldpStatsRemTablesInserts (2) IldpStatsRemTablesDeletes (3) IldpStatsRemTablesDrops (4) IldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2.	IldpXMedTopologyChangeDetected	A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding objects: (1) IldpRemChassisIdSubtype (2) IldpRemChassisId (3) IldpXMedRemDeviceClass	1.0.8808.1.1.2.1.5.4795.0.1

15.7 Loop Detect

ID	Trap Name	Trap Description	OID
1.	mnoLoopDetectNotification	Indicates the network loop occurred.	1.3.6.1.4.1.396.5.5.2.1
2.	mnoLoopRecoveryNotification	Indicates the network loop resolved.	1.3.6.1.4.1.396.5.5.2.2

15.8 MAC-based Access Control

ID	Trap Name	Trap Description	OID
1.	mnoMacBasedAccessControlLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: mnoMacBasedAuthInfoMacIndex The host MAC addresses. mnoMacBasedAuthInfoPortIndex The port interface. mnoMacBasedAuthVID The VLAN ID.	1.3.6.1.4.1.396.5.5.3.2.0.1
2.	mnoMacBasedAccessControlLoggedFail	The trap is sent when a MAC-based Access Control host login fails. Binding objects: mnoMacBasedAuthInfoMacIndex The host MAC addresses. mnoMacBasedAuthInfoPortIndex The port interface. mnoMacBasedAuthVID The VLAN ID.	1.3.6.1.4.1.396.5.5.3.2.0.2
3.	mnoMacBasedAccessControlAgesOut	The trap is sent when a MAC-based Access Control host ages out. Binding objects: mnoMacBasedAuthInfoMacIndex The host MAC addresses. (2) mnoMacBasedAuthInfoMacIndex The port interface. (3) mnoMacBasedAuthVID The VLAN ID.	1.3.6.1.4.1.396.5.5.3.2.0.3

15.9 MAC Notification

ID	Trap Name	Trap Description	OID
1.	mnoL2macNotification	<p>This trap indicates the MAC addresses variation in address table</p> <p>Binding objects: mnoL2macNotifyInfo</p> <p>Devices MAC address change information. And the detailed information include :</p> <p>Operation Code + MAC address + Box ID + Interface ID + Zero.</p> <p>Operation Code: 1, 2 1 means learned a new MAC address 2 means deleted an old MAC address.</p> <p>Box ID: The switch box ID Interface ID: The Interface ID learned or deleted on the box.</p> <p>Zero: Used to separate each message (Operate Code + MAC address + Box ID + Port Number).</p>	1.3.6.1.4.1.396 .5.5.3.1.0.1

15.10 MSTP

ID	Trap Name	Trap Description	OID
1.	newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1,3,6,1,2,1,17.0.1
2.	topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional	1,3,6,1,2,1,17.0.2

15.11 PIM6[ZEQUO6700RE/6600RE]

ID	Trap Name	Trap Description	OID
1.	pimNeighborLoss	A pimNeighborLoss notification signifies the loss of an adjacency with a neighbor. This notification should be generated when the neighbor timer expires, and the router has no other neighbor on the same interface with the same IP version and a lower IP address than itself. This notification is generated whenever the counter pimNeighborLossCount is incremented, subject to the rate limit specified by pimNeighborLossNotificationsPeriod. Binding objects: (1) pimNeighborUpTime	1.3.6.1.2.1.157.0.1
2.	pimInvalidRegister	A pimInvalidRegister notification signifies that an invalid PIM Register message was received by this device. This notification is generated whenever the counter pimInvalidRegisterMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidRegisterNotificationPeriod. Binding objects: (1) pimGroupMappingPimMode (2) pimInvalidRegisterAddressType (3) pimInvalidRegisterOrigin (4) pimInvalidRegisterGroup (5) pimInvalidRegisterRp	1.3.6.1.2.1.157.0.2
3.	pimInvalidJoinPrune	A pimInvalidJoinPrune notification signifies that an invalid PIM Join/Prune message was received by this device. This notification is generated whenever the counter pimInvalidJoinPruneMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidJoinPruneNotificationPeriod. Binding objects: (1) pimGroupMappingPimMode (2) pimInvalidJoinPruneAddressType (3) pimInvalidJoinPruneOrigin (4) pimInvalidJoinPruneGroup (5) pimInvalidJoinPruneRp (6) pimNeighborUpTime	1.3.6.1.2.1.157.0.3
4.	pimRPMappingChage	A pimRPMappingChange notification signifies a change to the active RP mapping on this device. This notification is generated whenever the counter pimRPMappingChangeCount is incremented, subject to the rate limit specified by pimRPMappingChangeNotificationPeriod. Binding objects: (1) pimGroupMappingPimMode (2) pimGroupMappingPrecedence	1.3.6.1.2.1.157.0.4

