

S3900 Series Switches Web Management Guide

Models: S3900-48T4S; S3900-24T4S; S3900-24F4S

Contents

1. Monitor.....	1
1.1 Monitor.....	1
2. Configure.....	1
2.1 Jumbo Frame.....	1
3. Port.....	1
3.1 Port Information.....	1
3.1.1 Configure.....	2
3.1.2 Transceiver.....	2
3.1.3 Cable Test.....	3
3.1.4 Port Isolate.....	4
3.2 Statistics.....	4
3.2.1 Port Statistics.....	4
3.2.2 Port History Management.....	5
3.2.3 Port History Info.....	5
4. Vlan.....	6
4.1 Vlan Management.....	6
4.1.1 Member List.....	6
4.1.2 Member Setting.....	7
4.1.3 Configure Interface.....	7
4.1.4 GVRP Status.....	7
4.1.5 GVRP Configure Interface.....	8
4.1.6 GVRP Dynamic VLAN.....	8
4.1.7 GVRP Dynamic VLAN Member.....	9
4.1.8 Protocol Mapping Table.....	9
4.1.9 Protocol Interface Mapping.....	10
4.1.10 IP Subnet-based Vlan.....	10
4.1.11 MAC-Based Vlan.....	11
4.1.12 Vlan Translation.....	12
4.2 QinQ.....	12
4.3 Voice Vlan.....	14
4.4 L2PT.....	16
4.5 MAC Address.....	17
4.5.1 Dynamic MAC.....	17
4.5.2 Clear Dynamic MAC.....	17
4.5.3 Configure Aging.....	18
4.5.4 Learning Status.....	18
4.5.5 Static Mac Setting.....	18
4.5.6 MAC Notification.....	19
4.6 Port Mirroring.....	20
4.6.1 Local Port Mirror.....	20
4.6.2 RSPAN.....	21
4.7 Static Link Aggregation.....	23
4.7.1 Static Group.....	23
4.7.2 Static Group Member.....	23
4.7.3 Static Group Management.....	24
4.8 LACP.....	24

4.8.1 Group Member.....	24
4.8.2 Group Link Configuration.....	25
4.8.3 Group LACP Configuration.....	25
4.8.4 Counters.....	26
4.8.5 Show Dynamic Group Member.....	26
4.9 Trunk Group Load Balance.....	26
4.10 Spanning Tree Protocol.....	27
4.10.1 STP Global Setting.....	27
4.10.2 STP-RSTP Global Management.....	27
4.10.3 STP-RSTP Interface Status.....	29
4.10.4 MST Global Management.....	32
4.10.5 MST Information.....	32
4.10.6 MST List.....	33
4.10.7 MST Member.....	34
4.10.8 MST Interface.....	34
4.11 IGMP Snooping.....	35
4.11.1 Global Setting.....	35
4.11.2 Current Multicast Router.....	36
4.11.3 Static Multicast Router.....	37
4.11.4 Static Member.....	37
4.11.5 VLAN Information.....	38
4.11.6 Configure Interface.....	40
4.11.7 Forwarding Entry.....	40
4.11.8 Query Statistics.....	41
4.11.9 VLAN Statistics.....	42
4.11.10 Port Statistics.....	43
4.11.11 Group Statistics.....	43
4.12 IGMP Filtering and Throttling.....	44
4.12.1 Global Setting.....	44
4.12.2 Filter Profile.....	45
4.12.3 Filter Range.....	46
4.12.4 Configure Filter Interface.....	46
4.13 MLD Snooping.....	47
4.13.1 Global Setting.....	47
4.13.2 Immediate Leave Status.....	48
4.13.3 Current Multicast Router.....	49
4.13.4 Static Multicast Router.....	49
4.13.5 Current Member.....	50
4.13.6 Static Member.....	51
4.13.7 Group Information.....	52
4.13.8 Statistics.....	52
4.14 MVR For IPv4.....	54
4.14.1 Configure Global.....	54
4.14.2 Configure Domain.....	55
4.14.3 Show Configure Profile.....	56
4.14.4 Add Configure Profile.....	57
4.14.5 Show Associate Profile.....	57
4.14.6 Add Associate Profile.....	58

4.14.7 Configure Interface.....	58
4.14.8 Show Static Group Member.....	59
4.14.9 Add Static Group Member.....	60
4.14.10 Show Member.....	60
4.14.11 Show Query Statistics.....	61
4.14.12 Show VLAN Statistics.....	62
4.14.13 Show Port Statistics.....	62
4.14.14 Show Group Statistics.....	63
4.15 MVR For IPv6.....	64
4.15.1 Configure Global.....	64
4.15.2 Configure Domain.....	65
4.15.3 Show Configure Profile.....	66
4.15.4 Add Configure Profile.....	66
4.15.5 Show Associate Profile.....	67
4.15.6 Add Associate Profile.....	67
4.15.7 Configure Interface.....	68
4.15.8 Show Static Group Member.....	69
4.15.9 Add Static Group Member.....	69
4.15.10 Show Member.....	70
4.15.11 Show Query Statistics.....	70
4.15.12 Show VLAN Statistics.....	71
4.15.13 Show Port Statistics.....	72
4.15.14 Show Group Statistics.....	73
4.15.15 Global Configuration.....	74
4.16 LLDP.....	74
4.16.1 Global Configuration.....	74
4.16.2 InterfaceConfiguration.....	75
4.16.3 Civil Address Type.....	77
4.16.4 Local Information.....	78
4.16.5 Peer Information.....	79
4.16.6 Statistics.....	83
4.17 ERPS.....	84
4.17.1 Domain Configuration.....	84
4.17.2 Statistics.....	87
4.18 Loopback Detection.....	87
4.18.1 Global Configuration.....	88
4.18.2 Interface Configuration.....	88
4.19 UDLD.....	89
4.19.1 Global Configuration.....	89
4.19.2 Interface Configuration.....	90
4.19.3 Neighbor Info.....	91
4.20 Rate Limit.....	91
4.21 Storm Control.....	92
4.22 Stacking.....	93
4.22.1 Global Configuration.....	93
4.22.2 Master Configuration.....	93
4.23 PPPoE.....	93
4.23.1 Global Configuration.....	93

4.23.2 Interface Configuration.....	94
4.23.3 Statistics.....	94
4.24 ACL.....	95
4.24.1 ACL Configuration.....	95
4.24.2 Rule Configuration.....	95
4.24.3 Bind Interface.....	100
4.25 CoS.....	100
4.26 QoS.....	101
4.26.1 Egress Queue.....	101
4.26.2 Trust Mode.....	102
4.26.3 QoS Map.....	102
4.26.4 Class.....	107
4.26.5 Class Match.....	108
4.26.6 Policy.....	108
4.26.7 Policy Map.....	108
4.26.8 Bind Interface.....	109
4.27 AAA.....	110
4.27.1 Global Configuration.....	110
4.27.2 Server Configuration.....	111
4.27.3 Server List.....	111
4.27.4 Accounting Strategy.....	111
4.27.5 Interface Accounting.....	112
4.27.6 Authorization Strategy.....	112
4.27.7 Authorization Configuration.....	112
4.28 Web Authentication.....	113
4.28.1 Global Configuration.....	113
4.28.2 Interface Configuration.....	113
4.28.3 Host List.....	113
4.29 802.1X.....	114
4.29.1 Global Configuration.....	114
4.29.2 Interface Configuration.....	114
4.29.3 Statistics.....	114
4.30 MAC Authentication.....	115
4.30.1 Global Configuration.....	115
4.30.2 Interface Configuration.....	115
4.30.3 MAC Filter.....	115
4.30.4 MAC Authentication Information.....	116
4.31 HTTPS.....	116
4.31.1 Global Configuration.....	116
4.31.2 Update Certificate.....	116
4.32 SSH.....	117
4.32.1 Global Configuration.....	117
4.32.2 Key of Switch.....	117
4.32.3 Key of User.....	118
4.33 Port Security.....	118
4.34 DAI.....	119
4.34.1 Global Configuration.....	119
4.34.2 VLAN Configuration.....	120

4.34.3 Interface Configuration.....	120
4.34.4 Statistics.....	121
4.34.5 Log.....	121
4.35 Login IP Management.....	122
4.36 DoS Protection.....	122
4.37 IPv4 DHCP Snooping.....	123
4.37.1 Global Configuration.....	123
4.37.2 VLAN Configuration.....	124
4.37.3 Interface Configuration.....	125
4.37.4 Information.....	125
4.38 IPv6 DHCP Snooping.....	126
4.38.1 Global Configuration.....	126
4.38.2 VLAN Configuration.....	127
4.38.3 Interface Configuration.....	128
4.38.4 Legal Client Table.....	128
4.39 IPv4 Source Guard.....	129
4.39.1 Interface Configuration.....	129
4.39.2 Static Table.....	130
4.39.3 Dynamic Binding.....	130
4.40 IPv6 Source Guard.....	131
4.40.1 Interface Configuration.....	131
4.40.2 Static Table.....	132
4.40.3 Dynamic Binding.....	133
4.41 Application Filter.....	134
4.42 CPU Guard.....	134
5. Network.....	135
5.1 IP Interface Configuration.....	135
5.2 IPv6 Configuration.....	136
5.2.1 Global Configuration.....	136
5.2.2 Interface Configuration.....	136
5.2.3 RA-Guard.....	138
5.2.4 Address Configuration.....	138
5.2.5 Neighbor List.....	139
5.2.6 Statistics.....	139
5.2.7 MTU.....	140
5.3 ARP.....	140
5.3.1 Global Configuration.....	140
5.3.2 Proxy ARP.....	140
5.3.3 Static ARP.....	141
5.3.4 ARP Address List.....	141
5.4 Static Routes.....	142
5.4.1 Routing Table.....	142
5.4.2 Static Routes.....	142
6. Maintenance.....	143
6.1 System Description.....	143
6.2 User Management.....	143
6.3 SNMP.....	144
6.3.1 Global Configuration.....	144

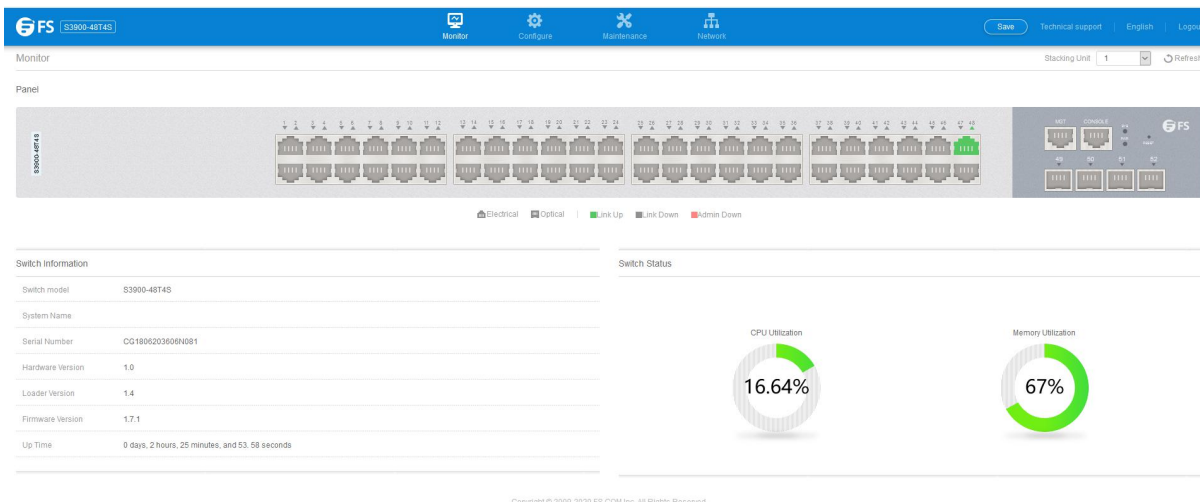
6.3.2 Community.....	144
6.3.3 Local Engine ID.....	145
6.3.4 Remote Engine ID.....	145
6.3.5 View Configuration.....	145
6.3.6 Group Configuration.....	146
6.3.7 SNMPv3 Local User.....	147
6.3.8 SNMPv3 Remote User.....	148
6.3.9 Trap.....	149
6.3.10 Statistics.....	150
6.4 RMON.....	151
6.4.1 Alarm Group.....	151
6.4.2 Event Group.....	152
6.4.3 History Group.....	153
6.4.4 Statistics Group.....	154
6.5 Cluster.....	155
6.5.1 Global Configuration.....	155
6.5.2 Member Configuration.....	155
6.5.3 Candidate Information.....	156
6.6 DNS.....	156
6.6.1 Global Configuration.....	156
6.6.2 Domain Names.....	157
6.6.3 Name Servers.....	157
6.6.4 Static Table.....	158
6.6.5 Cache.....	158
6.7 DHCP.....	159
6.7.1 DHCP Options.....	159
6.7.2 Relay.....	159
6.8 OAM.....	159
6.8.1 Interface.....	159
6.8.2 Statistics.....	160
6.8.3 Event Log.....	161
6.8.4 Peer Information.....	161
6.8.5 Loopback Result.....	162
6.8.6 Loopback Test.....	162
6.9 CFM.....	163
6.9.1 Global Configuration.....	163
6.9.2 Interface Configuration.....	165
6.9.3 MD Management.....	165
6.9.4 MD Details.....	166
6.9.5 MA Management.....	166
6.9.6 MA Details.....	167
6.9.7 MEP Management.....	168
6.9.8 Remote MEP Management.....	169
6.9.9 Transmit Link Trace.....	169
6.9.10 Transmit Loopback.....	170
6.9.11 Transmit Delay Measure.....	170
6.9.12 Local MEP.....	171
6.9.13 Local MEP Details.....	172

6.9.14 Local MIP.....	172
6.9.15 Remote MEP.....	173
6.9.16 Remote MEP Details.....	173
6.9.17 Link Trace Cache.....	174
6.9.18 Fault Notification Generator.....	175
6.9.19 Continuity Check Error.....	176
6.10 Time Setting.....	176
6.10.1 Time Configuration.....	176
6.10.2 SNTP Server.....	177
6.10.3 NTP Server.....	177
6.10.4 NTP Authentication Key.....	178
6.10.5 Time Zone Configuration.....	178
6.10.6 Summer Time.....	179
6.11 Log Management.....	180
6.11.1 Log Information.....	180
6.11.2 Global Configuration.....	180
6.11.3 Remote Log Server.....	180
6.11.4 SMTP.....	181
6.12 System Maintenance.....	182
6.12.1 File Management.....	182
6.12.2 System Reboot.....	184
6.13 Ping Diagnostics.....	184
6.14 Trace Route.....	184

1. Monitor

1.1 Monitor

Use the Monitor page to identify the system by displaying information.

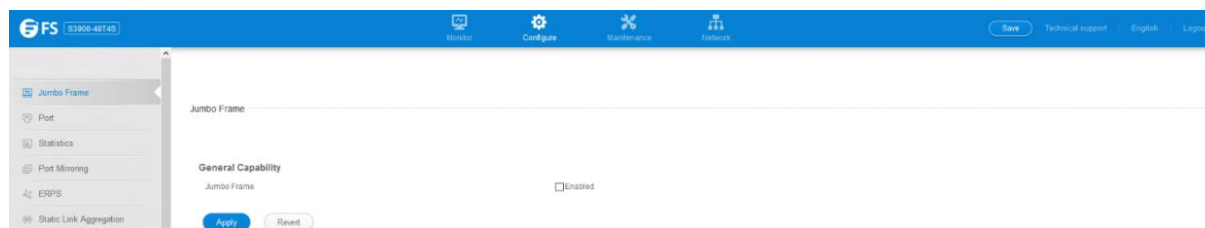


2. Configure

2.1 Jumbo Frame

Use the Configure > Jumbo Frame page to configure support for layer 2 jumbo frames. The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 10240 bytes for Gigabit Ethernet. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

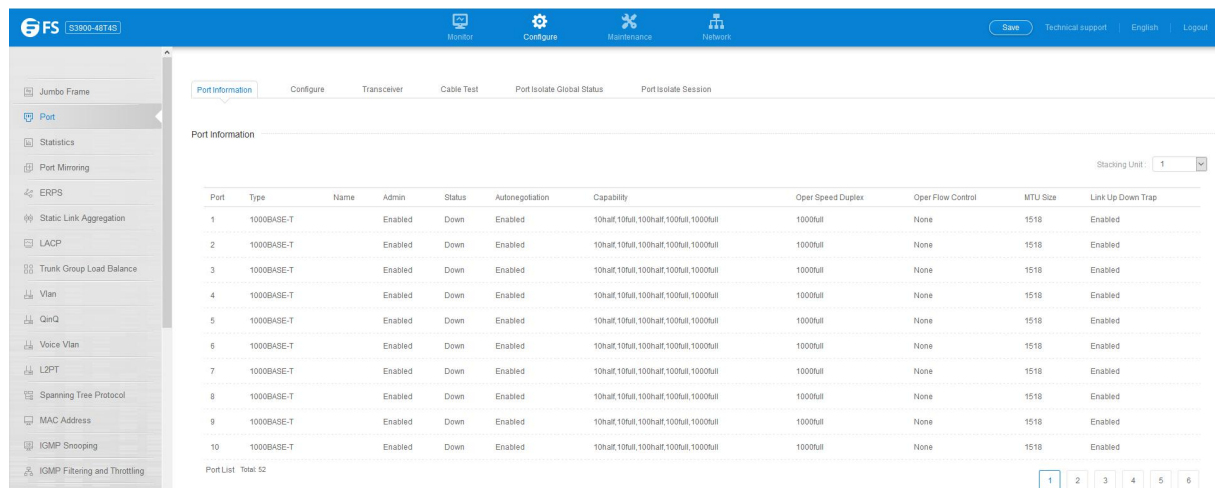
- Jumbo Frame – Configures support for jumbo frames. (Default: Disabled)



3. Port

3.1 Port Information

Use the Switch Configure > Port > Port Information page to display the information of ports.

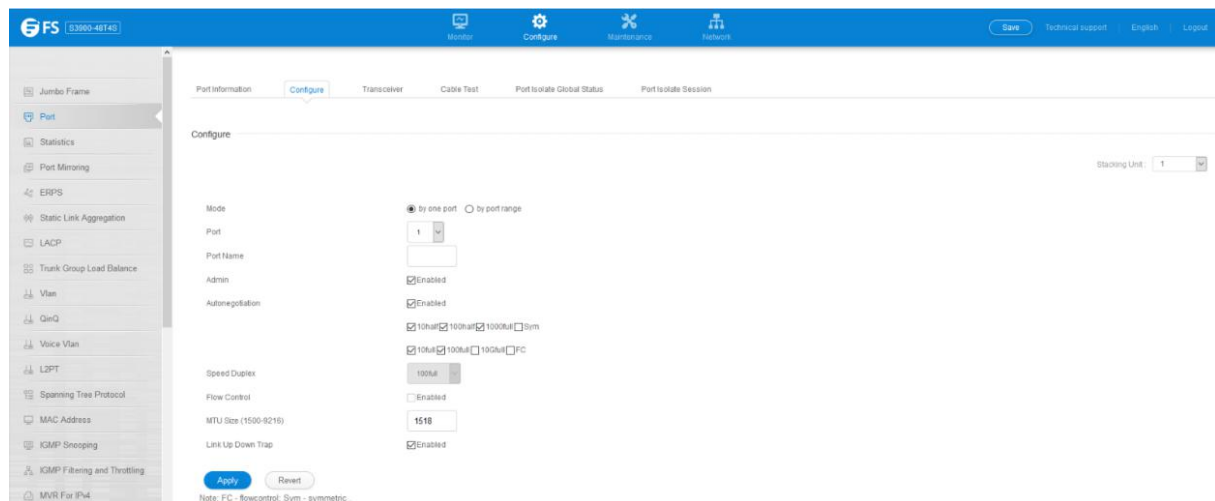


Port	Type	Name	Admin	Status	Autonegotiation	Capability	Oper Speed Duplex	Oper Flow Control	MTU Size	Link Up Down Trap
1	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
2	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
3	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
4	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
5	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
6	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
7	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
8	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
9	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
10	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled

3.1.1 Configure

Configure > Port > Configure page is used to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

For more information on command usage and a description of the parameters.



Mode: ☒ by one port ☐ by port range

Port:

Port Name:

Admin: ☒ Enabled

Autonegotiation: ☒ Enabled

Speed Duplex: ☒ 10half ☒ 100half ☒ 1000full ☐ Sym

Flow Control: ☐ Enabled

MTU Size (1500-9216):

Link Up Down Trap: ☒ Enabled

Apply Reset

Note: FC - flowcontrol, Sym - symmetric

3.1.2 Transceiver

Message when the high threshold is crossed.

- High Warning – Sends a warning message when the high threshold is crossed.
- Low Warning – Sends a warning message when the low threshold is crossed.
- Low Alarm – Sends an alarm Configure>Port>Transceiver page is used to configure thresholds for alarm and warning messages for optical transceivers which support Digital Diagnostic Monitoring (DDM). This page also displays identifying information for supported transceiver types, and operational parameters for transceivers which support DDM.
- Port – Port number. (ECS4620-28F/28F-DC: 1-28, Other models: SFP/SFP+ ports 25-28 / 49-52)
- General – Information on connector type and vendor-related parameters.
- DDM Information – Information on temperature, supply voltage, laser bias current, laser power, and received optical power. The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) provides information on transceiver parameters.

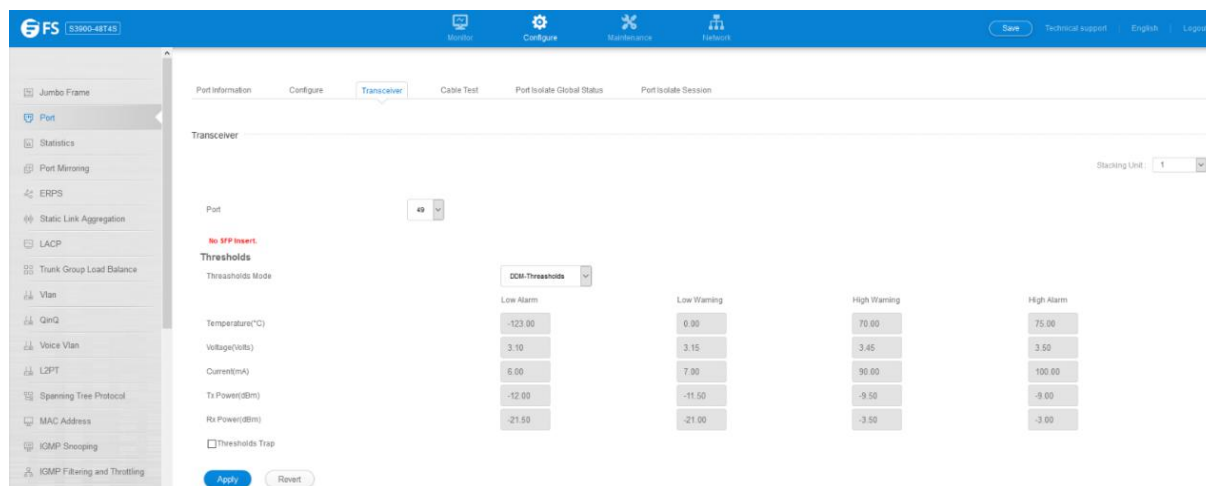
- **Thresholds Trap** – Sends a trap when any of the transceiver's operation values falls outside of specified thresholds. (Default: Disabled)
- **Thresholds Mode** –DDM Thresholds and Manual-Thresholds. DDM Thresholds means using default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent. (Default: Enabled).
- **Thresholds** – Information on alarm and warning thresholds. The switch can be configured to send a trap when the measured parameter falls outside of the specified thresholds.

The following alarm and warning parameters are supported:

- **High Alarm** – Sends an alarm message when the low threshold is crossed.
- The configurable ranges are:
 - Temperature: -128.00-128.00 °C
 - Voltage: 0.00-6.55 Volts
 - Current: 0.00-131.00 mA
 - Power: -40.00-8.20 dBm

The threshold value for Rx and Tx power is calculated as the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW). Threshold values for alarm and warning messages can be configured as described below.

- A high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.
- A low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.
- Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above and below either the high threshold or the low threshold.
- Trap messages configured by this command are sent to any management station configured as an SNMP trap manager using the Administration > SNMP (Configure Trap) page.



Parameter	Low Alarm	Low Warning	High Warning	High Alarm
Temperature(°C)	-123.00	0.00	70.00	75.00
Voltage(Volts)	3.50	3.15	3.45	3.50
Current(mA)	6.00	7.00	90.00	100.00
Tx Power(dBm)	-12.00	-11.50	-9.50	-9.00
Rx Power(dBm)	-21.00	-21.00	-3.50	-3.00

3.1.3 Cable Test

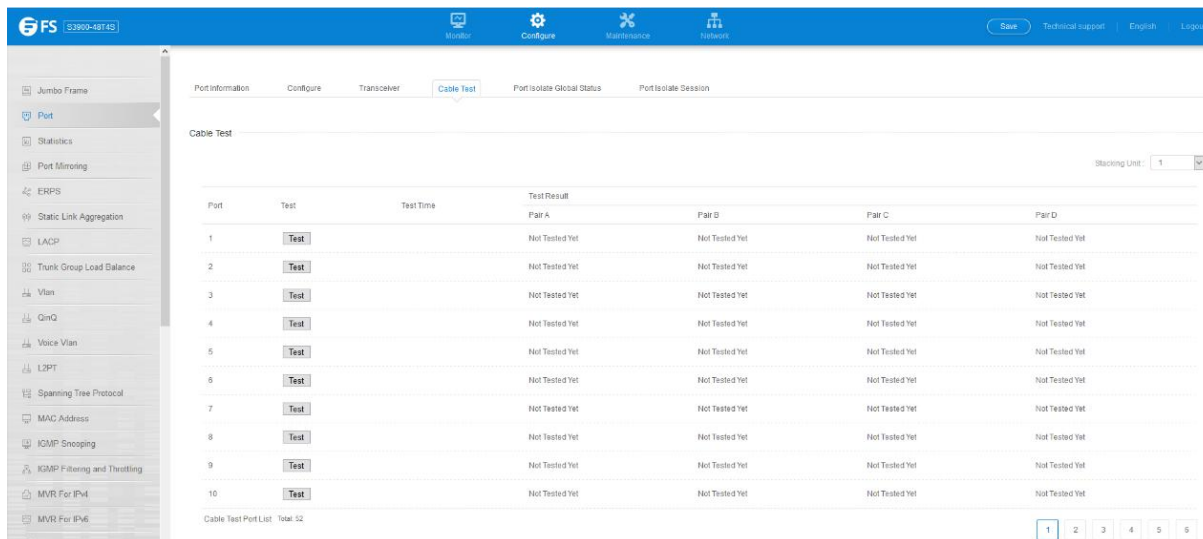
Configure >Port>Cable Test page is used to test the cable attached to a port. The cable test will check for any cable faults (short, open, etc.). If a fault is found, the switch reports the length to the fault. Otherwise, it reports the cable length. It can be used to determine the quality of the cable, connectors, and terminations. Problems such as opens, shorts, and cable impedance mismatch can be diagnosed with this test.

- **Port** – Switch port identifier.
- **Test Result** – The results include common cable failures, as well as the status and approximate distance to a fault, or the

approximate cable length if no fault is found.

To ensure more accurate measurement of the length to a fault, first disable power-saving mode on the link partner before running cable diagnostics. For link-down ports, the reported distance to a fault is accurate to within +/- 2 meters. For link-up ports, the accuracy is +/- 10 meters.

- **Test Time** – Shows the last time this port was tested.



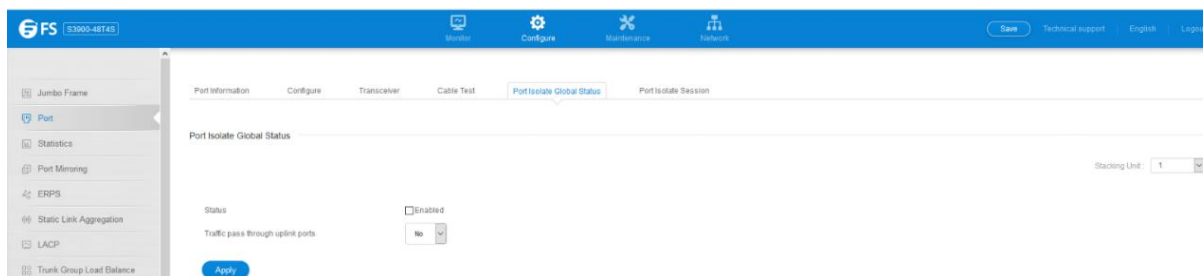
Port	Test	Test Time	Test Result	Pair A	Pair B	Pair C	Pair D
1	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
2	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
3	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
4	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
5	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
6	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
7	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
8	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
9	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
10	Test		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet

Cable Test Port List: Total: 0/2

3.1.4 Port Isolate

Configure >Port> Port Isolate page is used to enable traffic segmentation.

- **Status** – Enables port-based traffic segmentation. (Default: Disabled)
- **Traffic pass through uplink ports**– Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions.
 - **No**– Blocks traffic between uplink ports assigned to different sessions.
 - **Yes**– Forwards traffic between uplink ports assigned to different sessions.



Port Isolate Global Status

Status ☐ Enabled

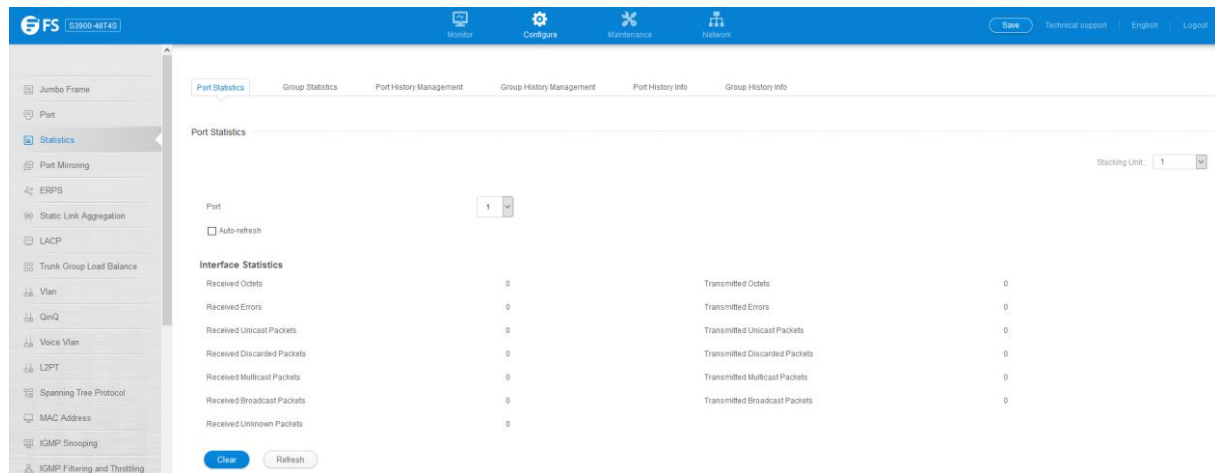
Traffic pass through uplink ports: No

Apply

3.2 Statistics

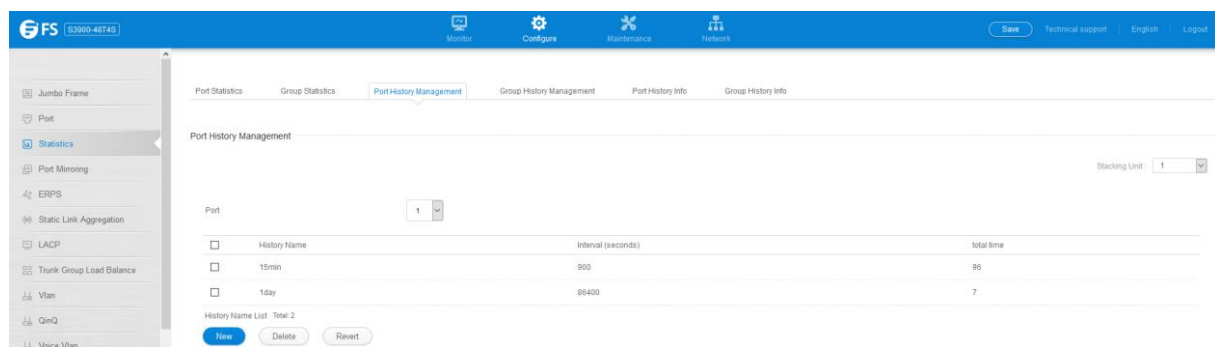
3.2.1 Port Statistics

Configure >Statistics> Port Statistics page is used to display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy traffic). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

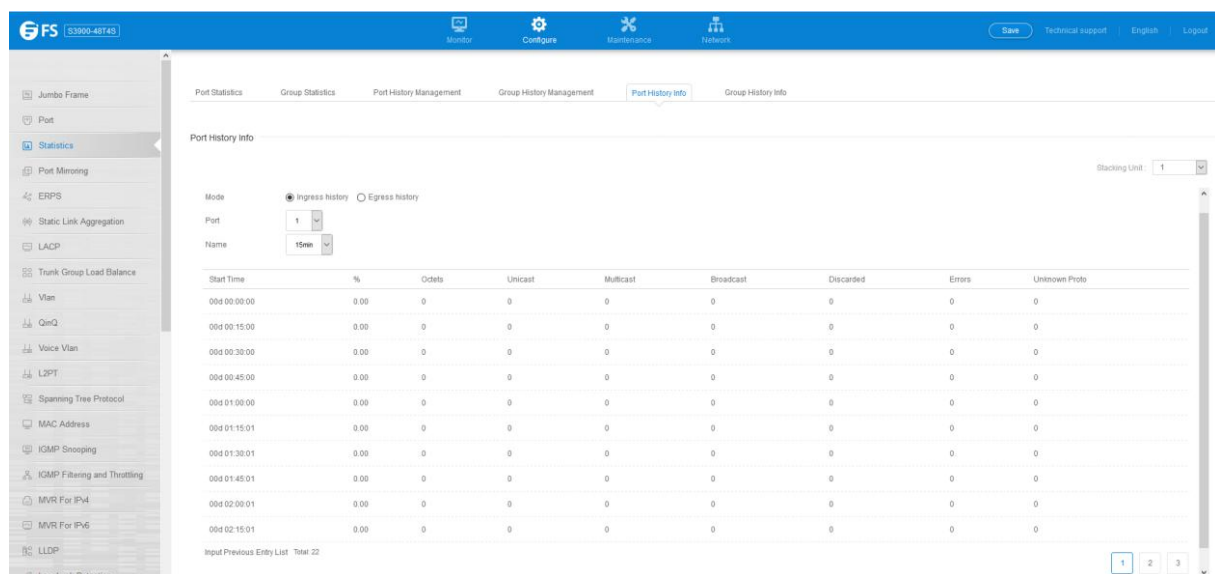


3.2.2 Port History Management

Configure > Statistics > Port History Management page is used to display statistical history for the specified interfaces.



3.2.3 Port History Info



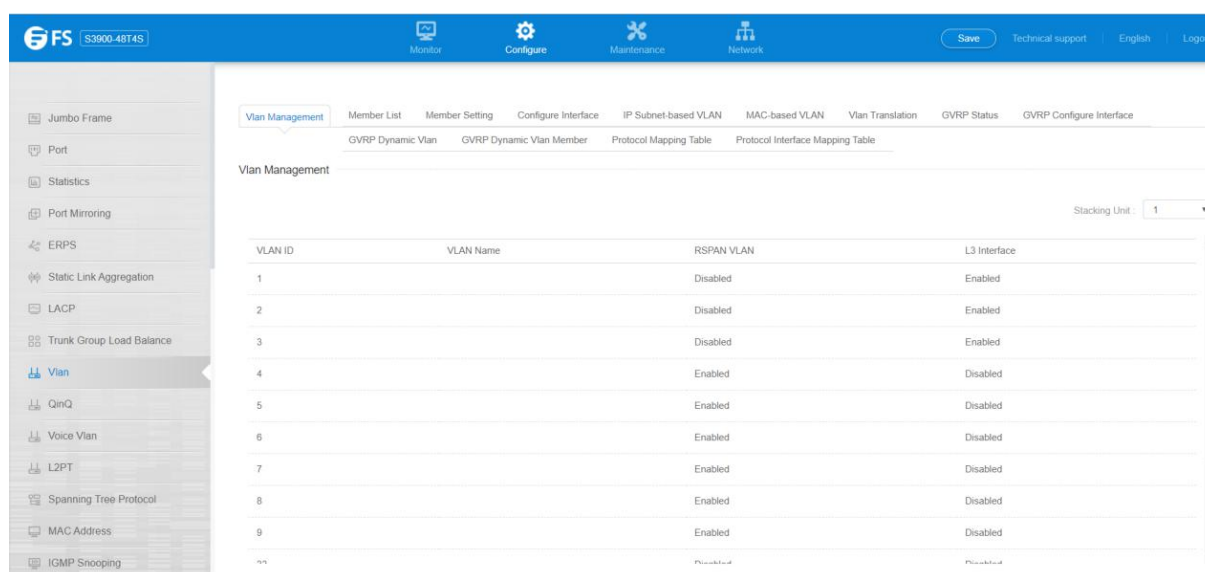
4. Vlan

4.1 Vlan Management

Configure >Vlan > Vlan Management page is used to add,modify or delete static VLAN groups, set administrative status, or specify Remote VLAN type.

To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

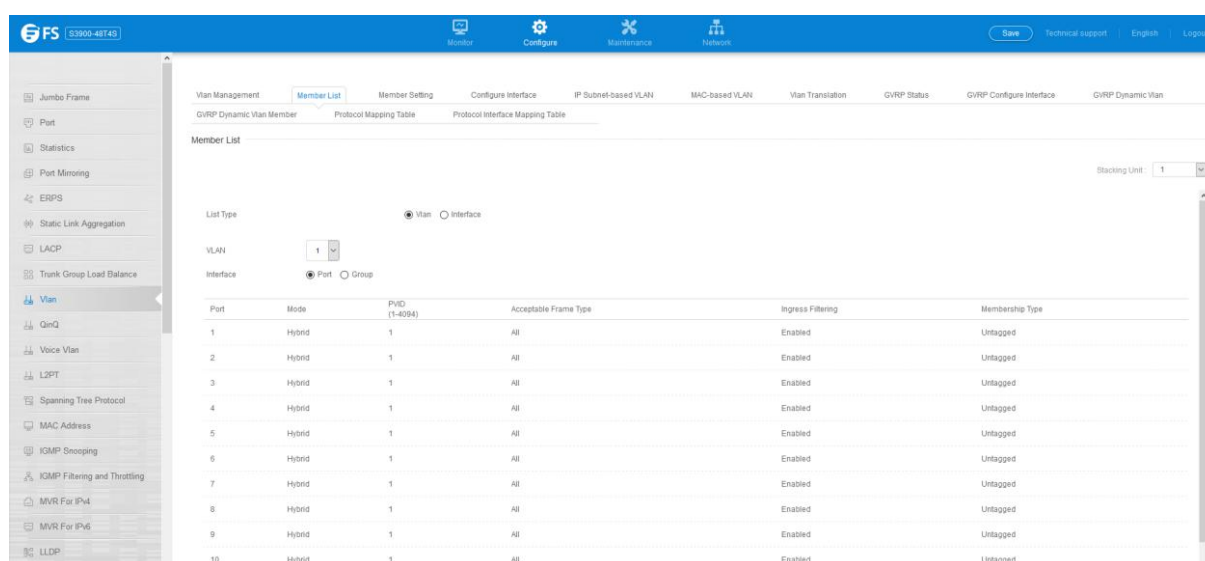
- VLAN ID – ID of VLAN or range of VLANs (1-4093).Up to 4093 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- VLAN Name – Name of the VLAN (1 to 32 characters).
- Status – Enables or disables the specified VLAN.
- Remote VLAN – Reserves this VLAN for RSPAN.
- L3 Interface – Sets the interface to support Layer 3 configuration, and reserves memory space required to maintain additional information about this interface type. This parameter must be enabled before you can assign an IP address to a VLAN



VLAN ID	VLAN Name	RSPAN VLAN	L3 Interface
1		Disabled	Enabled
2		Disabled	Enabled
3		Disabled	Enabled
4		Enabled	Disabled
5		Enabled	Disabled
6		Enabled	Disabled
7		Enabled	Disabled
8		Enabled	Disabled
9		Enabled	Disabled

4.1.1 Member List

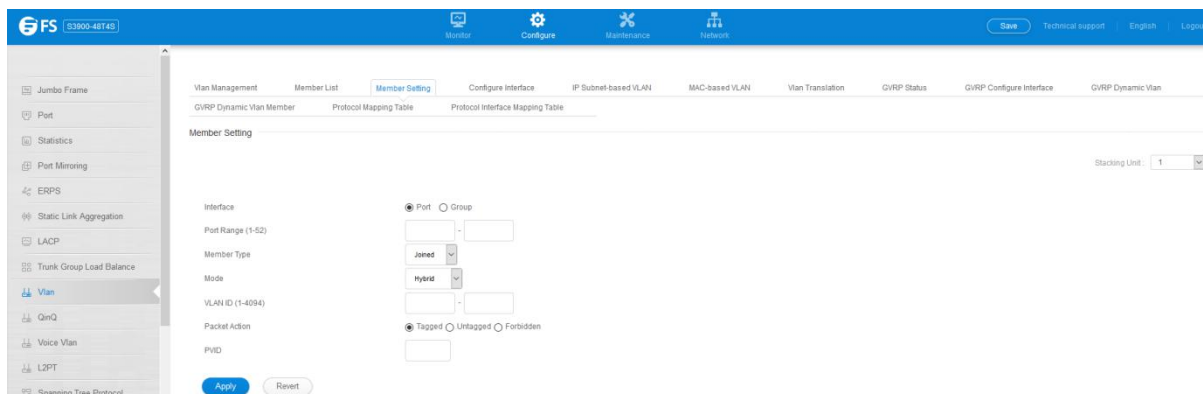
Configure >Vlan >Member List page is used to display vlan members.



Port	Mode	PVID (1-4094)	Acceptable Frame Type	Ingress Filtering	Membership Type
1	Hybrid	1	All	Enabled	Untagged
2	Hybrid	1	All	Enabled	Untagged
3	Hybrid	1	All	Enabled	Untagged
4	Hybrid	1	All	Enabled	Untagged
5	Hybrid	1	All	Enabled	Untagged
6	Hybrid	1	All	Enabled	Untagged
7	Hybrid	1	All	Enabled	Untagged
8	Hybrid	1	All	Enabled	Untagged
9	Hybrid	1	All	Enabled	Untagged
10	Hybrid	1	All	Enabled	Untagged

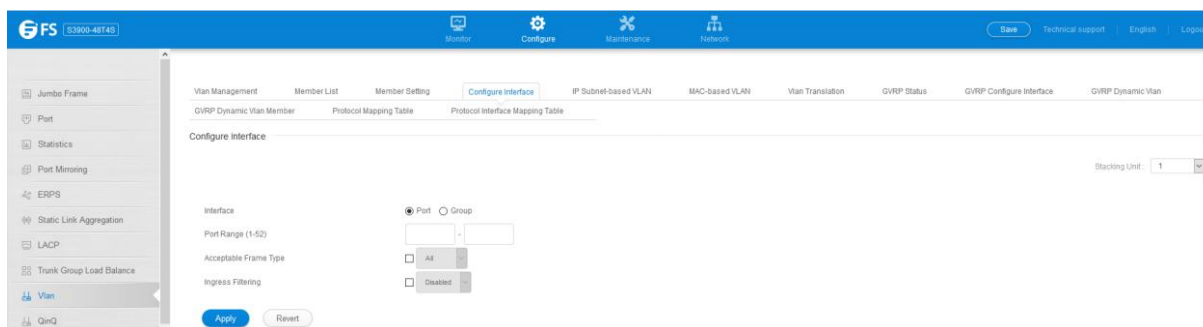
4.1.2 Member Setting

Configure >Vlan >Member Setting page is used to add/delete a interface member to/from multiple vlan



4.1.3 Configure Interface

Configure >Vlan >Configure Interface page is used to configure Acceptable Frame Type and Ingress Filtering.



4.1.4 GVRP Status

Configure >Vlan >GVRP Status page is used to enable GVRP globally on the switch, or to enable GVRP and adjust the protocol timers per interface.

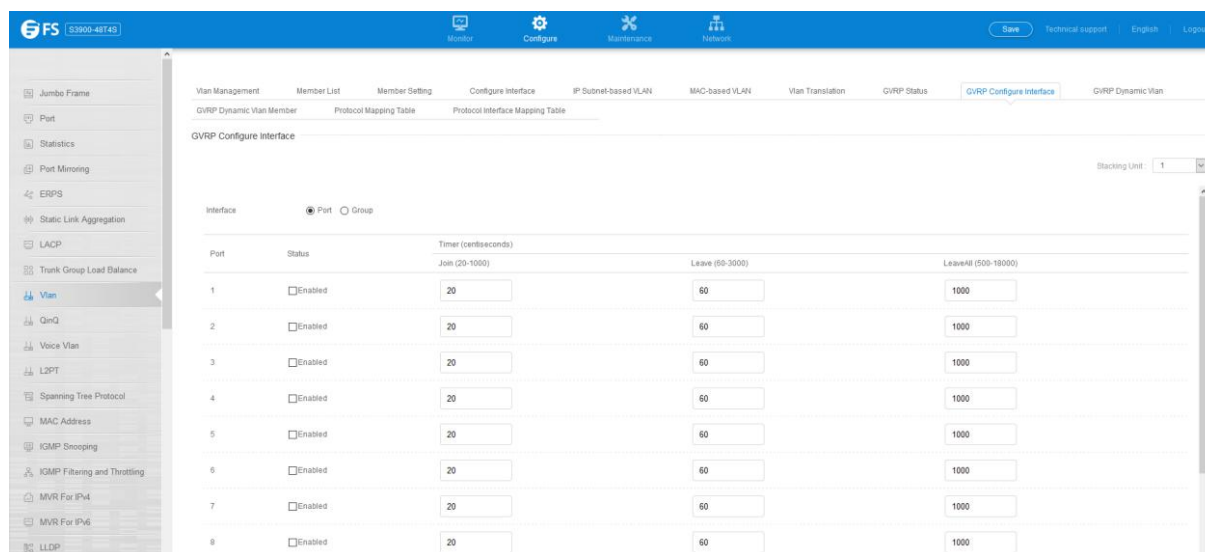
- **GVRP Status** – GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

4.1.5 GVRP Configure Interface

Configure >Vlan > GVRP Configure Interface

- Interface – Displays a list of ports or group.
- Port – Port Identifier. (Range: 1-28)
- Group– Group Identifier. (Range: 1-12)
- GVRP Status – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect (using the Configure General page). When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled) GVRP cannot be enabled for ports set to Access mode
- GVRP Timers – Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer
 - Join – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
 - Leave – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
 - LeaveAll – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

Show Dynamic VLAN – Show VLAN

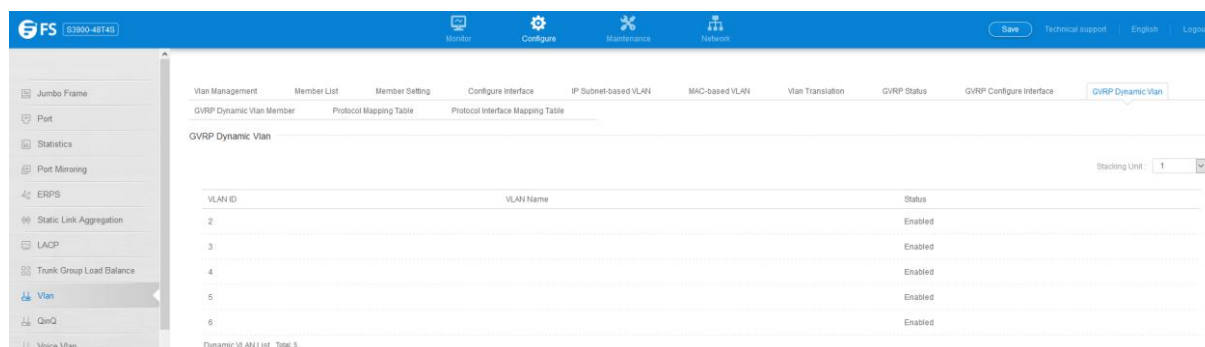


Port	Status	Timer (centiseconds)		
		Join (20-1000)	Leave (60-3000)	LeaveAll (500-18000)
1	<input checked="" type="checkbox"/> Enabled	20	60	1000
2	<input checked="" type="checkbox"/> Enabled	20	60	1000
3	<input checked="" type="checkbox"/> Enabled	20	60	1000
4	<input checked="" type="checkbox"/> Enabled	20	60	1000
5	<input checked="" type="checkbox"/> Enabled	20	60	1000
6	<input checked="" type="checkbox"/> Enabled	20	60	1000
7	<input checked="" type="checkbox"/> Enabled	20	60	1000
8	<input checked="" type="checkbox"/> Enabled	20	60	1000
9	<input checked="" type="checkbox"/> Enabled	20	60	1000

4.1.6 GVRP Dynamic VLAN

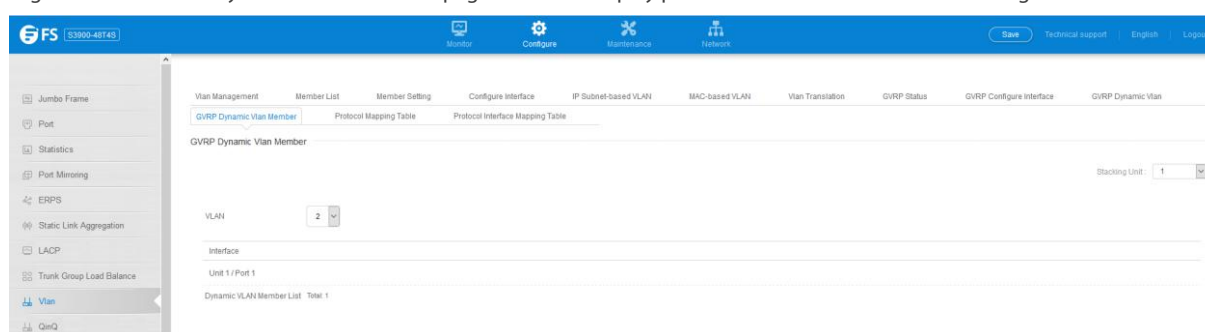
Configure >Vlan > GVRP Dynamic VLAN page is used to display dynamic VLAN learnt from GVRP.