ID	Trap Name	Trap Description	OID
5.	pimInterfaceElection	A pimInterfaceElection notification signifies that a new DR or DF has been elected on a network. This notification is generated whenever the counter pimInterfaceElectionWinCount is incremented, subject to the rate limit specified by pimInterfaceElectionNotificationPeriod. Binding objects: (1) pimInterfaceAddressType (2) pimInterfaceAddress	1.3.6.1.2.1.157.0.5

15.12 Port Security

ID	Trap Name	Trap Description	OID
1.	mnoL2PortSecurityViolationTrap	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out. Binding objects: mnoPortSecPortIndex The port interface. mnoL2PortSecurityViolationMac The host MAC addresses.	1.3.6.1.4.1.396. 5.5.3.3.0.1

15.13 Port

ID	Trap Name	Trap Description	OID
1.	linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6. 3.1.1.5.4
2.	linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6. 3.1.1.5.3

15.14 RMON

ID	Trap Name	Trap Description	OID
1.	risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1)alarmIndex (2)alarmVariable (3)alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16 .0.1
2.	fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1)alarmIndex (2) alarmVariable (3)alarmSampleType (4)alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16 .0.2

15.15 SNMP Authentication

ID	Trap Name	Trap Description	OID
1.	authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5

15.16 Stacking

ID	Trap Name	Trap Description	OID
1.	mnoUnitInsert	Unit Hot Insert notification. Binding objects: mnoUnitMgmtId. The Box ID of hot inserted device mnoUnitMgmtMacAddr. The MAC address of hot insert device	1.3.6.1.4.1.39 6.5.5.1.3.0.1
2.	mnoUnitRemove	Unit Hot Remove notification. Binding objects: mnoUnitMgmtId. The Box ID of hot removed device mnoUnitMgmtMacAddr. The MAC address of hot removed device	1.3.6.1.4.1.39 6.5.5.1.3.0.2
3.	mnoUnitFailure	Unit Failure notification. Binding objects: mnoUnitMgmtId. The Box ID of failure device	1.3.6.1.4.1.39 6.5.5.1.3.0.3
4.	mnoUnitTPChange	The stacking topology change notification. Binding objects: mnoStackTopologyType The current stacking topology after change: chain(1) ring(2) mnoUnitMgmtId The Master's Box ID mnoUnitMgmtMacAddr The Master's MAC address	1.3.6.1.4.1.39 6.5.5.1.3.0.4
5.	mnoUnitRoleChange	The stacking unit role change notification. Binding objects: mnoStackRoleChangeType The type of stacking role change: backup-to-master(1) slave-to-master(2) mnoUnitMgmtId The Master's Box ID	1.3.6.1.4.1.39 6.5.5.1.3.0.5

15.17 System

ID	Trap Name	Trap Description	OID
1.	coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
2.	warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2

15.18 Temperature

ID	Trap Name	Trap Description	OID
1.	mnoTemperatureRising Alarm	This notification will send out when current temperature more than high threshold.	1.3.6.1.4.1.396.5.5.1.2.1
2.	mnoTemperatureFalling Alarm	This notification will send out when current temperature falling from high threshold.	1.3.6.1.4.1.396.5.5.1.2.2

15.19 Traffic Control

ID	Trap Name	Trap Description	OID
1.	mnoPktStormOccurred	When packet storm is detected by packet storm mechanism and take shutdown as action. Binding objects: mnoPktStormCtrlPortIndex The port interface.	1.3.6.1.4.1.396.5.5.3.5.0.1
2.	mnoPktStormCleared	When the packet storm is clear. Binding objects: mnoPktStormCtrlPortIndex The port interface.	1.3.6.1.4.1.396.5.5.3.5.0.2
3.	mnoPktStormDisablePort	When the port is disabled by the packet storm mechanism. Binding objects: mnoPktStormCtrlPortIndex The port interface.	1.3.6.1.4.1.396.5.5.3.5.0.3

15.20 VRRP

ID	Trap Name	Trap Description	OID
1.	vrrpTrapNewMaster	The newMaster trap indicates that the sending agent has transitioned to 'Master' state. Binding objects: (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.68.0.1
2.	vrrpTrapAuthFailure	A vrrpAuthFailure trap signifies that a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional. Binding objects: (1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	1.3.6.1.2.1.68.0.2

© Panasonic Electric Works Networks Co., Ltd. 2022

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>

P0222-3102