- VLAN ID – Identifier of a VLAN this switch has joined through GVRP.
- VLAN Name – Name of a VLAN this switch has joined through GVRP.
- Status – Indicates if this VLAN is currently operational.



4.1.7 GVRP Dynamic VLAN Member

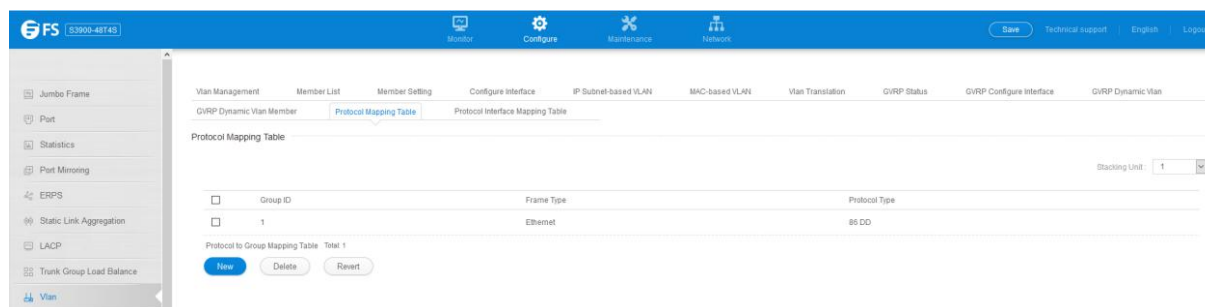
Configure > Vlan > GVRP Dynamic VLAN Member page is used to display port members of selected VLAN through GVRP.



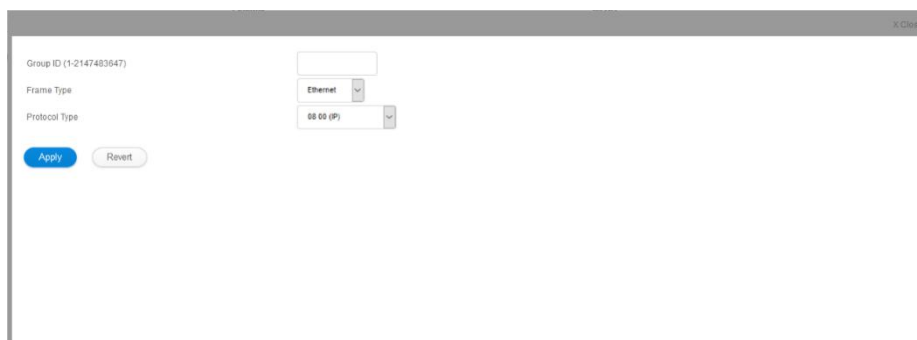
4.1.8 Protocol Mapping Table

- To configure protocol-based VLANs, follow these steps:
 - First configure VLAN groups for the protocols you want to use. Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network.
Do not add port members at this time.
 - Create a protocol group for each of the protocols you want to assign to a VLAN using the Configure Protocol (Add) page.
 - Then map the protocol for each interface to the appropriate VLAN using the Configure Interface (Add) page.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

Configure > VLAN > Protocol Mapping Table page is used to create and delete a protocol vlan entry.



Press New button to create a protocol vlan entry:



Group ID (1-2147483647)

Frame Type: Ethernet

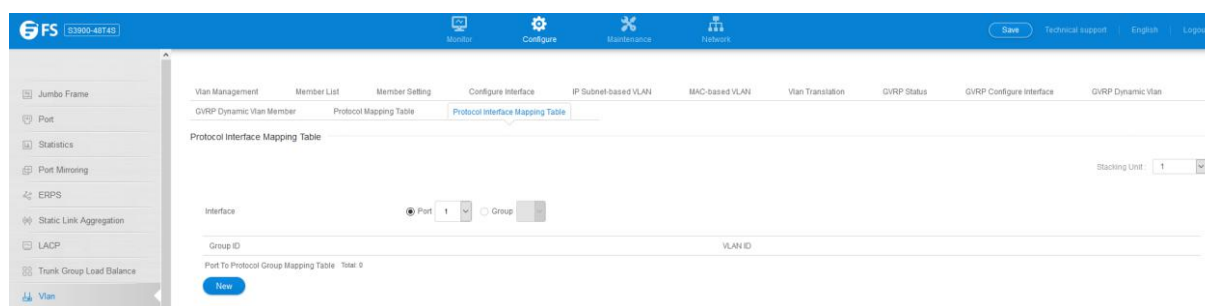
Protocol Type: 08 00 (IP)

Buttons: Apply, Revert

- Frame Type – Choose either Ethernet, RFC 1042, or LLC Other as the frame type used by this protocol.
- Protocol Type – Specifies the protocol type to match. The available options are IP, ARP, RARP and IPv6. If LLC Other is chosen for the Frame Type, the only available Protocol Type is IPX Raw.
- Group ID – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)

4.1.9 Protocol Interface Mapping

Configure > VLAN > Protocol Interface Mapping Table page is used to add/delete a interface member to protocol vlan group.



FS S3900-48T48

Monitor Configure Maintenance Network

Save Technical support English Logout

Vlan Management Member List Member Setting Configure Interface IP Subnet-based VLAN MAC-based VLAN Vlan Translation GVRP Status GVRP Configure Interface GVRP Dynamic Vlan

GVRP Dynamic Vlan Member Protocol Mapping Table Protocol Interface Mapping Table

Protocol Interface Mapping Table

Stacking Unit: 1

Interface: Port 1 Group

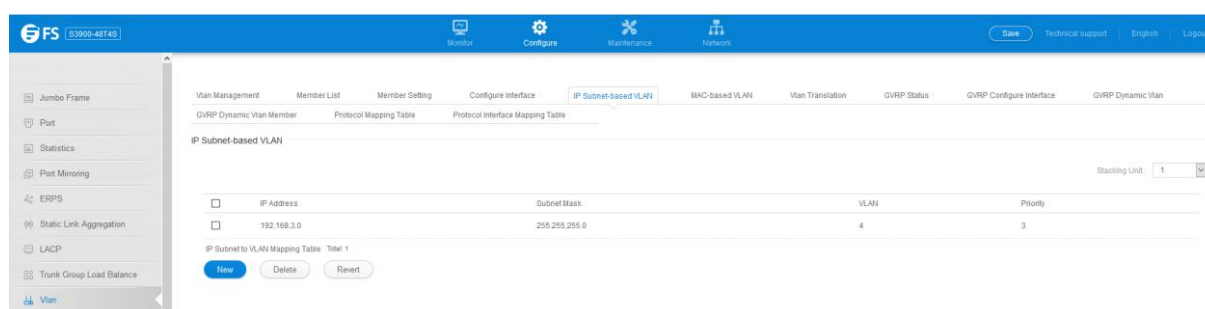
Group ID: VLAN ID:

Port To Protocol Group Mapping Table: Total: 0

New

4.1.10 IP Subnet-based Vlan

Configure > VLAN > IP Subnet-based VLAN page is used to configure IP subnet-based VLANs.



FS S3900-48T48

Monitor Configure Maintenance Network

Save Technical support English Logout

Vlan Management Member List Member Setting Configure Interface IP Subnet-based VLAN MAC-based VLAN Vlan Translation GVRP Status GVRP Configure Interface GVRP Dynamic Vlan

GVRP Dynamic Vlan Member Protocol Mapping Table Protocol Interface Mapping Table

IP Subnet-based VLAN

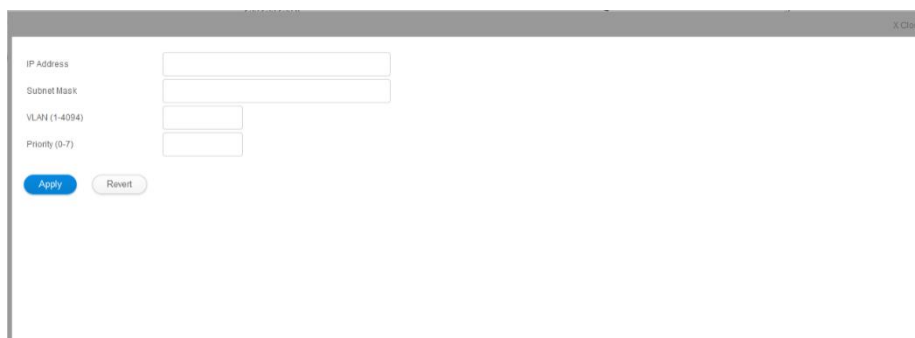
Stacking Unit: 1

IP Address	Subnet Mask	VLAN	Priority
192.168.3.0	255.255.255.0	4	3

IP Subnet to VLAN Mapping Table: Total: 1

New Delete Revert

Press New button to create a IP subnet vlan entry.

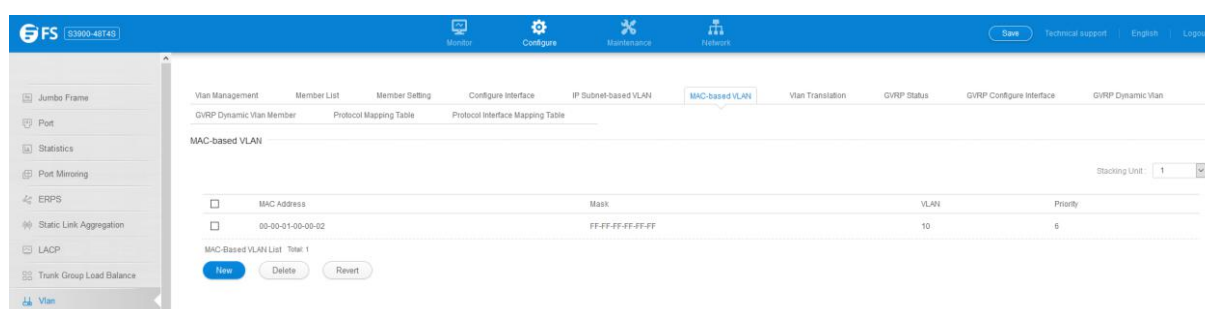


- IP Address – The IP address for a subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- Subnet Mask – This mask identifies the host address bits of the IP subnet.
- VLAN – VLAN to which matching IP subnet traffic is forwarded.(Range: 1-4093)
- Priority – The priority assigned to untagged ingress traffic.(Range: 0-7, where 7 is the highest priority; Default: 0)

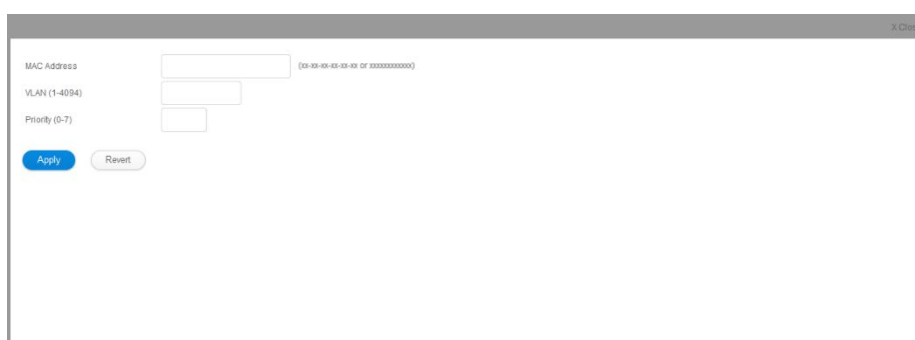
To delete a IP subnet vlan entry, select the entry and press delete button.

4.1.11 MAC-Based Vlan

Configure > VLAN > Mac-Based Vlan page is used to configure VLAN based on MAC addresses.



To create a Mac based vlan, press New button:

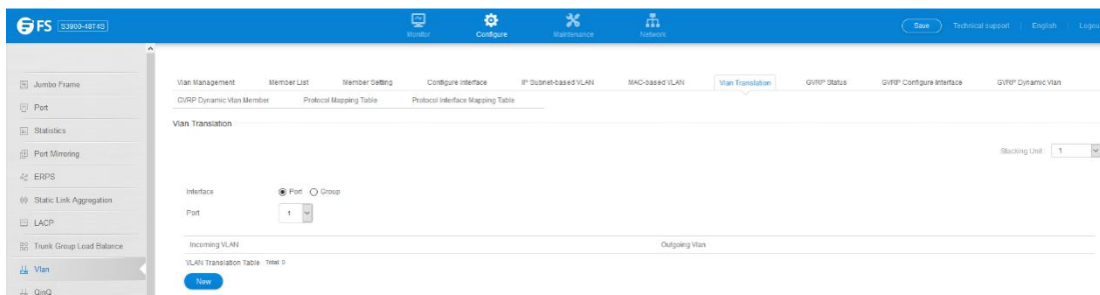


- MAC Address – A source MAC address which is to be mapped to a specific VLAN. The MAC address must be specified in the format xx-xxxx-xx-xx-xx.
- VLAN – VLAN to which ingress traffic matching the specified source MAC address is forwarded. (Range: 1-4093)
- Priority – The priority assigned to untagged ingress traffic.(Range: 0-7, where 7 is the highest priority; Default: 0)

To delete a Mac based vlan entry, select the entry and press delete button.

4.1.12 Vlan Translation

Configure > VLAN > Vlan Translation page is used to map VLAN IDs between the customer and service provider for networks that do not support IEEE802.1Q tunneling.



Press New button to create a vlan translation.



These parameters are displayed:

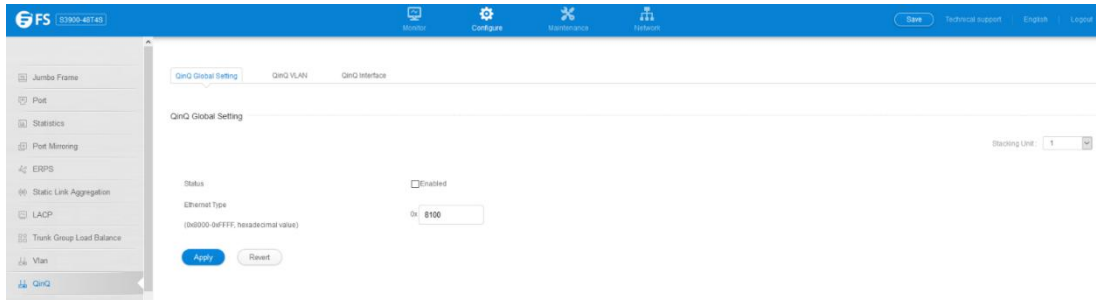
- Incoming VLAN – The original VLAN ID. (Range: 1-4093)
- Outgoing VLAN – The new VLAN ID. (Range: 1-4093)

To delete a entry, select the entry and press delete button.

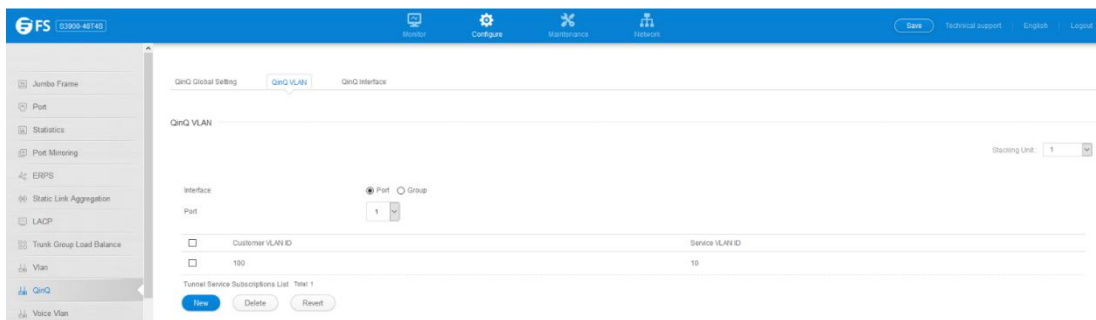
4.2 QinQ

Configure > QinQ > QinQ Global Setting page is used to configure the switch to operate in IEEE 802.1Q (QinQ) tunneling mode, which is used for passing Layer 2 traffic across a service provider's metropolitan area network. You can also globally set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethernet type to identify 802.1Q tagged frames.

- Tunnel Status – Sets the switch to QinQ mode. (Default: Disabled)
- Ethernet Type – The Tag Protocol Identifier (TPID) specifies the ethernet type of incoming packets on a tunnel port. (Range: hexadecimal 0800-FFFF; Default: 8100)



Configure > Qinq > Qinq VLAN page is used to configure the Qinq entry.

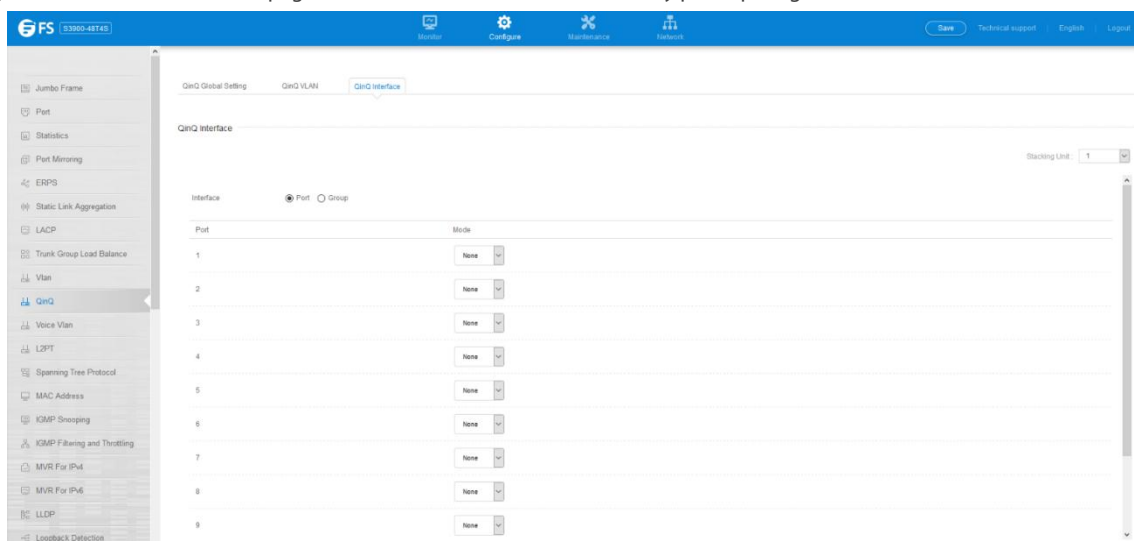


Press New button to create new Qinq entry.



To delete a entry, select the entry and press delete button.

Configure > Qinq > Qinq Interface page is used to set the tunnel mode for any participating interface.

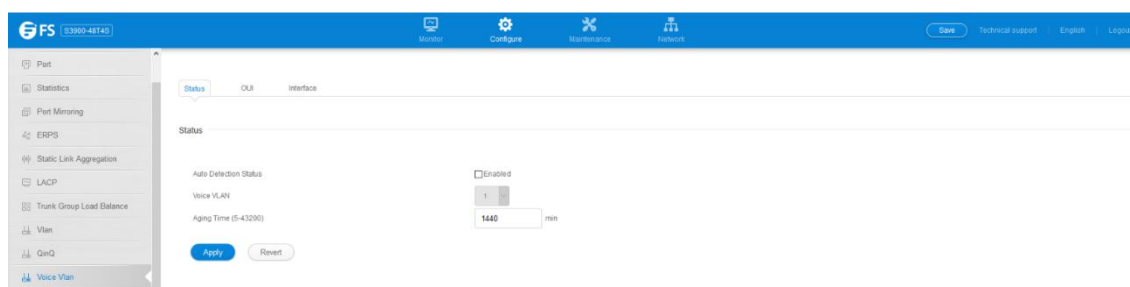


- Interface – Displays a list of ports or groups.
- Port – Port Identifier. (Range: 1-28)
- Group– Group Identifier. (Range: 1-12)
- Mode – Sets the VLAN membership mode of the port.
 - None – The port operates in its normal VLAN mode. (This is the default.)
 - Access – Configures QinQ tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
 - Uplink – Configures QinQ tunneling for an uplink port to another device within the service provider network.
- Use the Configure Global page to set the switch to QinQ mode before configuring a QinQ access port or tunnel uplink port.

4.3 Voice Vlan

Configure >Voice Vlan>Status page is used to configure the voice vlan.

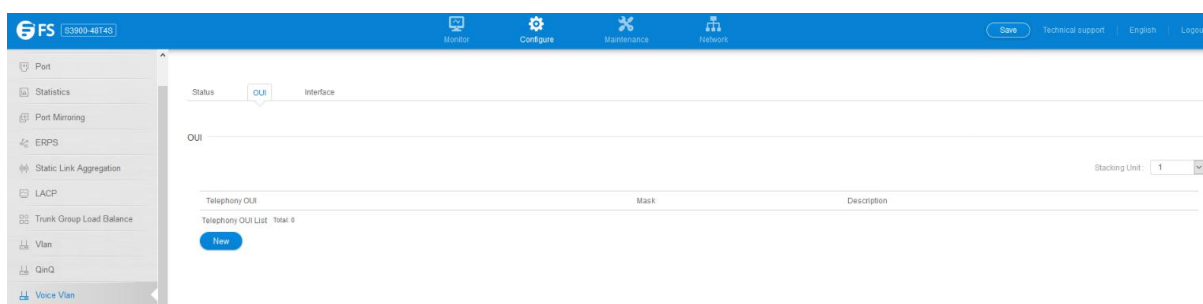
VLAN membership can not be set to access mode.



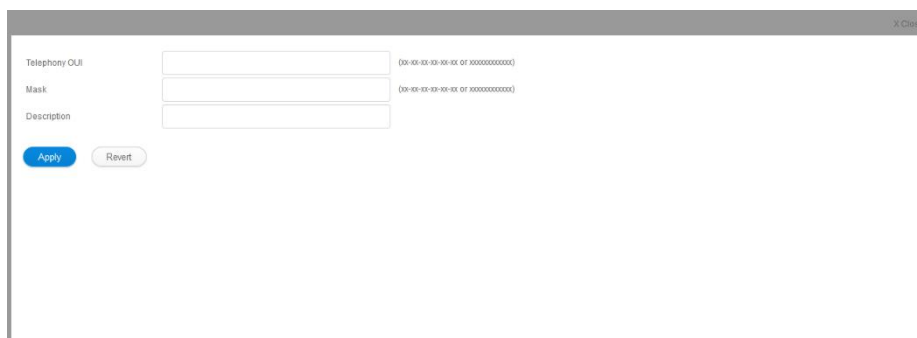
- Auto Detection Status – Enables the automatic detection of VoIP traffic on switch ports. (Default: Disabled)
- Voice VLAN – Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported and it must already be created on the switch. (Range: 1-4094)
- Aging Time – The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port.(Range: 5-43200 minutes; Default: 1440 minutes)

Note: The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

Configure > Voice Vlan > OUI page is used to configure the Organizational Unique Identifier (OUI) in the source MAC address of received packets.



To create a OUI, press New button.



Telephony OUI: (00-00-00-00-00-00 or XXXXXXXXXX)

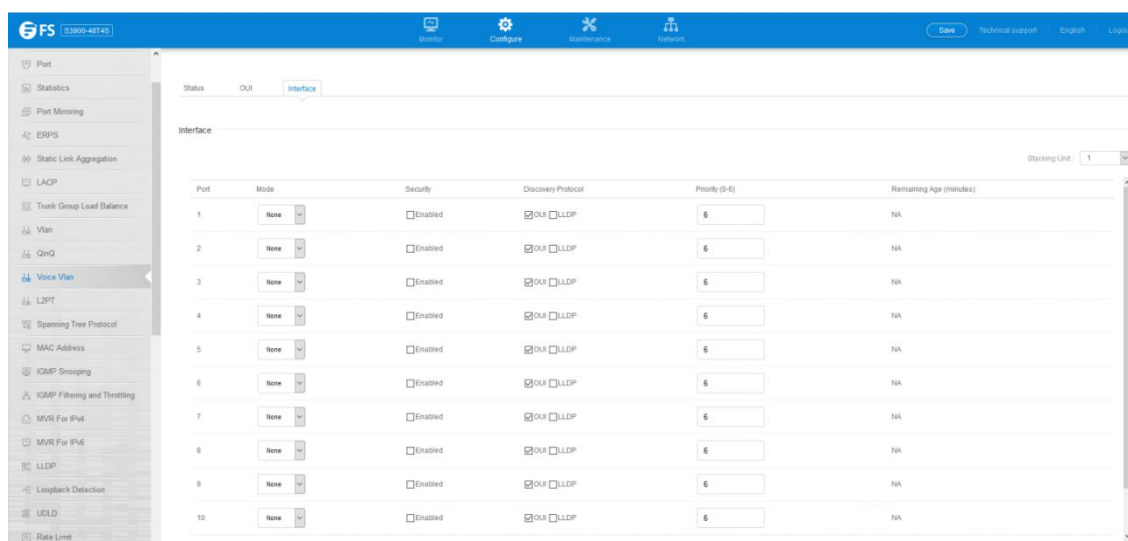
Mask: (00-00-00-00-00-00 or XXXXXXXXXX)

Description:

- **Telephony OUI** – Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.
- **Mask** – Identifies a range of MAC addresses. Setting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Setting a mask of FF-FF-FF-FF-FF-FF specifies a single MAC address. (Default: FF-FF-FF-00-00-00)
- **Description** – User-defined text that identifies the VoIP devices

To delete a OUI, select the OUI and press delete button.

Configure > Voice Vlan > Interface page is used to configure ports for voice vlan, you need to set the mode (Auto or Manual), specify the discovery method to use, and set the traffic priority. You can also enable security filtering to ensure that only voice vlan traffic is forwarded on the Voice VLAN.



Interface configuration table:

Port	Mode	Security	Discovery Protocol	Priority (0-6)	Remaining Age (minutes)
1	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A
2	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A
3	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A
4	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A
5	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A
6	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A
7	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A
8	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A
9	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A
10	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	N/A

All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), first ensure that VLAN membership is not set to access mode.

- **Mode** – Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. (Default: None)
 - **None** – The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be added to the Voice VLAN.
 - **Auto** – The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port. You must select a method for detecting VoIP traffic, either OUI or 802.1AB (LLDP). When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list.
 - **Manual** – The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.
- **Security** – Enables security filtering that discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP

devices attached to the switch. Packets received from non-VoIP sources are dropped. (Default: Disabled)

- **Discovery Protocol** – Selects a method to use for detecting VoIP traffic on the port. (Default: OUI)
 - **OUI** – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to vendors and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
 - **LLDP** – Uses LLDP (IEEE 802.1AB) to discover voice vlan devices attached to the port. LLDP checks that the “telephone bit” in the system capability TLV is turned on.
- **Priority** – Defines a CoS priority for port traffic on the Voice VLAN. The priority of any received voice vlan packet is overwritten with the new priority when the Voice VLAN feature is active for the port. (Range: 0-6; Default: 6)
- **Remaining Age** – Number of minutes before this entry is aged out.

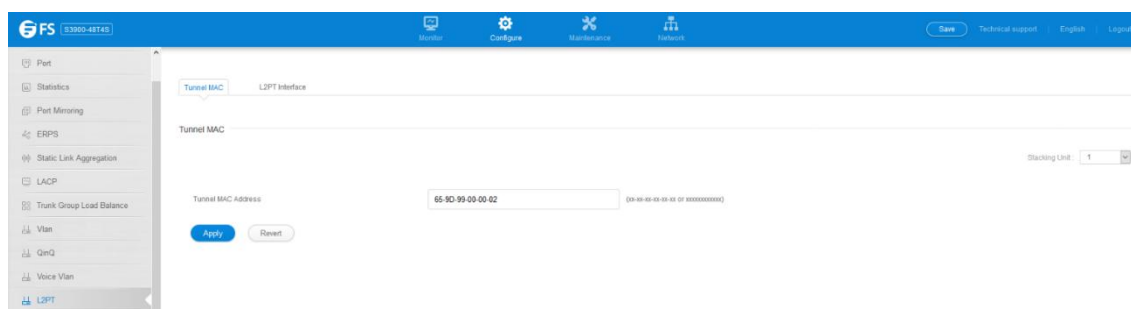
The Remaining Age starts to count down when the OUI's MAC address expires from the MAC address table. Therefore, the MAC address aging time should be added to the overall aging time. For example, if you configure the MAC address table aging time to 30 seconds, and the voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from voice VLAN when voice vlan traffic is no longer received on the port. Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the Remaining Age.

4.4 L2PT

Configure > L2PT is used to configure the l2 protocol tunnel.

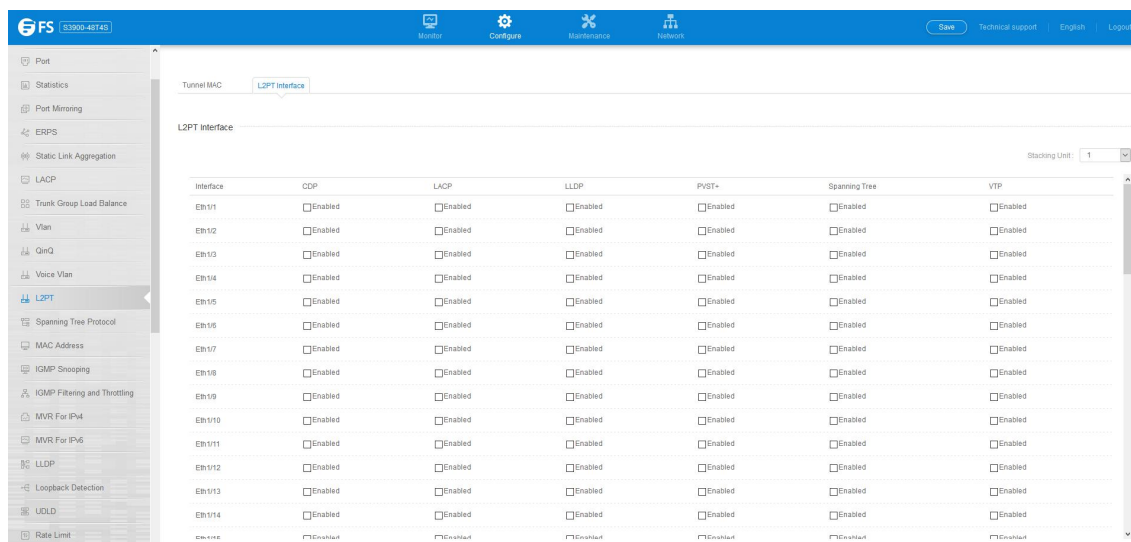
Tunnel MAC page:

Used to configure the destination of the tunnel.



L2PT Interface page:

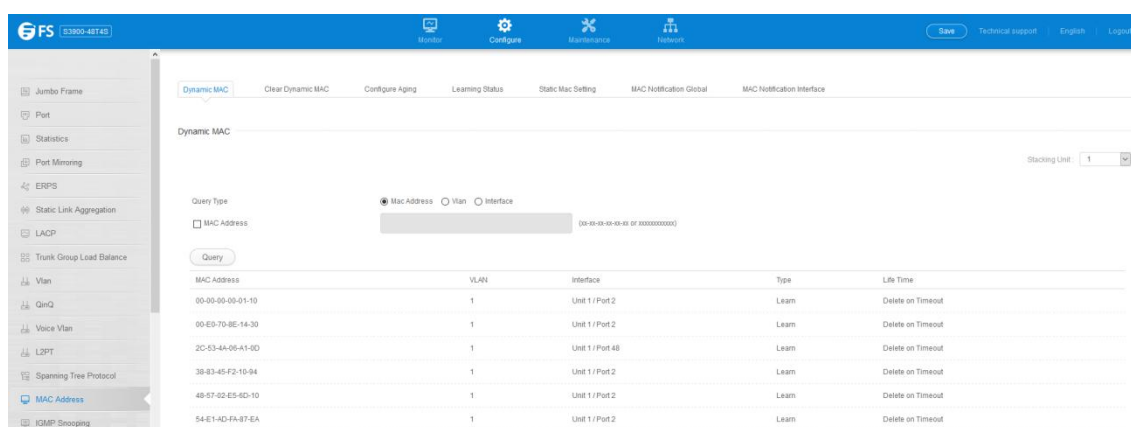
Used to configure which protocol will pass through in the tunnel.



4.5 MAC Address

4.5.1 Dynamic MAC

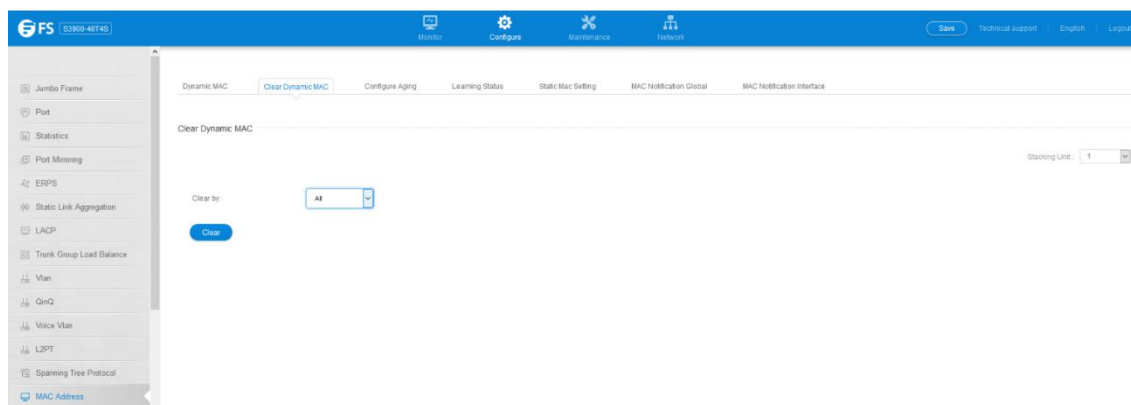
Configure > MAC Address > Dynamic Mac page is used to display the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.



4.5.2 Clear Dynamic MAC

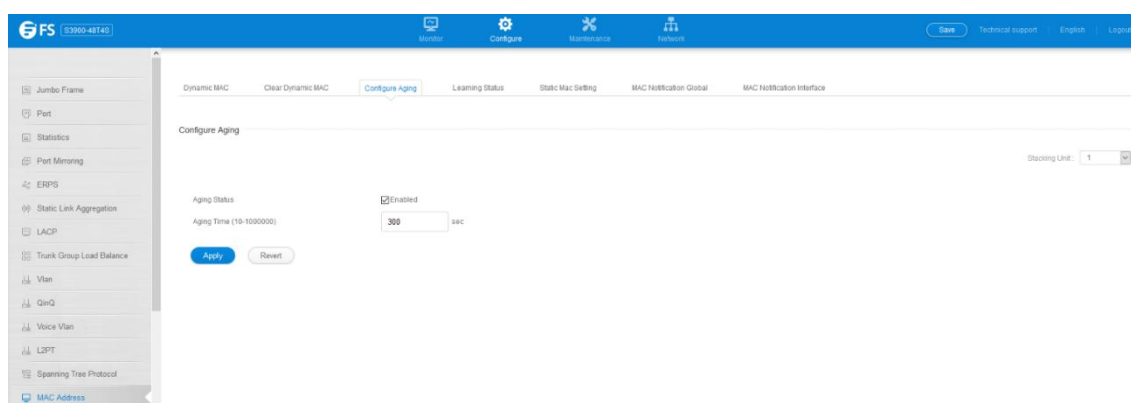
Configure > MAC Address > Clear Dynamic MAC page is used to remove any learned entries from the forwarding database.

- **Clear by** – All entries can be cleared; or you can clear the entries for a specific MAC address, all the entries in a VLAN, or all the entries associated with a port or group.



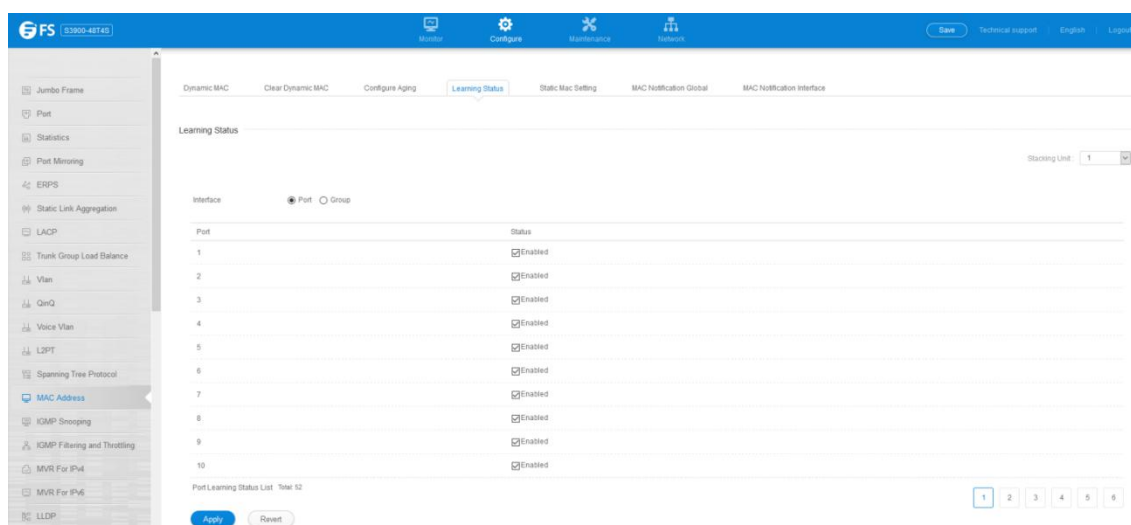
4.5.3 Configure Aging

Configure > MAC Address > Configure Aging page is used to set the aging time for entries in the dynamic address table. The aging time is used to age out dynamically learned forwarding information.



4.5.4 Learning Status

Configure > MAC Address > Learning status page is used to set learning status on port.



4.5.5 Static Mac Setting

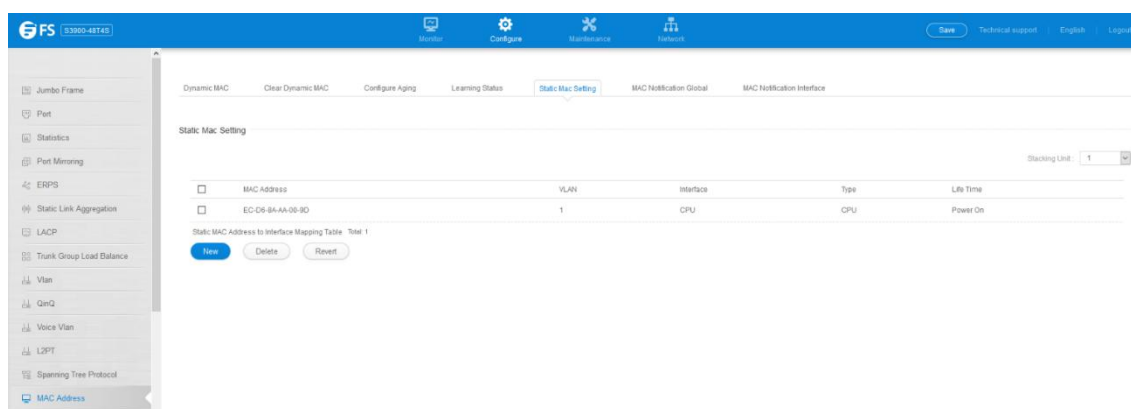
Configure > MAC Address > Static Mac Setting page is used to configure static MAC addresses. A static address can be assigned to a

specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

- **VLAN** – ID of configured VLAN. (Range: 1-4093)
- **Interface** – Port or group associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface. Enter an address in the form of xx-xx-xx-xx-xx-xx or XXXX.XXXX.XXXX.
- **Static Status** – Sets the time to retain the specified address.
 - Delete-on-reset - Assignment lasts until the switch is reset.
 - Permanent - Assignment is permanent. (This is the default.)

To configure a static MAC address:

1. Click Configure, MAC Address, Static Mac Setting, New button.
2. Specify the VLAN, the port or group to which the address will be assigned, the MAC address, and the time to retain this entry.
3. Click Apply.



- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- Static addresses will not be removed from the address table when a given interface link is down.
- A static address cannot be learned on another port until the address is removed from the table.

4.5.6 MAC Notification

Configure > MAC Address > MAC Notification is used to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed.

Configure Global

- **Trap Status** – Issues a trap when a dynamic MAC address is added or removed. (Default: Disabled)
- **Trap Interval** – Specifies the interval between issuing two consecutive traps. (Range: 1-3600 seconds; Default: 1 second)

Configure Interface

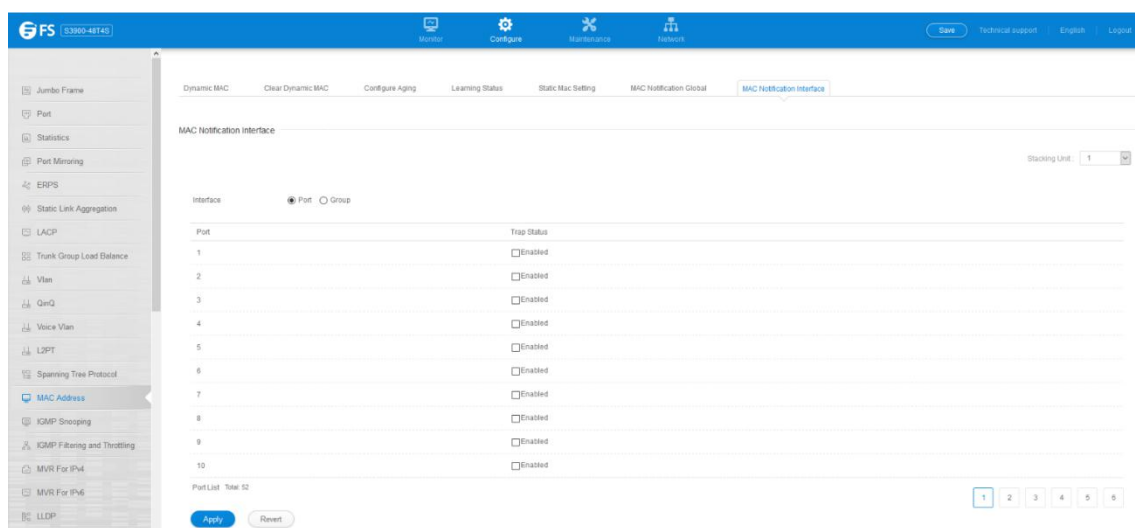
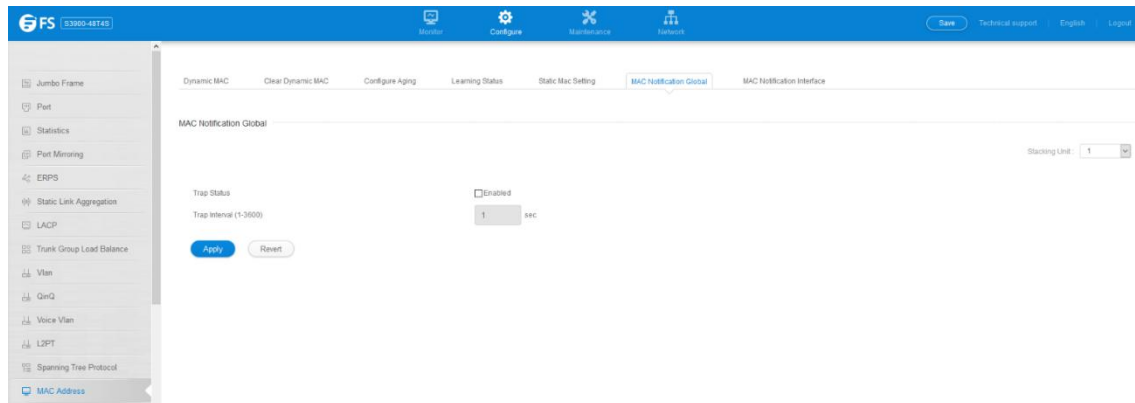
- **Port** – Port Identifier. (Range: 1-28/52)
- **Trap Status** – Enables MAC authentication traps on the current interface. (Default: Disabled)

MAC authentication traps must be enabled at the global level for this attribute to take effect.

Web Interface

To enable MAC address traps at the global level:

1. Click Configure, MAC Address, MAC Notification.
2. Select Global from the Step list.
3. Configure MAC notification traps and the transmission interval.
4. Click Apply.

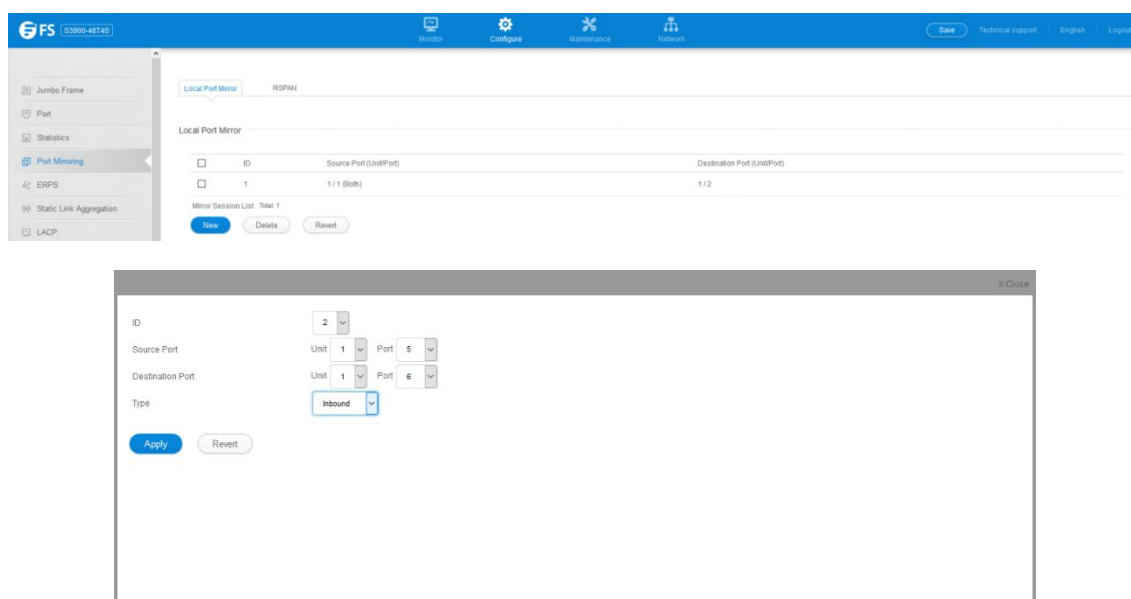


4.6 Port Mirroring

4.6.1 Local Port Mirror

Configure > Port Mirroring > Local Port Mirror page is used to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

- **Source Port** – The port whose traffic will be monitored.
- **Target Port** – The port that will mirror the traffic on the source port.
- **Type** – Allows you to select which traffic to mirror to the target port, Rx(receive), Tx (transmit), or Both. (Default: Rx)



4.6.2 RSPAN

Configure > Port Mirroring > RSPAN page is used to mirror traffic from remote switches for analysis at a destination port on the local switch.

Take the following step to configure an RSPAN session:

1. Use the VLAN Static List to reserve a VLAN for use by RSPAN (marking the "Remote VLAN" field on this page. (Default VLAN 1 is prohibited.)
2. Set up the source switch on the RSPAN configuration page by specifying the mirror session, the switch's role (Source), the RSPANVLAN, and the uplink port1. Then specify the source port(s), and the traffic type to monitor (Rx, Tx or Both).
3. Set up all intermediate switches on the RSPAN configuration page, entering the mirror session, the switch's role (Intermediate), the RSPAN VLAN, and the uplink port(s).
4. Set up the destination switch on the RSPAN configuration page by specifying the mirror session, the switch's role (Destination), the destination port, whether or not the traffic exiting this port will be tagged or untagged, and the RSPAN VLAN. Then specify each uplink port where the mirrored traffic is being received.

- **RSPAN Limitations**

The following limitations apply to the use of RSPAN on this switch:

- **RSPAN Ports** – Only ports can be configured as an RSPAN source, destination, or uplink; static and dynamic trunks are not allowed. A port can only be configured as one type of RSPAN interface – source, destination, or uplink. Also, note that the source port and destination port cannot be configured on the same switch.
- **Local/Remote Mirror** – The destination of a local mirror session (created on the Interface > Port > Mirror page) cannot be used as the destination for RSPAN traffic.
- **Spanning Tree** – If the spanning tree is disabled, BPDUs will not be flooded onto the RSPAN VLAN.
- **MAC address learning** is not supported on RSPAN uplink ports when RSPAN is enabled on the switch. Therefore, even if spanning tree is enabled after RSPAN has been configured, MAC address learning will still not be re-started on the RSPAN uplink ports.
- **IEEE 802.1X** – RSPAN and 802.1X are mutually exclusive functions.

When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.

- **Port Security** – If port security is enabled on any port, that port cannot be set as an RSPAN uplink port, even though it can still be configured as an RSPAN source or destination port. Also, when a port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

- **Session** – A number identifying this RSPAN session. (Range: 1)

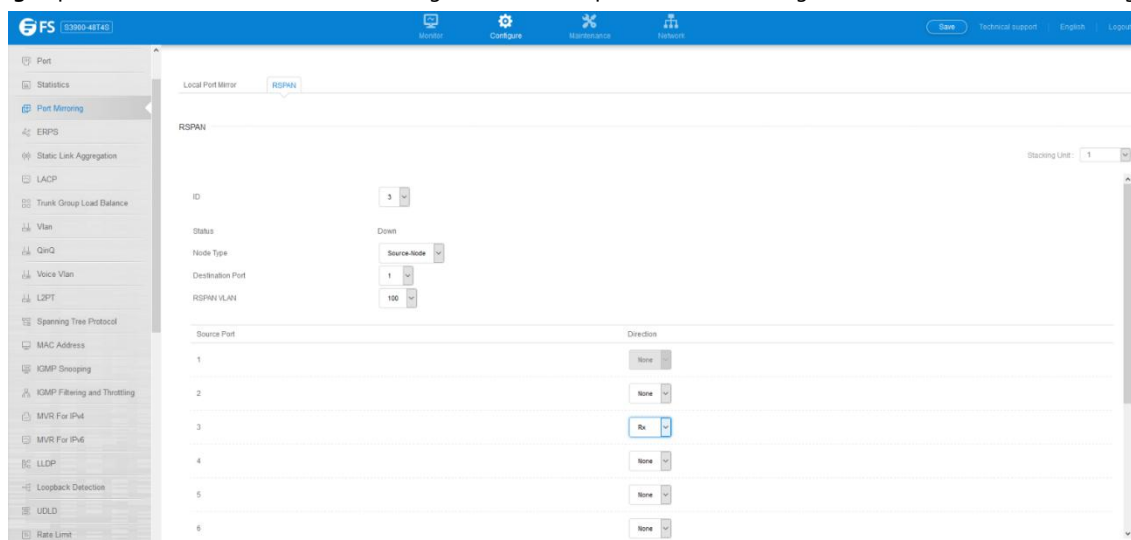
Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled, then no session can be configured for RSPAN.

- **Operation Status** – Indicates whether or not RSPAN is currently functioning.
- **Switch Role** – Specifies the role this switch performs in mirroring traffic.
 - **None** – This switch will not participate in RSPAN.
 - **Source** - Specifies this device as the source of remotely mirrored traffic.
 - **Intermediate** - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.
- **Destination** - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.
- **Remote VLAN** – The VLAN to which traffic mirrored from the source port will be flooded. The VLAN specified in this field must first be reserved for the RSPAN application using the Configure >VLAN >Static Vlan page.
- **Uplink Port** – A port on any switch participating in RSPAN through which mirrored traffic is passed on to or received from the RSPANVLAN.

Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.

Only destination and uplink ports will be assigned by the switch as members of the RSPAN VLAN. Ports cannot be manually assigned to an RSPAN VLAN through the Configure >VLAN >Static Vlan page. Nor can GVRP dynamically add port members to an RSPAN VLAN. Also, note that the Configure >VLAN >Static Vlan page will not display any members for an RSPANVLAN, but will only show configured RSPAN VLAN identifiers.

- **Type** – Specifies the traffic type to be mirrored remotely. (Options: Rx,Tx, Both)
- **Destination Port** – Specifies the destination port to monitor the traffic mirrored from the source ports. Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session. Also note that a destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.
- **Tag** – Specifies whether or not the traffic exiting the destination port to the monitoring device carries the RSPAN VLAN tag.



Source Port	Direction
1	None
2	None
3	Rx
4	None
5	None
6	None

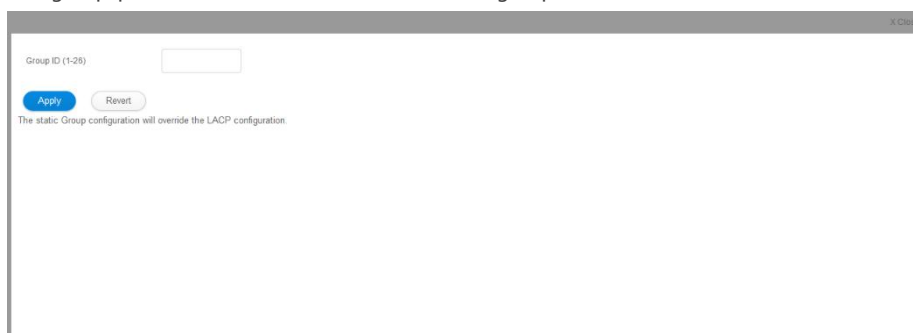
4.7 Static Link Aggregation

4.7.1 Static Group

Configure > Static Link Aggregation > Static Group page is used to create and delete static trunk group.



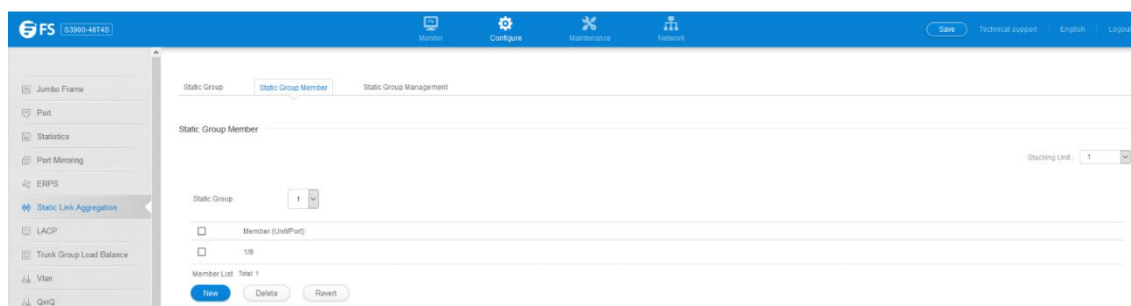
To create a static trunk group, press New button. You can create a new group.



- **Group ID** – Trunk identifier. (Range: 1-12)

4.7.2 Static Group Member

Configure > Static Link Aggregation > Static Group member page is used to add and delete static group member.



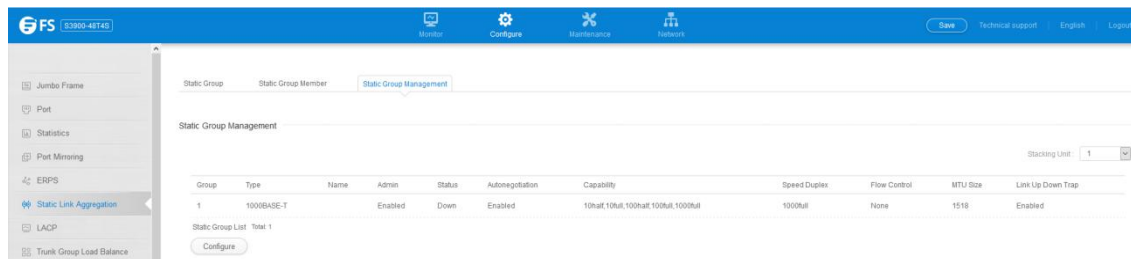
Member – The initial group member.

Unit – Unit identifier. (Range: 1)

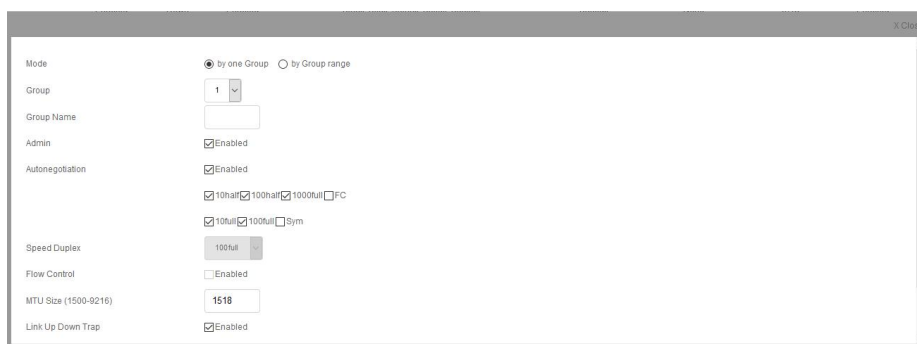
Port – Port identifier. (Range: 1-28)

4.7.3 Static Group Management

Configure > Static Link Aggregation > Static Group Management page is used to configure the parameters of trunk group.



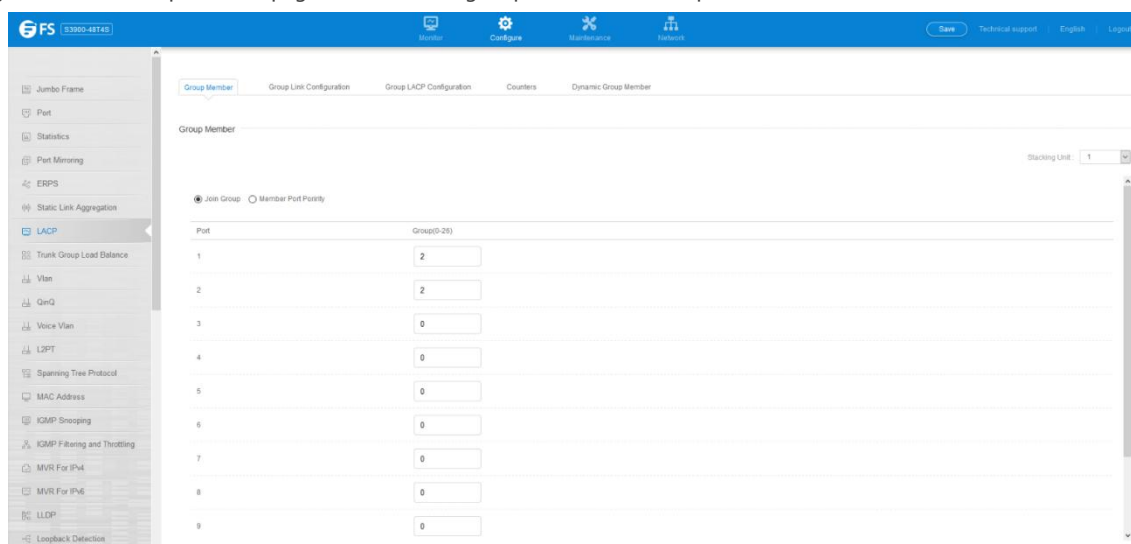
To configure the parameters, press Configure button.

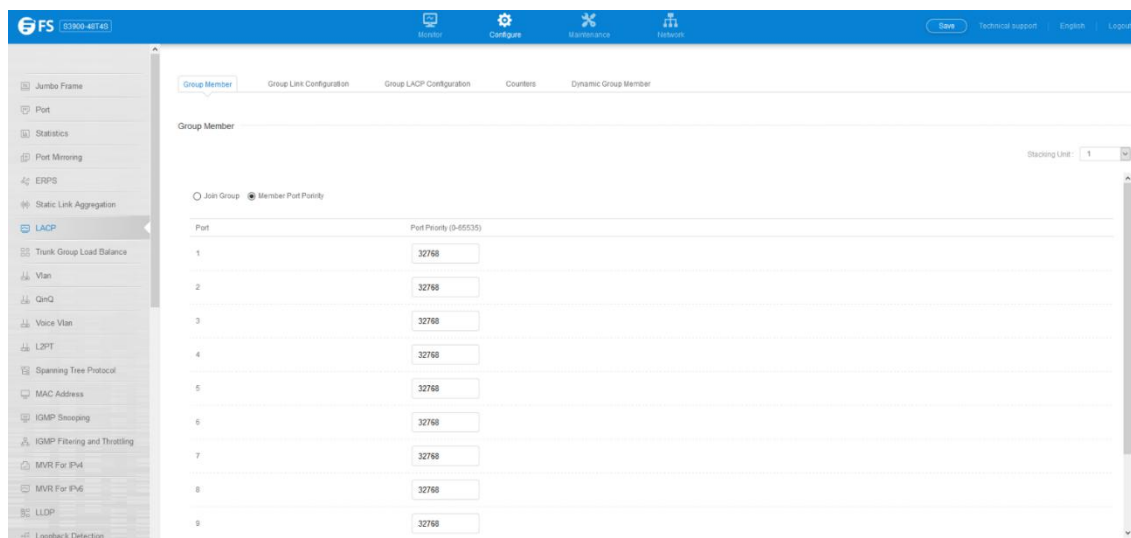


4.8 LACP

4.8.1 Group Member

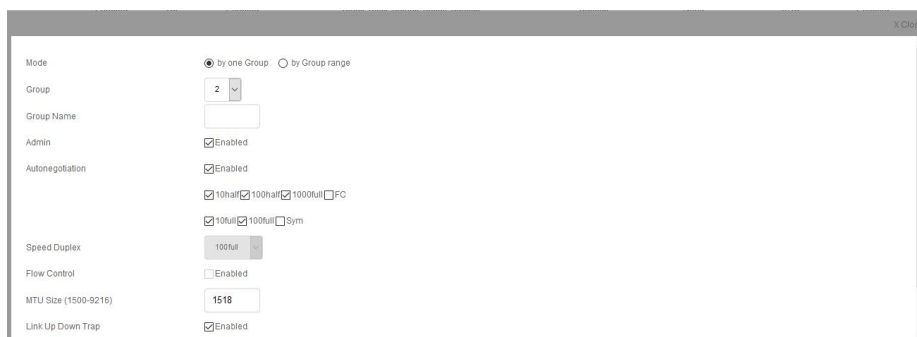
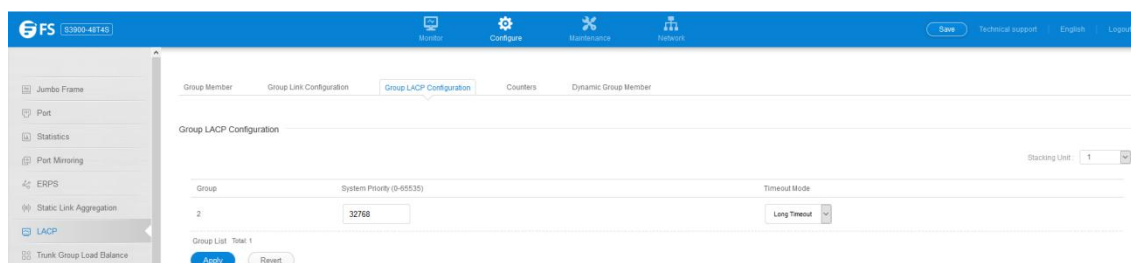
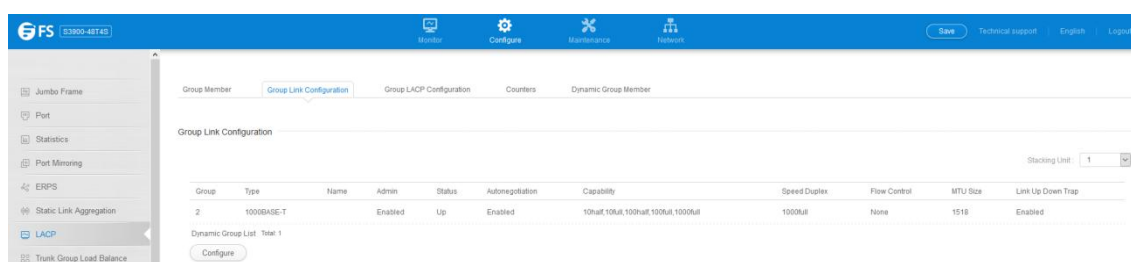
Configure > LACP > Group Member page is used to configure parameters of Group.





4.8.2 Group Link Configuration

Configure > LACP > Group Link Configuration page is used to display and configure parameters of LCAP trunk group.

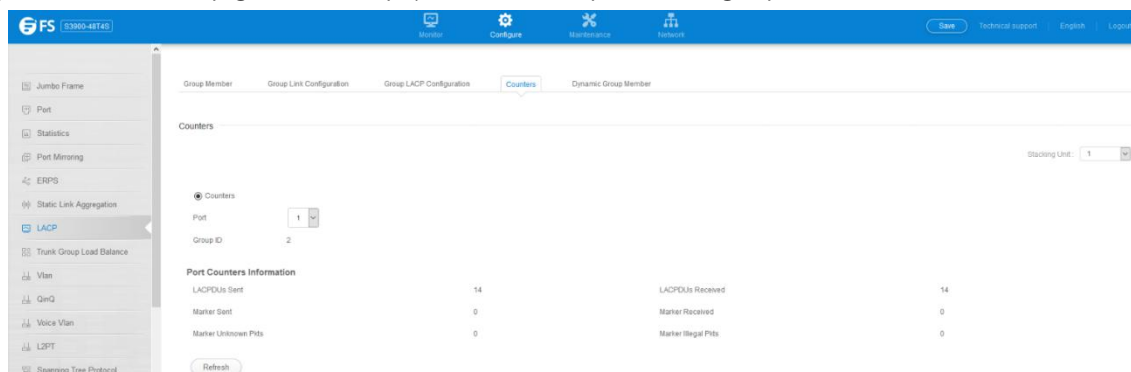


4.8.3 Group LACP Configuration

Configure > LACP > Group LACP Configuration page is used to display and configure System Priority and Timeout Mode of LCAP trunk group.

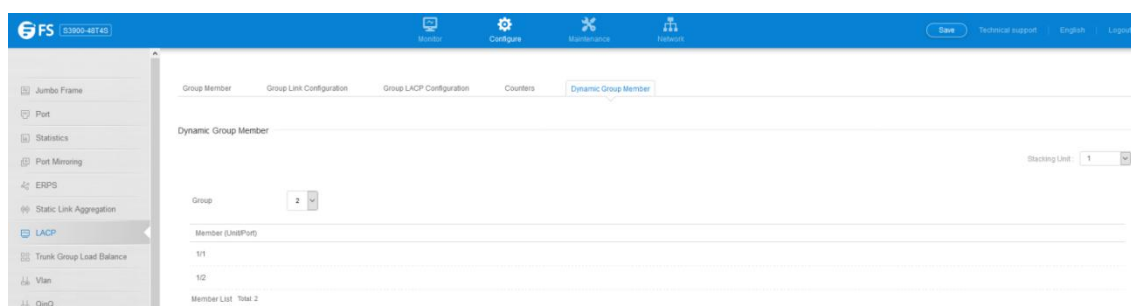
4.8.4 Counters

Configure > LACP > Counters page is used to display counters of local ports in LACP group.



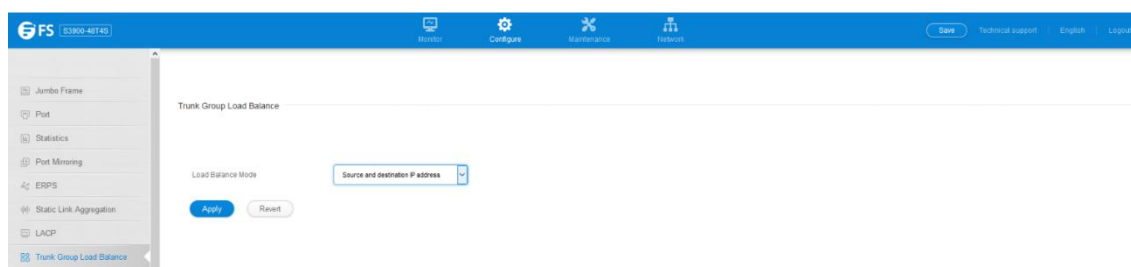
4.8.5 Show Dynamic Group Member

Configure > LACP > Show Dynamic Group Member page is used to display the current members of a LACP group.



4.9 Trunk Group Load Balance

Configure > Trunk Group Load Balance page is used to configure the load balance mode of trunk group.



- This page applies to all static and dynamic trunks on the switch.
- To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:
 - **Destination IP Address:** All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.
 - **Destination MAC Address:** All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.
 - **Source and Destination IP Address:** All traffic with the same source and destination IP address is output on the same link

in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is received from and destined for many different hosts.

- **Source and Destination MAC Address:** All traffic with the same source and destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from and destined for many different hosts.
- **Source IP Address:** All traffic with the same source IP address is output on the same link in a trunk. This mode works best for switch-to-router or switch-to-server trunk links where traffic through the switch is received from many different hosts.
- **Source MAC Address:** All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to switch trunk links where traffic through the switch is received from many different hosts.

4.10 Spanning Tree Protocol

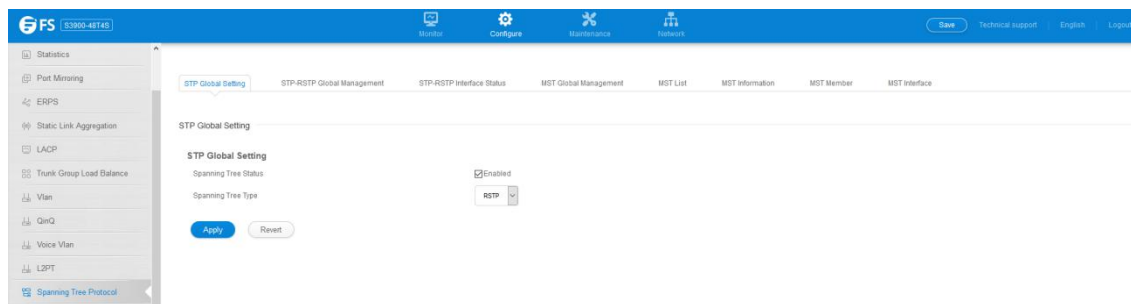
Versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s).

4.10.1 STP Global Setting

Configure >Spanning Tree Protocol >STP Global Setting page is used to configure STA status and the type of spanning tree.

- **Spanning Tree Status** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
 - **STP:** Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
 - **RSTP:** Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
 - **MSTP:** Multiple Spanning Tree (IEEE 802.1s).



4.10.2 STP-RSTP Global Management

Configure >Spanning Tree Protocol >STP-RSTP Global Management page is used to configure global settings for the spanning tree that apply to the entire switch.

- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
 - Default: 32768
 - Range: 0-61440, in steps of 4096
 - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
- **BPDU Flooding** – Configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port.

- To VLAN: Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID). This is the default.
- To All: Floods BPDUs to all other ports on the switch. The setting has no effect if BPDU flooding is disabled on a port.

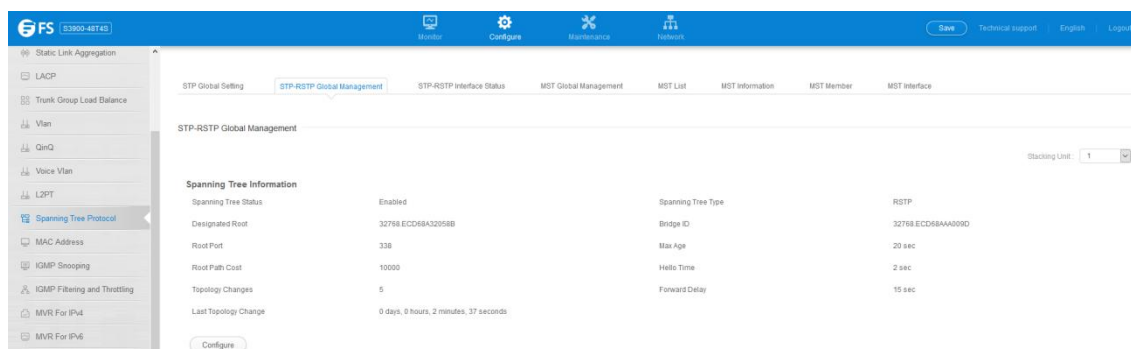
The following attributes are based on RSTP, but also apply to STP since the switch uses a backwards-compatible subset of RSTP to implement STP, and also apply to MSTP which is based on RSTP according to the standard:

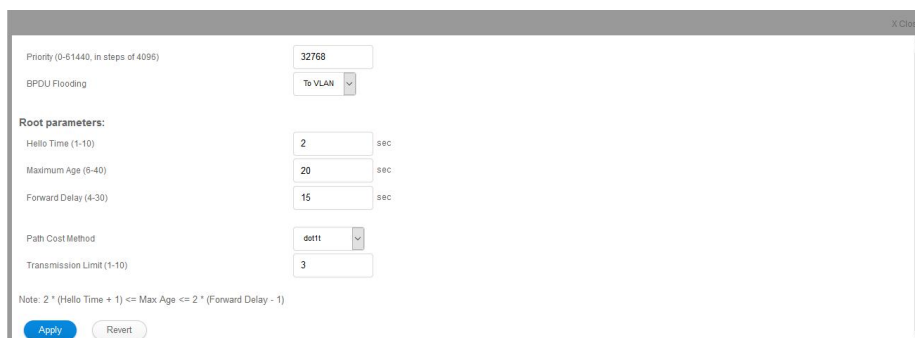
- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
 - Dot1t: Specifies 32-bit based values that range from 1-200,000,000.(This is the default.)
 - Dot1d-1998: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

When the Switch Becomes Root

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
 - Default: 2
 - Minimum: 1
 - Maximum: The lower of 10 or $[(\text{Max. Message Age} / 2) - 1]$
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconverge. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and groups.)
 - Default: 20
 - Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$
 - Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$
- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
 - Default: 15
 - Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$
 - Maximum: 30

RSTP does not depend on the forward delay timer in most cases. It is able to confirm that a port can transition to the forwarding state without having to rely on any timer configuration. To achieve fast convergence, RSTP relies on the use of edge ports, and automatic detection of point-to-point link types, both of which allow a port to directly transition to the forwarding state.





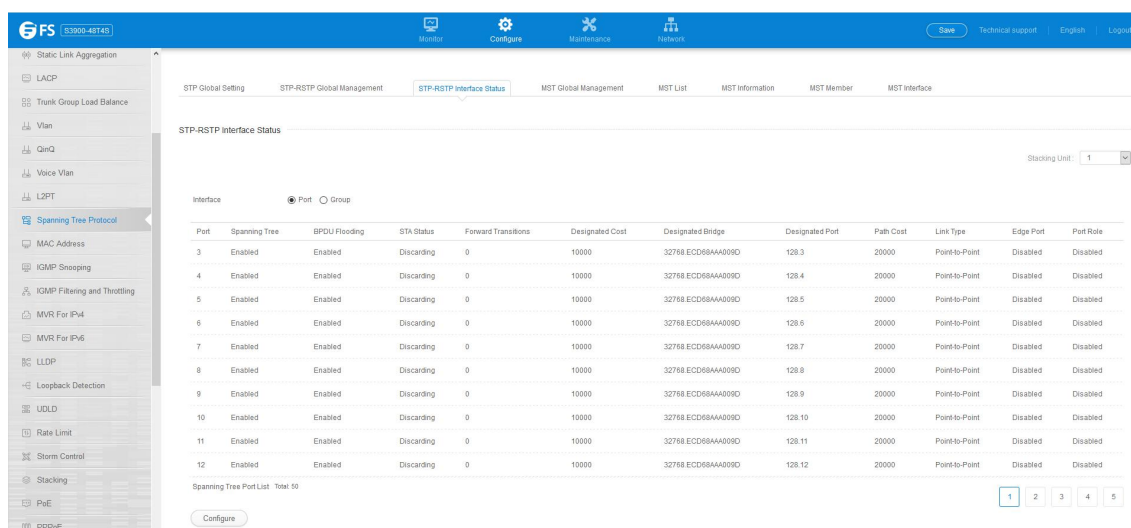
4.10.3 STP-RSTP Interface Status

Configure >Spanning Tree Protocol >STP-RSTP Interface Status page is used to display the current status of ports or groups in the Spanning Tree.

- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **BPDU Flooding** – Shows if BPDUs will be flooded to other ports when spanning tree is disabled globally on the switch or disabled on a specific port.
- **STA Status** – Displays current state of this port within the Spanning Tree:
 - **Discarding** - Port receives STA configuration messages, but does not forward packets.
 - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** - Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.
- If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
- All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration .
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology, that is the best port connecting a non-root bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), is the MSTI regional root (i.e., **master** port), or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.



Configure button is used to configure RSTP and MSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared media connection, and edge port to indicate if the attached device can support fast forwarding. (References to “ports” in this section means “interfaces” which includes both ports and groups.)

- **Interface** – Displays a list of ports or groups.
- **Spanning Tree** – Enables/disables STA on this interface.(Default: Enabled)
- **BPDU Flooding** - Enables/disables the flooding of BPDUs to other ports when global spanning tree is disabled or when spanning tree is disabled on a specific port. When flooding is enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port’s native VLAN as specified by the Spanning Tree BPDU Flooding attribute . (Default: Enabled)
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
 - Default: 128
 - Range: 0-240, in steps of 16
- **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost takes precedence over port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost methods, 1-200,000,000 for the long path cost method). By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 802.1w standard exceeds 65,535, the default is set to 65,535.

Table 12: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

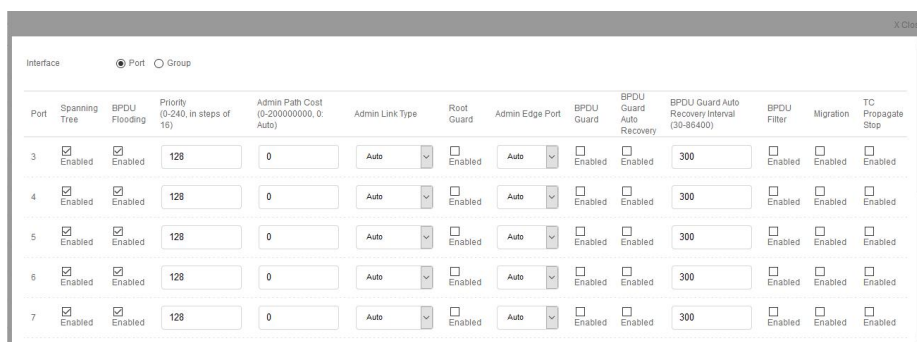
Table 13: Default STA Path Costs

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

- **Admin Link Type** – The link type attached to this interface.
 - Point-to-Point – A connection to exactly one other bridge.
 - Shared – A connection to two or more bridges.
 - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- **Root Guard** – STA allows a bridge with a lower bridge identifier (or same identifier and lower MAC address) to take over as the root bridge at any time. Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed. (Default: Disabled)
- **Admin Edge Port** – Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end node device. (Default: Auto)
 - **Enabled** – Manually configures a port as an Edge Port.
 - **Disabled** – Disables the Edge Port setting.
 - **Auto** – The port will be automatically configured as an edge port if the edge delay time expires without receiving any RSTP or MSTP BPDUs. Note that edge delay time (802.1D-2004 17.20.4) equals the protocol migration time if a port's link type is point-to-point (which is 3 seconds as defined in IEEE 802.3D-2004 17.20.4); otherwise it equals the spanning tree's maximum age for configuration messages. An interface cannot function as an edge port under the following conditions:
 - If spanning tree mode is set to STP, edge-port mode cannot automatically transition to operational edge-port state using the automatic setting.
 - If loopback detection is enabled and a loopback BPDU is detected, the interface cannot function as an edge port until the loopback state is released.
 - If an interface is in forwarding state and its role changes, the interface cannot continue to function as an edge port even if the edge delay time has expired.
 - If the port does not receive any BPDUs after the edge delay timer expires, its role changes to designated port and it immediately enters forwarding state.
- **BPDU Guard** – This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU an invalid configuration exists, such as a connection to an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)
- **BPDU Filter** – BPDU filtering allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes.

By default, STA sends BPDUs to all ports regardless of whether administrative edge is enabled on a port. BPDU filtering is configured on a per-port basis. (Default: Disabled)

- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

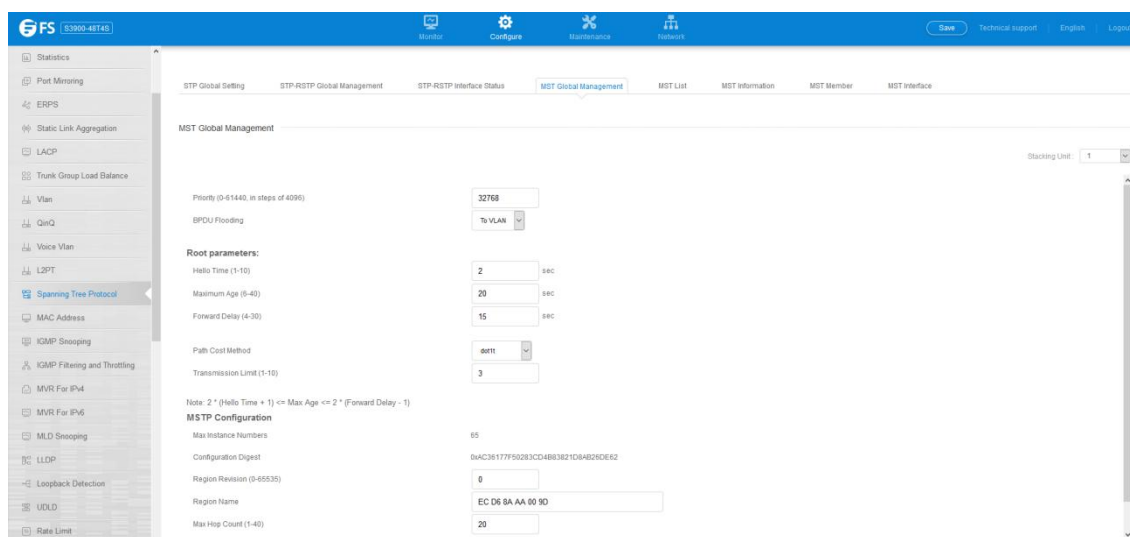


Port	Spanning Tree	BPDU Flooding	Priority (0-240, in steps of 16)	Admin Path Cost (0-200000000, 0: Auto)	Admin Link Type	Root Guard	Admin Edge Port	BPDU Guard	BPDU Guard Auto Recovery	BPDU Guard Auto Recovery Interval (30-3600s)	BPDU Filter	Migration	TC Propagate Stop
3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	300	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
4	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	300	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
5	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	300	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
6	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	300	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
7	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	300	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

4.10.4 MST Global Management

Configure > Spanning Tree Protocol > MST Global Management page is used configure MSTP global settings

- **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned.
- **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.
- **Region Revision** – The revision for this MSTI. (Range: 0-65535; Default: 0)
- **Region Name** – The name for this MSTI. (Maximum length: 32 characters; switch's MAC address)
- **Max Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)



STP Global Setting STP-RSTP Global Management STP-RSTP Interface Status **MST Global Management** MST List MST Information MST Member MST Interface

MST Global Management

Priority (0-61440, in steps of 4096): 32768

BPDU Flooding: To VLAN

Root parameters:

Hello Time (1-10): 2 sec

Maximum Age (6-40): 20 sec

Forward Delay (4-30): 15 sec

Path Cost Method: dotti

Transmission Limit (1-10): 3

Note: 2 * (Hello Time + 1) <= Max Age <= 2 * (Forward Delay - 1)

MSTP Configuration

Max Instance Numbers: 65

Configuration Digest: 0x4C36177F50283CD48B3821084828DE62

Region Revision (0-65535): 0

Region Name: EC D6 BA AA 00 90

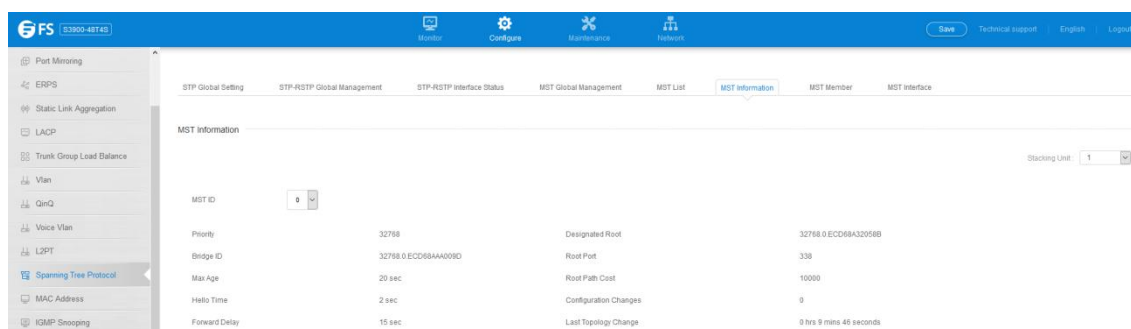
Max Hop Count (1-40): 20

4.10.5 MST Information

- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree type is set to MSTP, and MAC address (where the address is taken from the switch system).
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device

through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

- **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.



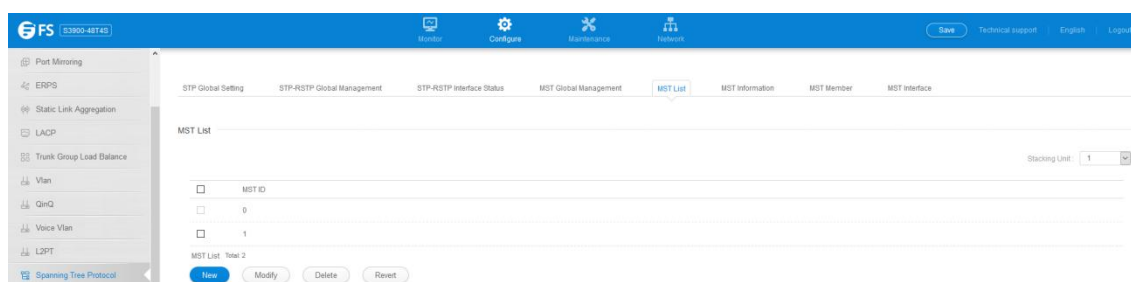
4.10.6 MST List

Configure > Spanning Tree Protocol > MST List page is used to create an MSTP instance, or to add VLAN groups to an MSTP instance.

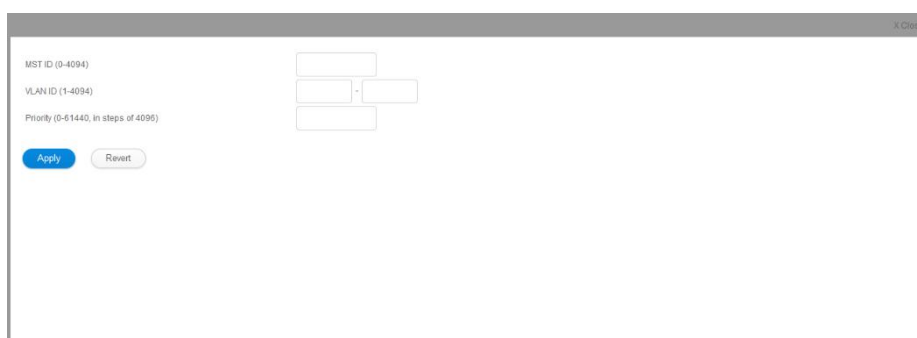
To use multiple spanning trees:

1. Set the spanning tree type to MSTP.
2. Enter the spanning tree priority for the selected MST instance on the Spanning Tree > MSTP (MST List - New) page.
3. Add the VLANs that will share this MSTI on the Spanning Tree > MSTP > (MST List - New) page.

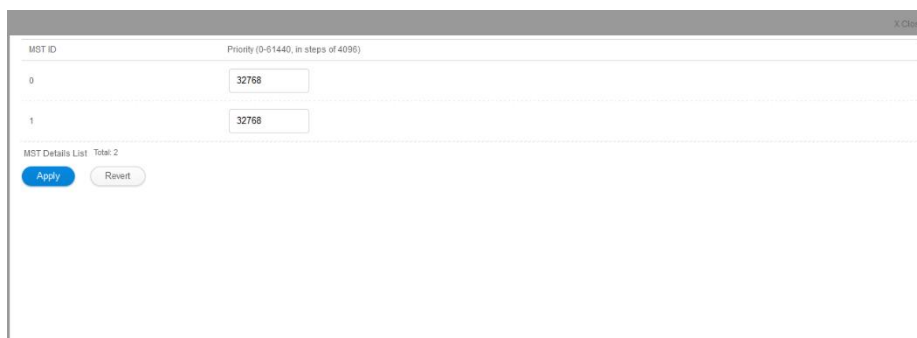
To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.



- **MST ID** – Instance identifier to configure. (Range: 0-4094)
- **VLAN ID** – VLAN to assign to this MST instance. (Range: 1-4093)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)



Press Modify button to edit the priority of the selected MST instance



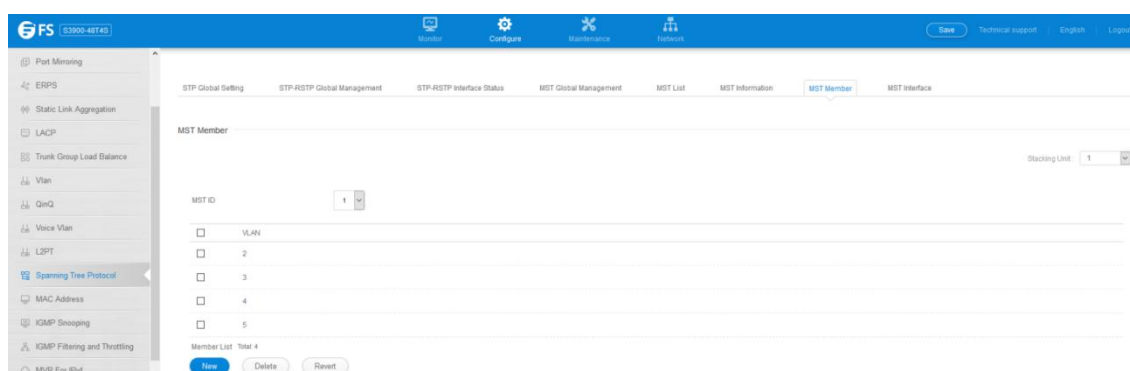
MST ID	Priority (0-61440, in steps of 4096)
0	32768
1	32768

MST Details List Total: 2

[Apply](#) [Revert](#)

4.10.7 MST Member

Configure > Spanning Tree Protocol > MST Member is used to display and configure VLAN members of an MST instance



Press New button to add VLAN members to the selected MST instance



4.10.8 MST Interface

Configure > Spanning Tree Protocol > MST Interface page is used to configure the STA interface settings for an MST instance.

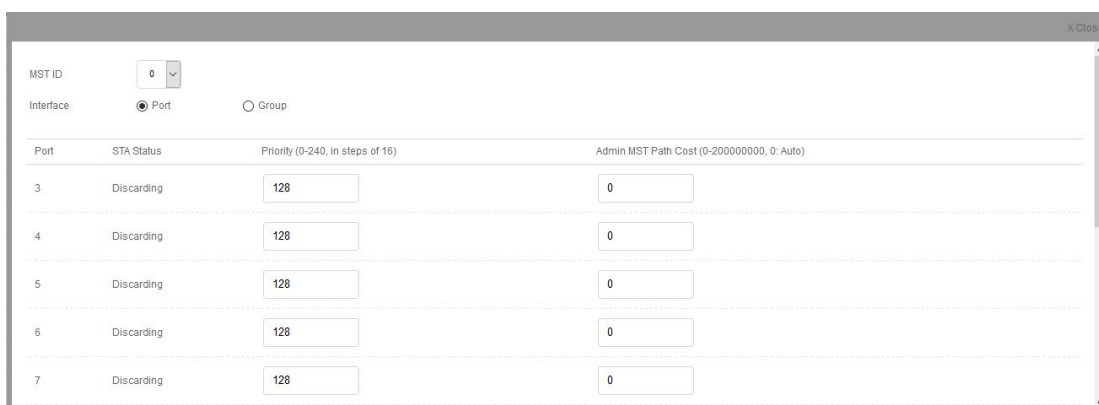
- **MST ID** – Instance identifier to configure. (Default: 0)
- **Interface** – Displays a list of ports or groups.
- **STA Status** – Displays the current state of this interface within the Spanning Tree.
 - **Discarding** – Port receives STA configuration messages, but does not forward packets.
 - **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** – Port forwards packets, and continues learning addresses.
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the

same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Default: 128; Range: 0-240, in steps of 16)

- **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535. By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

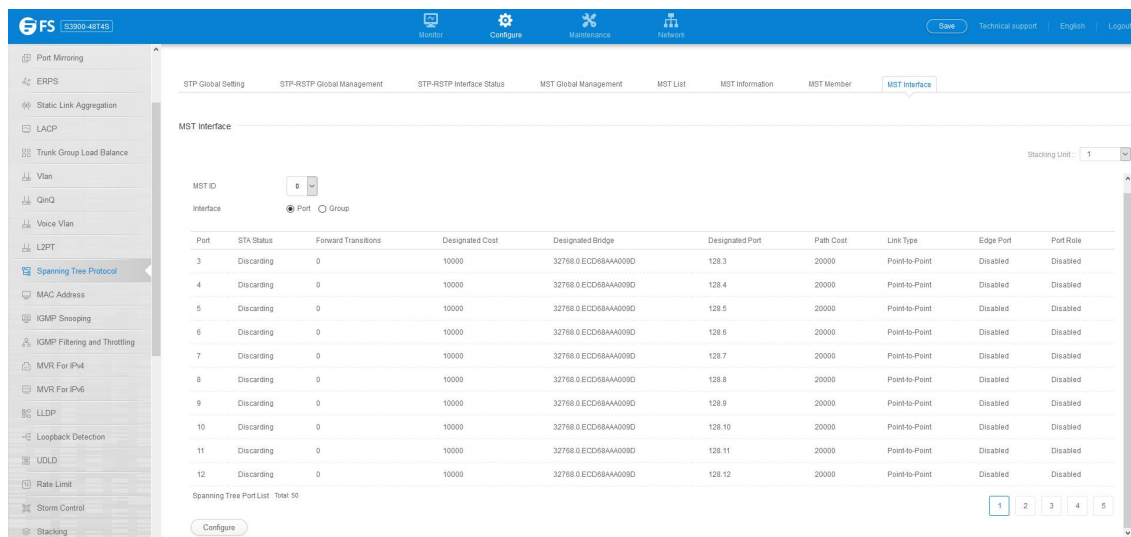
The recommended range is listed in [Table 12](#).

The default path costs are listed in [Table 13](#).



Port	STA Status	Priority (0-240, in steps of 16)	Admin MST Path Cost (0-200000000, 0: Auto)
3	Discarding	128	0
4	Discarding	128	0
5	Discarding	128	0
6	Discarding	128	0
7	Discarding	128	0

To display MSTP parameters for a port or group:



Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Path Cost	Link Type	Edge Port	Port Role
3	Discarding	0	10000	32768.0.ECD68AA009D	128.3	20000	Point-to-Point	Disabled	Disabled
4	Discarding	0	10000	32768.0.ECD68AA009D	128.4	20000	Point-to-Point	Disabled	Disabled
5	Discarding	0	10000	32768.0.ECD68AA009D	128.5	20000	Point-to-Point	Disabled	Disabled
6	Discarding	0	10000	32768.0.ECD68AA009D	128.6	20000	Point-to-Point	Disabled	Disabled
7	Discarding	0	10000	32768.0.ECD68AA009D	128.7	20000	Point-to-Point	Disabled	Disabled
8	Discarding	0	10000	32768.0.ECD68AA009D	128.8	20000	Point-to-Point	Disabled	Disabled
9	Discarding	0	10000	32768.0.ECD68AA009D	128.9	20000	Point-to-Point	Disabled	Disabled
10	Discarding	0	10000	32768.0.ECD68AA009D	128.10	20000	Point-to-Point	Disabled	Disabled
11	Discarding	0	10000	32768.0.ECD68AA009D	128.11	20000	Point-to-Point	Disabled	Disabled
12	Discarding	0	10000	32768.0.ECD68AA009D	128.12	20000	Point-to-Point	Disabled	Disabled

4.11 IGMP Snooping

4.11.1 Global Setting

Configure > IGMP Snooping > Global Setting page is used to configure the switch to forward multicast traffic.

- **IGMP Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled)

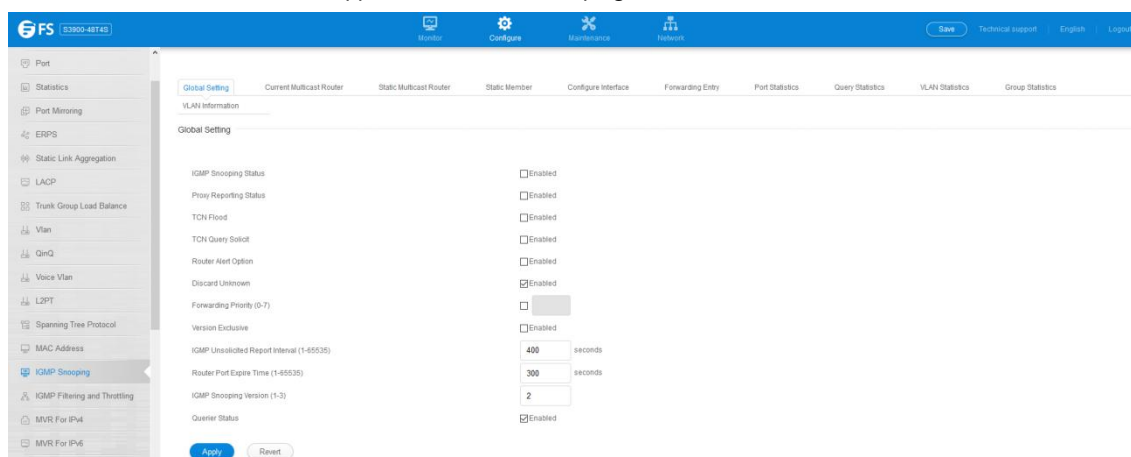
When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence. When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

- **Proxy Reporting Status** – Enables IGMP Snooping with Proxy Reporting. (Default: Disabled)

When proxy reporting is enabled with this command, the switch performs “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.

When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.

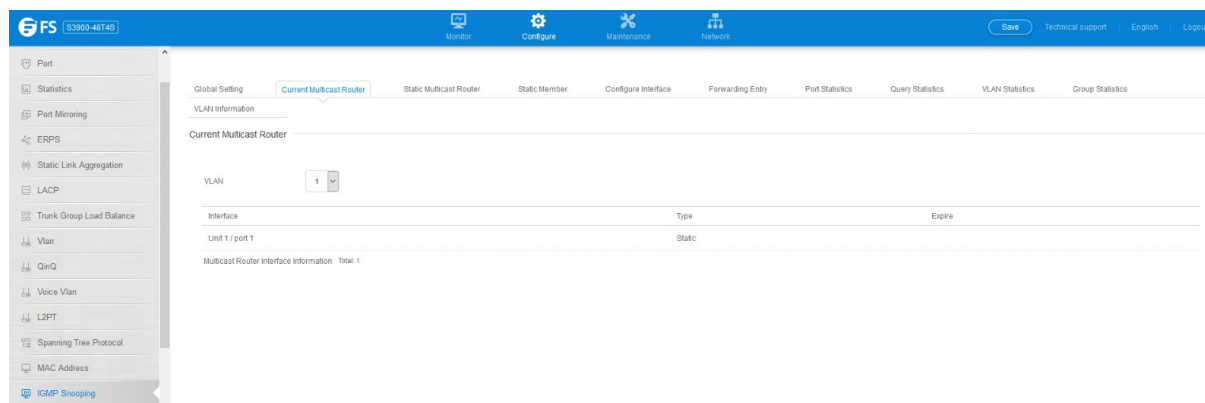
- **TCN Flood** – Enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. (Default: Disabled)
- **TCN Query Solicit** – Sends out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. (Default: Disabled)
- **Router Alert Option** – Discards any IGMPv2/v3 packets that do not include the Router Alert option. (Default: Disabled)
- **Discard Unknown** – Discards unregistered multicast traffic. (Default: Enabled)
- **Forwarding Priority** – Assigns a CoS priority to all multicast traffic. (Range: 0-6, where 6 is the highest priority)
- **Version Exclusive** – Discards any received IGMP messages which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)
- **IGMP Unsolicited Report Interval** – Specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. (Range: 1-65535 seconds, Default: 400 seconds)
- **Router Port Expire Time** – The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535, Recommended Range: 300-500 seconds, Default: 300)
- **IGMP Snooping Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2)
- **Querier Status** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. This feature is not supported for IGMPv3 snooping. (Default: Disabled)



4.11.2 Current Multicast Router

Configure >IGMP Snooping >Current Multicast Router page is used to statically show an interface to a multicast router/switch.

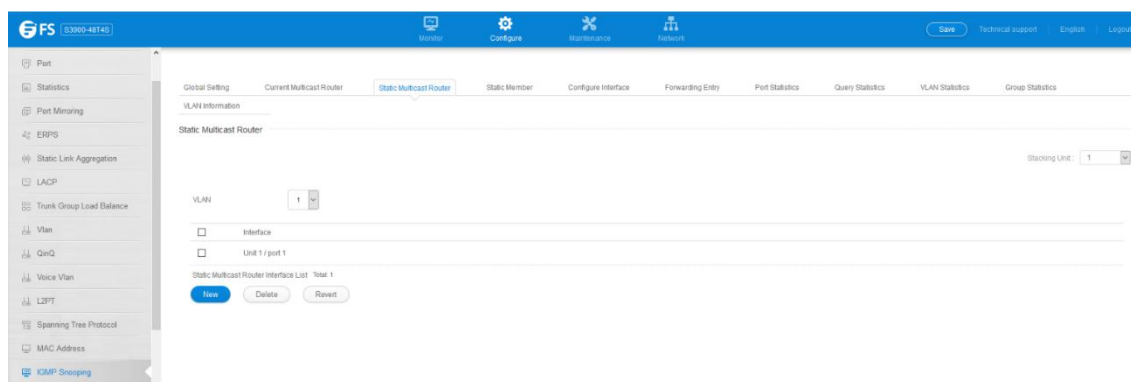
- **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4093)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port or Group** – Specifies the interface attached to a multicast router.



4.11.3 Static Multicast Router

Configure >IGMP Snooping >Static Multicast Router page is used to statically attach an interface to a multicast router/switch.

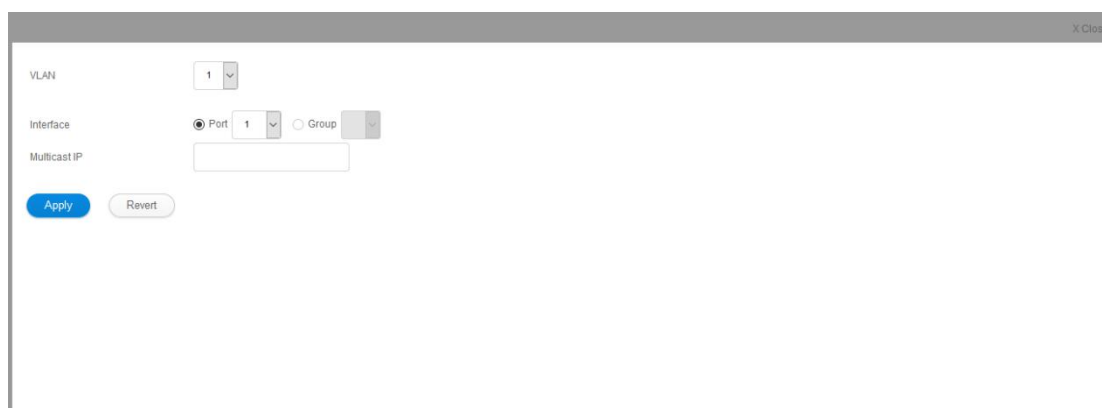
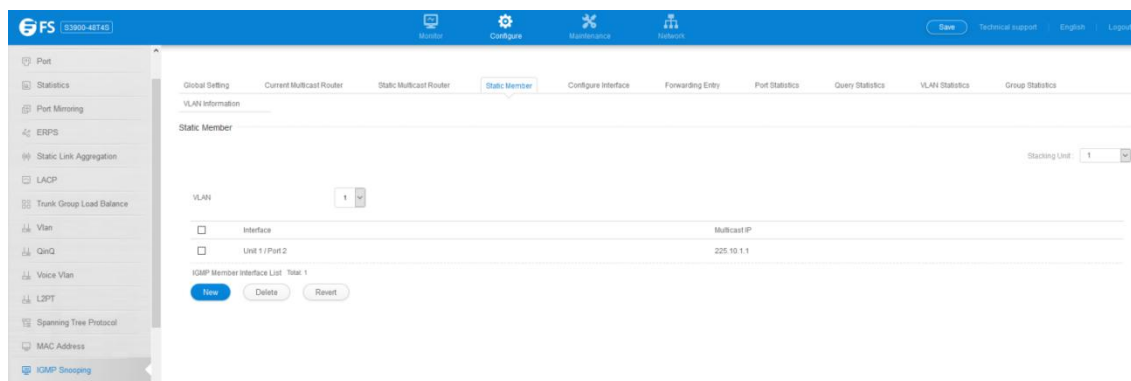
- **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4093)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port or Group** – Specifies the interface attached to a multicast router.



4.11.4 Static Member

Configure >IGMP Snooping >Static Member page is used to statically assign a multicast service to an interface. Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages.

- **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4093)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port or Group** – Specifies the interface assigned to a multicast group.
- **Multicast IP** – The IP address for a specific multicast service.



4.11.5 VLAN Information

Configure >IGMP Snooping >VLAN Information page is used to configure IGMP snooping attributes for a VLAN.

- **VLAN** – ID of configured VLANs. (Range: 1-4093)
- **IGMP Snooping Status** – When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled)

When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence. When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

- **Version Exclusive** – Discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled) If version exclusive is disabled on a VLAN, then this setting is based on the global setting configured on the Multicast > IGMP Snooping > General page. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- **Immediate Leave Status** – Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled) If immediate leave is not used, a multicast router (or querier) will send a group-specific query message when an IGMPv2 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified time out period.

Note that this time out is set to Last Member Query Interval *Robustness Variable (fixed at 2) as defined in RFC 2236.

If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping. This attribute is only effective if IGMP snooping is enabled, and IGMPv2 snooping is used.

- **Multicast Router Discovery** – MRD is used to discover which interfaces are attached to multicast routers. (Default: Enabled)
- **General Query Suppression** – Suppresses general queries except for ports attached to downstream multicast hosts. (Default: Disabled) By default, general query messages are flooded to all ports, except for the multicast router through which they are

received. If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

- **Proxy Reporting** – Enables IGMP Snooping with Proxy Reporting.(Default: Based on global setting)When proxy reporting is enabled with this command, the switch performs “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression.Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.
- **Interface Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2)This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.
- **Query Interval** – The interval between sending IGMP proxy general queries. (Range: 2-31744 seconds; Default: 125 seconds)An IGMP general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined. This command applies when the switch is serving as the querier, or as a proxy host when IGMP snooping proxy reporting is enabled .
- **Query Response Interval** – The maximum time the system waits for a response to proxy general queries. (Range: 10-31744 tenths of a second; Default: 10 seconds)This command applies when the switch is serving as the querier , or as a proxy host when IGMP snooping proxy reporting is enabled .
- **Last Member Query Interval** – The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31740 tenths of a second in multiples of 10; Default: 1 second)When a multicast host leaves a group, it sends an IGMP leave message.When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router. A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more burst traffic. This attribute will take effect only if IGMP snooping proxy reporting is enabled or IGMP querier is enabled .
- **Last Member Query Count** – The number of IGMP proxy group specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. (Range: 1-255; Default: 2) This attribute will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled.
- **Proxy Query Address** – A static source address for locally generated query and report messages used by IGMP Proxy Reporting. (Range: Any valid IP unicast address; Default: 0.0.0.0) IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

To resolve this problem, the source address in proxied IGMP query messages can be replaced with any valid unicast address (other than the router's own address).

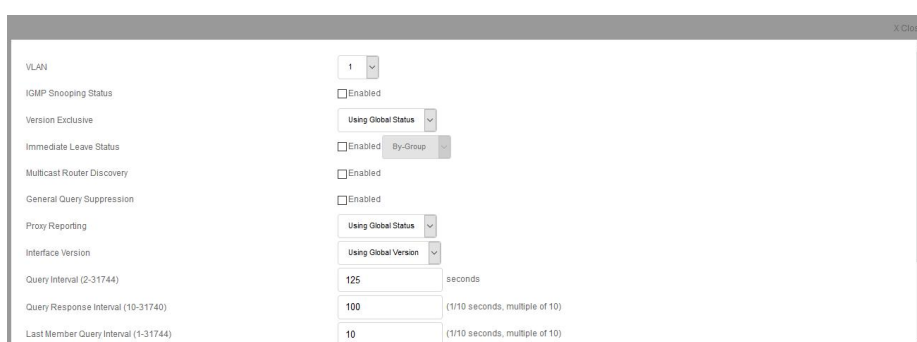
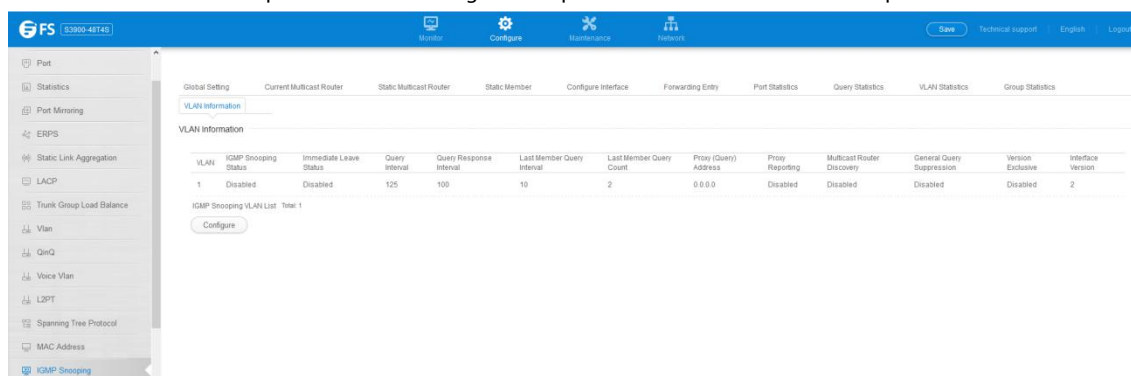
Rules Used for Proxy Reporting

When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set.

When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

- If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.
- If a proxy query address is not configured, the switch will use the VLAN's IP address as the IP source address in general and

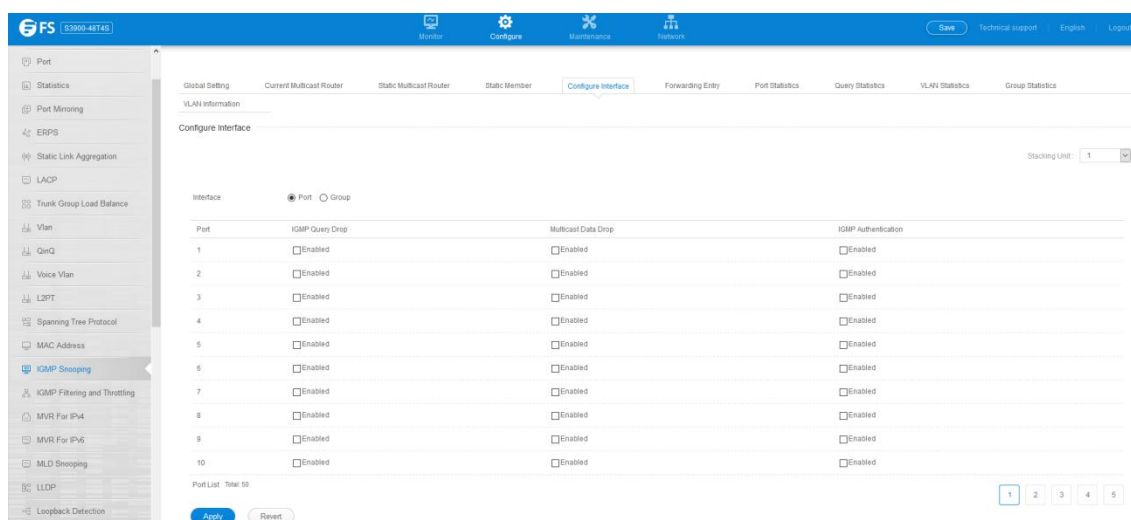
group specific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.



4.11.6 Configure Interface

Configure >IGMP Snooping >Configure Interface page is used to configure an interface to drop IGMP query packets.

- **IGMP Query Drop** – Configures an interface to drop any IGMP query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.



4.11.7 Forwarding Entry

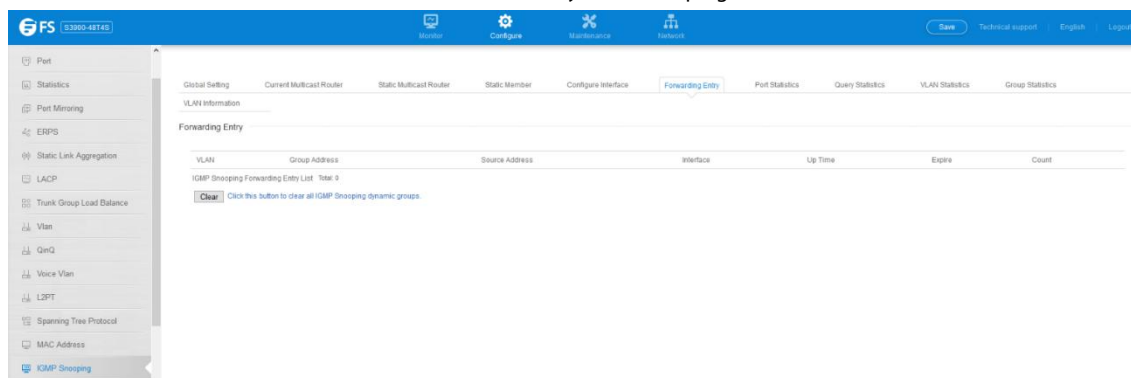
Configure >IGMP Snooping >Forwarding Entry page is used to display the forwarding entries learned through IGMP Snooping.

COMMAND USAGE

To display information about multicast groups, IGMP Snooping must first be enabled on the switch .

- **VLAN** – An interface on the switch that is forwarding traffic to downstream ports for the specified multicast group address.

- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- **Interface** – A downstream port or trunk that is receiving traffic for the specified multicast group. This field may include both dynamically and statically configured multicast router ports.
- **Up Time** – Time that this multicast group has been known.
- **Expire** – Time until this entry expires.
- **Count** – The number of times this address has been learned by IGMP snooping.



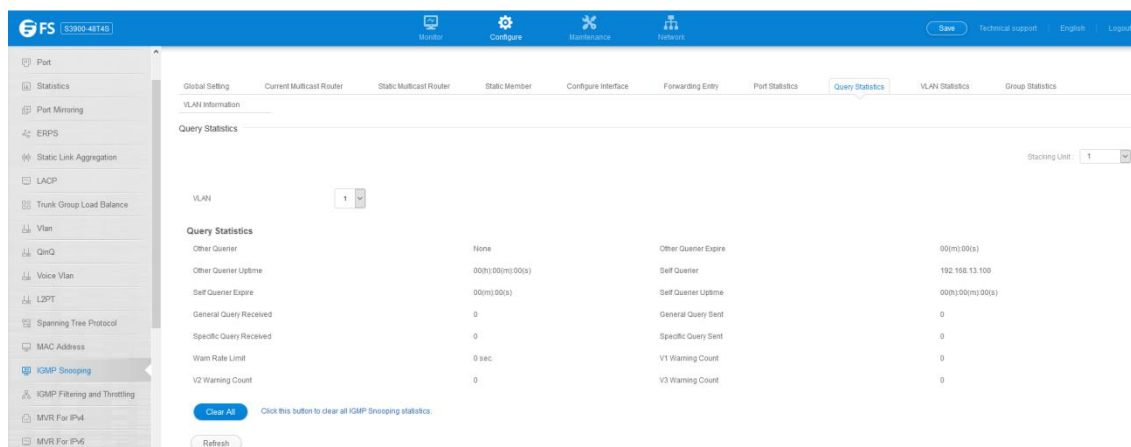
4.11.8 Query Statistics

Configure >IGMP Snooping >Query Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

- **VLAN** – VLAN identifier. (Range: 1-4093)
- **Port** – Port identifier. (Range: 1-28)
- **Group** – Group identifier. (Range: 1-12)

Query Statistics

- **Querier IP Address** – The IP address of the querier on this interface.
- **Querier Expire Time** – The time after which this querier is assumed to have expired.
- **General Query Received** – The number of general queries received on this interface.
- **General Query Sent** – The number of general queries sent from this interface.
- **Specific Query Received** – The number of specific queries received on this interface.
- **Specific Query Sent** – The number of specific queries sent from this interface.
- **Number of Reports Sent** – The number of reports sent from this interface.
- **Number of Leaves Sent** – The number of leaves sent from this interface. VLAN, Port, and Group Statistics Input Statistics
- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of IGMP groups active on this interface. Output Statistics
- **Report** – The number of IGMP membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.



4.11.9 VLAN Statistics

Configure > IGMP Snooping > Vlan Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

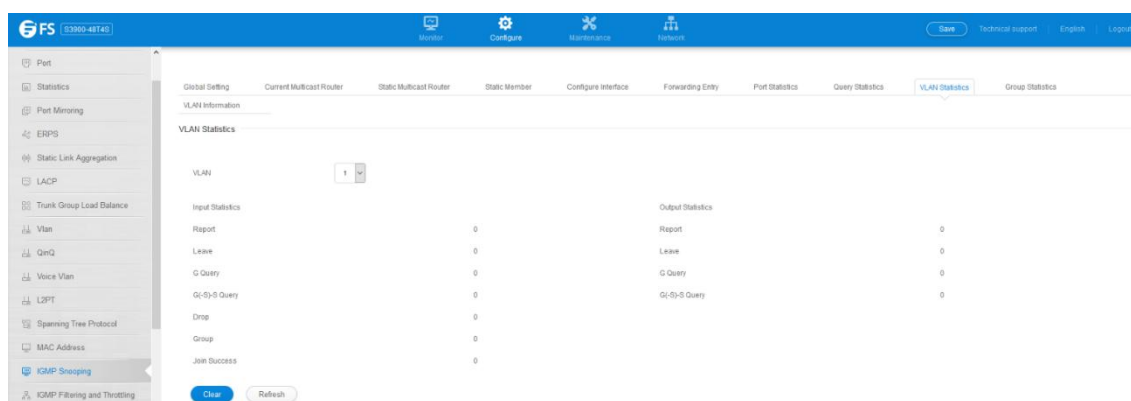
- **VLAN** – VLAN identifier. (Range: 1-4093)

Query Statistics

- **Querier IP Address** – The IP address of the querier on this interface.
- **Querier Expire Time** – The time after which this querier is assumed to have expired.
- **General Query Received** – The number of general queries received on this interface.
- **General Query Sent** – The number of general queries sent from this interface.
- **Specific Query Received** – The number of specific queries received on this interface.
- **Specific Query Sent** – The number of specific queries sent from this interface.
- **Number of Reports Sent** – The number of reports sent from this interface.
- **Number of Leaves Sent** – The number of leaves sent from this interface. VLAN, Port, and Group Statistics Input Statistics
- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of IGMP groups active on this interface.

Output Statistics

- **Report** – The number of IGMP membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.



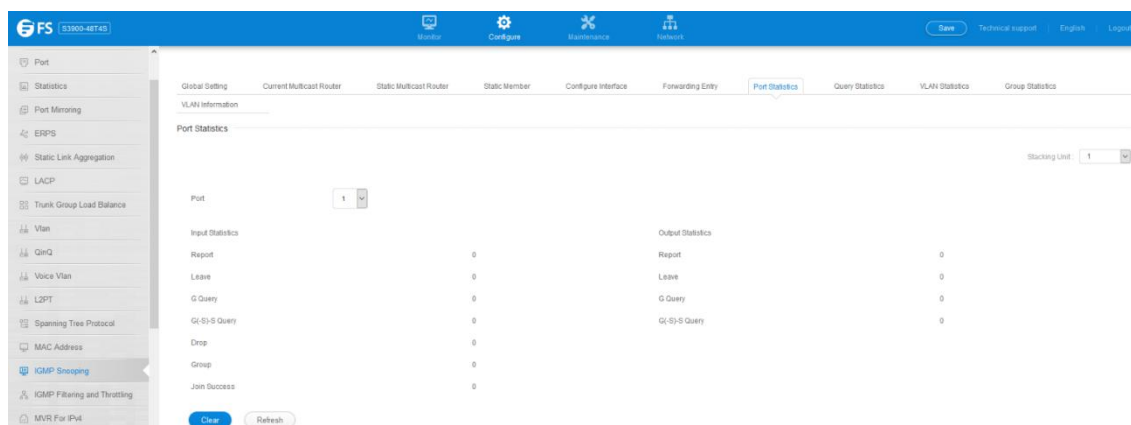
4.11.10 Port Statistics

Configure >IGMP Snooping >Port Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

- **Port** – Port identifier. (Range: 1-28)

Input Statistics

- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.
- **Join Success** – The number of times a multicast group was successfully joined.



- **Group** – The number of IGMP groups active on this interface.

Output Statistics

- **Report** – The number of IGMP membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.11.11 Group Statics

Configure >IGMP Snooping >Group Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

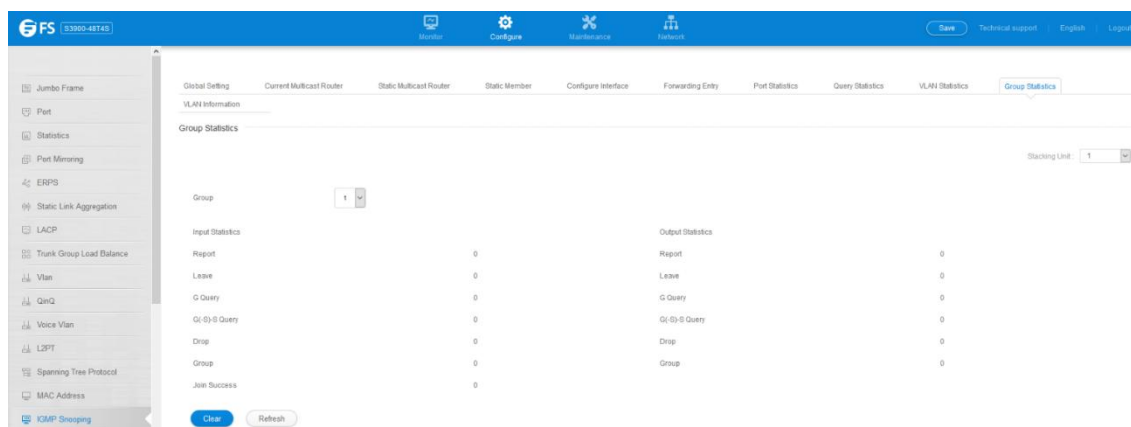
- **Group** – Group identifier. (Range: 1-12)

Query Statistics

- **Querier IP Address** – The IP address of the querier on this interface.
- **Querier Expire Time** – The time after which this querier is assumed to have expired.
- **General Query Received** – The number of general queries received on this interface.
- **General Query Sent** – The number of general queries sent from this interface.
- **Specific Query Received** – The number of specific queries received on this interface.
- **Specific Query Sent** – The number of specific queries sent from this interface.
- **Number of Reports Sent** – The number of reports sent from this interface.
- **Number of Leaves Sent** – The number of leaves sent from this interface. VLAN, Port, and Group Statistics Input Statistics
- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of IGMP groups active on this interface.

Output Statistics

- **Report** – The number of IGMP membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

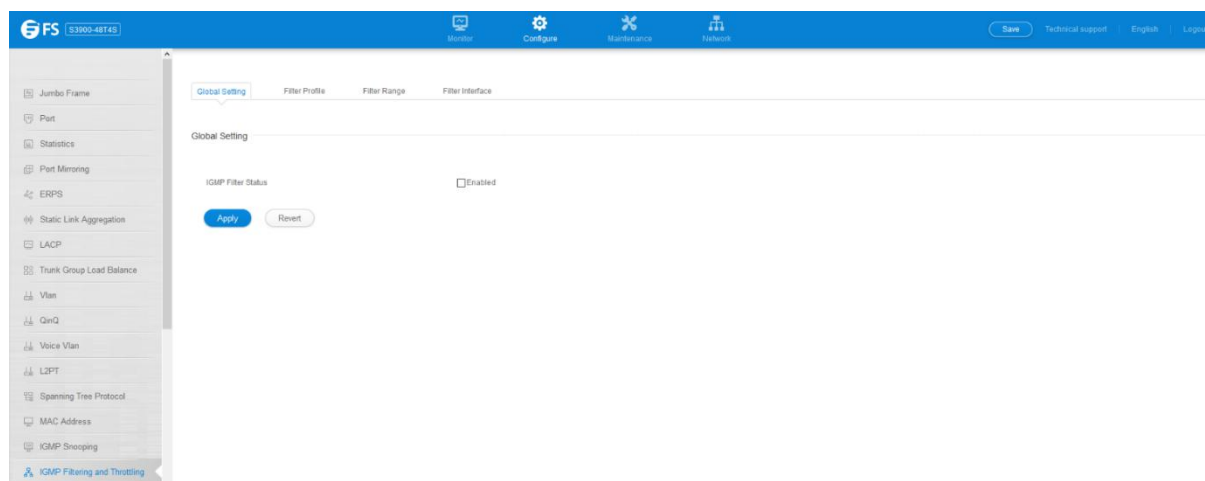


4.12 IGMP Filtering and Throttling

4.12.1 Global Setting

Configure > IGMP Filtering and Throttling > Global Setting page is used to enable IGMP filtering and throttling globally on the switch.

- **IGMP Filter Status** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)



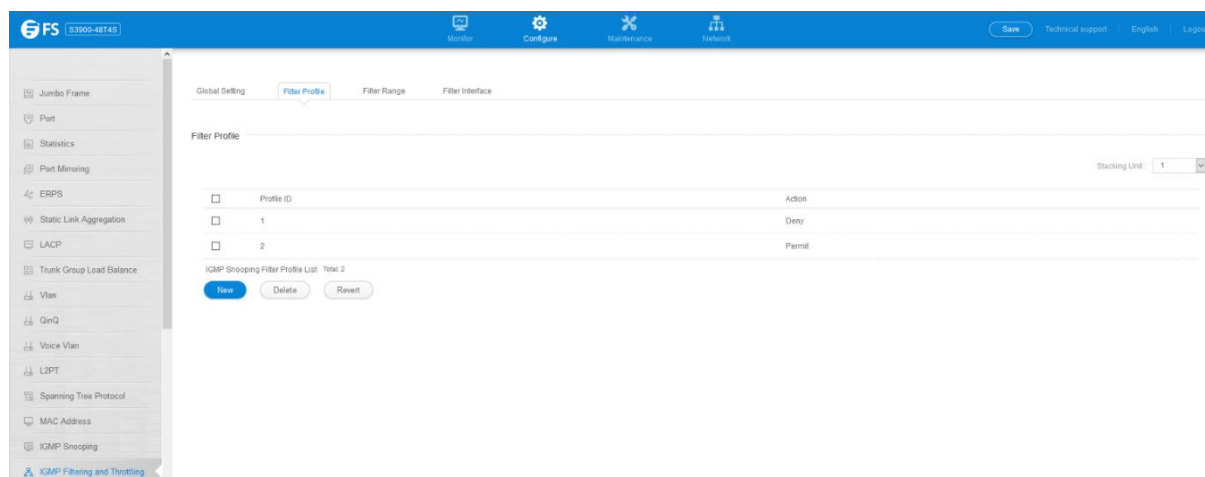
4.12.2 Filter Profile

Configure >IGMP Filtering and Throttling >Filter Profile page is used to create an IGMP profile and set its access mode. Then use the (Add Multicast Group Range) page to configure the multicast groups to filter.

- **Profile ID** – Creates an IGMP profile. (Range: 1-4294967295)
- **Access Mode** – Sets the access mode of the profile; either permit or deny. (Default: Deny)

When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when the multicast group is not in the controlled range. Add Multicast Group Range

- **Profile ID** – Selects an IGMP profile to configure.
- **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.
- **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.





Profile ID (1-4294867295)

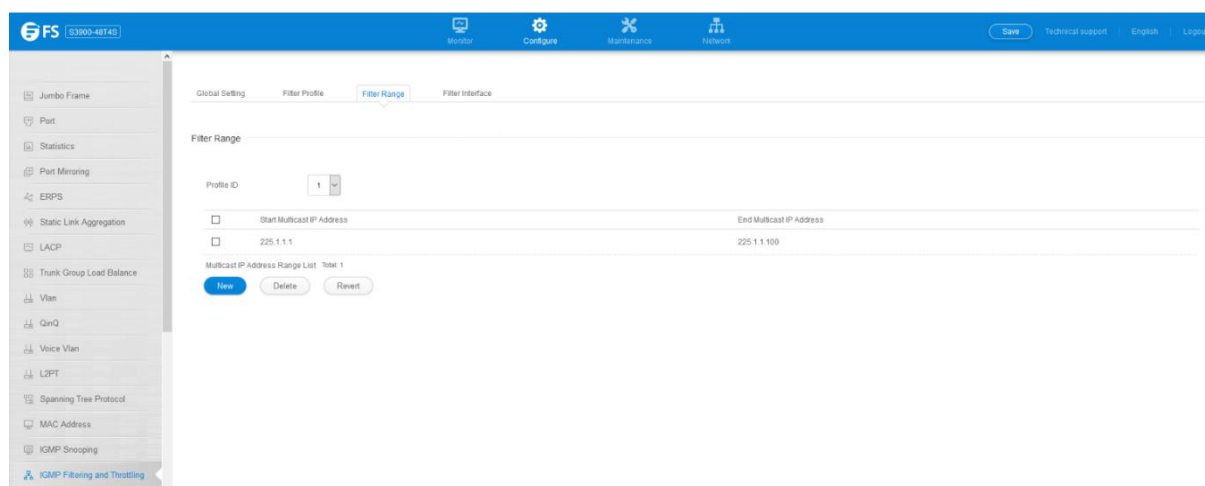
Action: Deny

Buttons: Apply, Revert

4.12.3 Filter Range

Configure >IGMP Filtering and Throttling >Filter Range page is used to create an IGMP range and set its access mode. Then use the (new Multicast Group Range) page to configure the multicast groups to filter.

- **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.
- **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.



FS S3900-48T4S

Monitor Configure Maintenance Network

Save Technical support English Logout

Global Setting Filter Profile **Filter Range** Filter Interface

Filter Range

Profile ID: 1

Start Multicast IP Address	End Multicast IP Address
225.1.1.1	225.1.1.100

Multicast IP Address Range List Total: 1

Buttons: New, Delete, Revert



Profile ID: 1

Start Multicast IP Address:

End Multicast IP Address:

Buttons: Apply, Revert

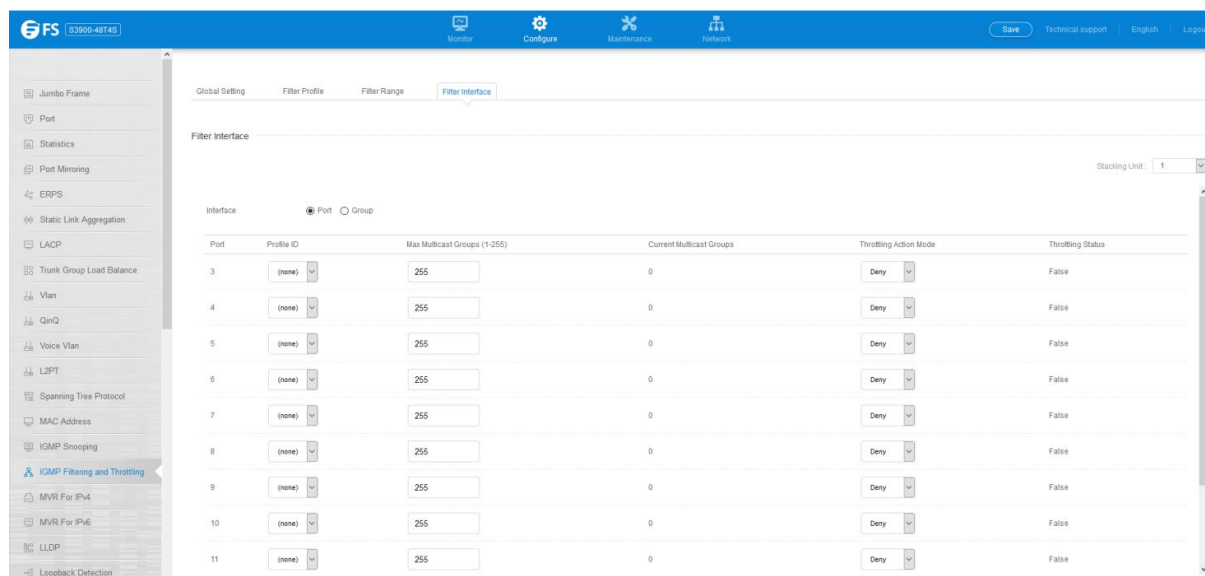
4.12.4 Configure Filter Interface

Configure >IGMP Filtering and Throttling >Configure Filter Interface page is used to assign and IGMP filter profile to interfaces on the switch, or to throttle multicast traffic by limiting the maximum number of multicast groups an interface can join at the same time.

- **Interface** – Port or group identifier.

An IGMP profile or throttling setting can be applied to a port or trunk. When ports are configured as trunk members, the trunk uses the settings applied to the first port member in the trunk.

- **Profile ID** – Selects an existing profile to assign to an interface.
- **Max Multicast Groups** – Sets the maximum number of multicast groups an interface can join at the same time. (Range: 1-255; Default: 255)
- **Current Multicast Groups** – Displays the current multicast groups the interface has joined.
- **Throttling Action Mode** – Sets the action to take when the maximum number of multicast groups for the interface has been exceeded.(Default: Deny)
 - **Deny** - The new multicast group join report is dropped.
 - **Replace** - The new multicast group replaces an existing group.
- **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)



4.13 MLD Snooping

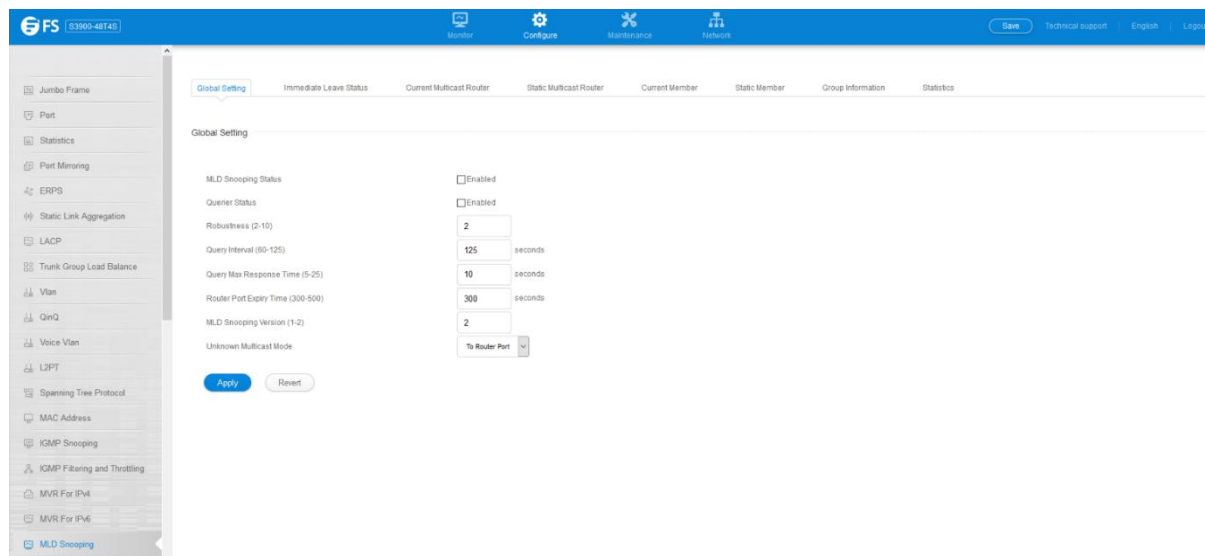
4.13.1 Global Setting

Configure >MLD Snooping >Global Setting page is used to configure the switch to forward multicast traffic intelligently.

- **MLD Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. (Default: Disabled)
- **Querier Status** – When enabled, the switch can serve as the querier for MLDv2 snooping if elected. The querier is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled) An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses this IPv6 address as the query source address. The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.
- **Robustness** – MLD Snooping robustness variable. A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report. (Range: 2-10 Default: 2)
- **Query Interval** – The interval between sending MLD general queries. (Range: 60-125 seconds; Default: 125 seconds) This attribute applies when the switch is serving as the querier. An MLD general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.
- **Query Max Response Time** – The maximum response time advertised in MLD general queries. (Range: 5-25 seconds; Default: 10 seconds) This attribute controls how long the host has to respond to an MLD Query message before the switch deletes the group

if it is the last member.

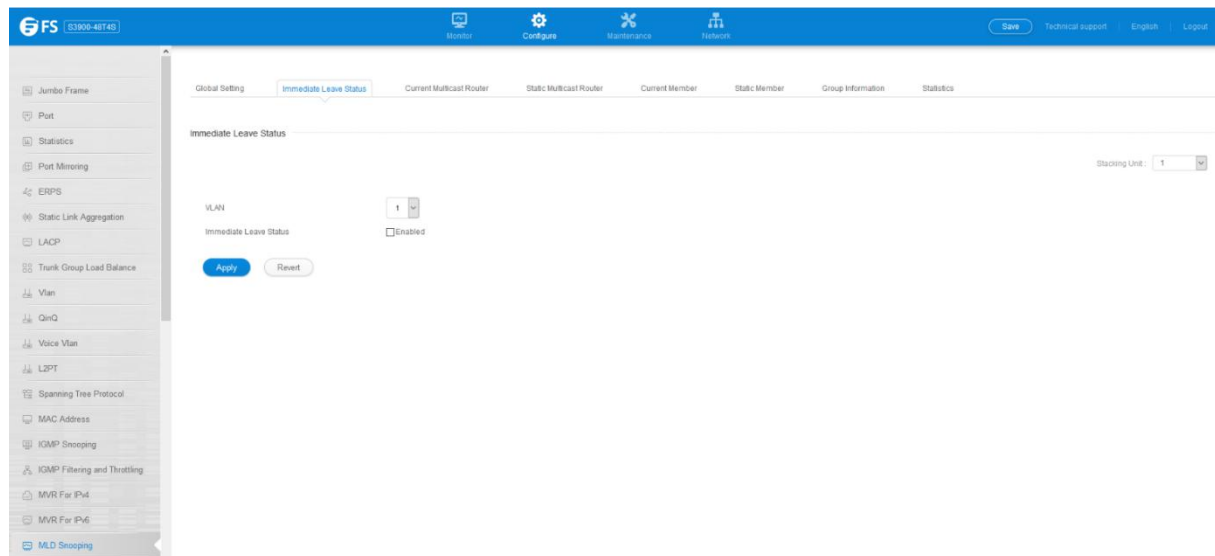
- **Router Port Expiry Time** – The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired. (Range: 300-500 seconds; Default: 300 seconds)
- **MLD Snooping Version** – The protocol version used for compatibility with other devices on the network. This is the MLD version the switch uses to send snooping reports. (Range: 1-2; Default: 2)
- **Unknown Multicast Mode** – The action for dealing with unknown multicast packets. Options include:
 - **Flood** – Floods any received IPv6 multicast packets that have not been requested by a host to all ports in the VLAN.
 - **To Router Port** – Forwards any received IPv6 multicast packets that have not been requested by a host to ports that are connected to a detected multicast router. (This is the default action.)



4.13.2 Immediate Leave Status

Configure > MLD Snooping > Immediate Leave Status page is used to configure Immediate Leave status for a VLAN.

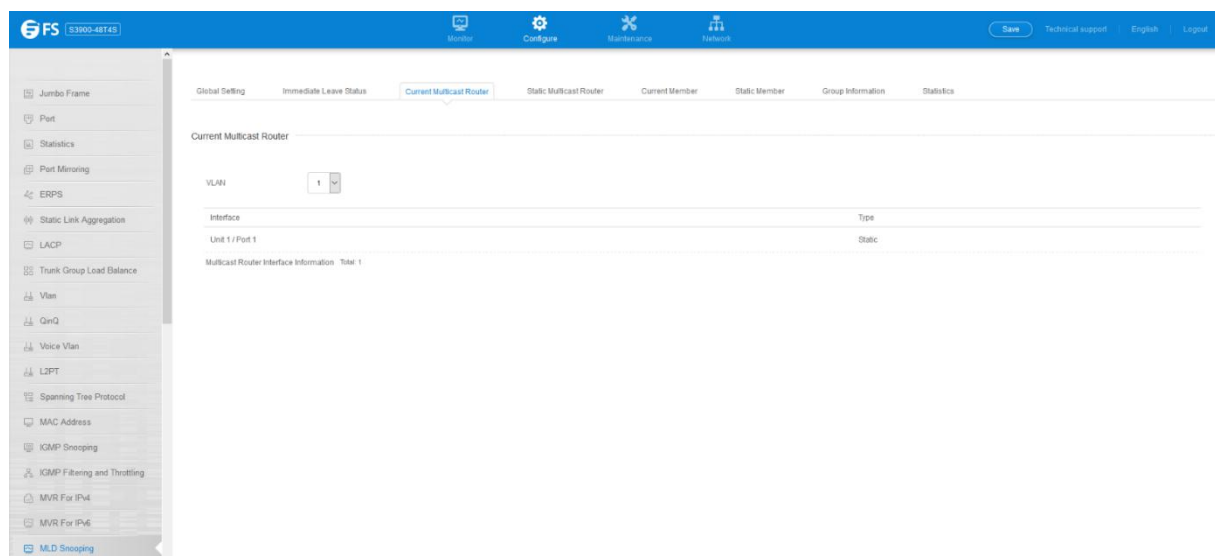
- **VLAN** – A VLAN identification number. (Range: 1-4094)
- **Immediate Leave Status** – Immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled) If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.



4.13.3 Current Multicast Router

Configure > MLD Snooping > Current Multicast Router page is used to statically show an interface to an IPv6 multicast router/switch.

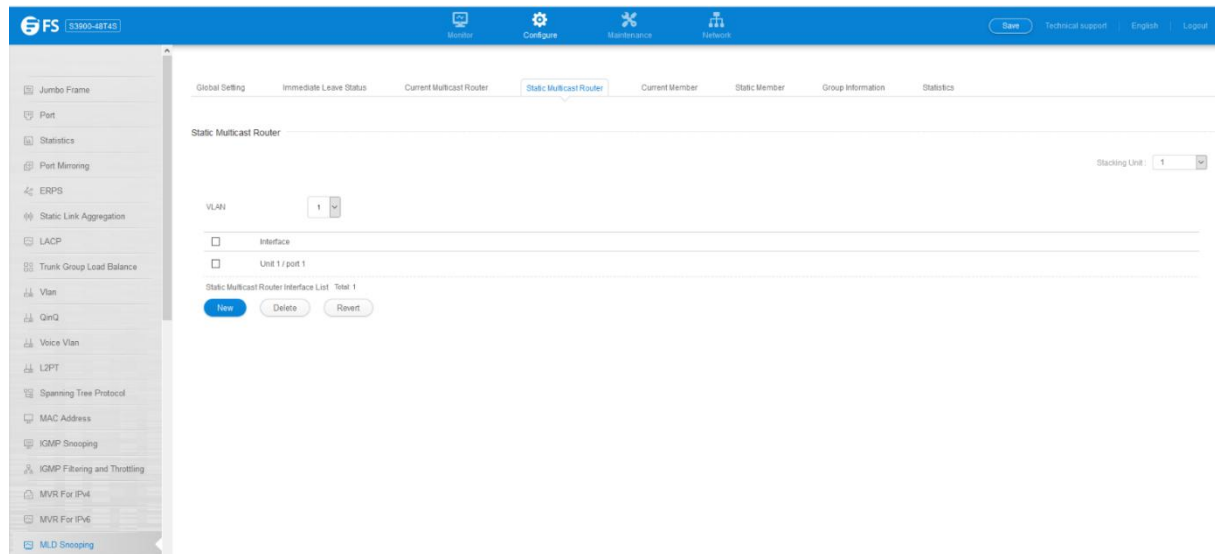
- **VLAN** – Selects the VLAN which is to propagate all IPv6 multicast traffic coming from the attached multicast router. (Range: 1-4094)
- **Interface** – Activates the Port or group scroll down list.



4.13.4 Static Multicast Router

Configure > MLD Snooping > Static Multicast Router page is used to statically add an interface to an IPv6 multicast router/switch.

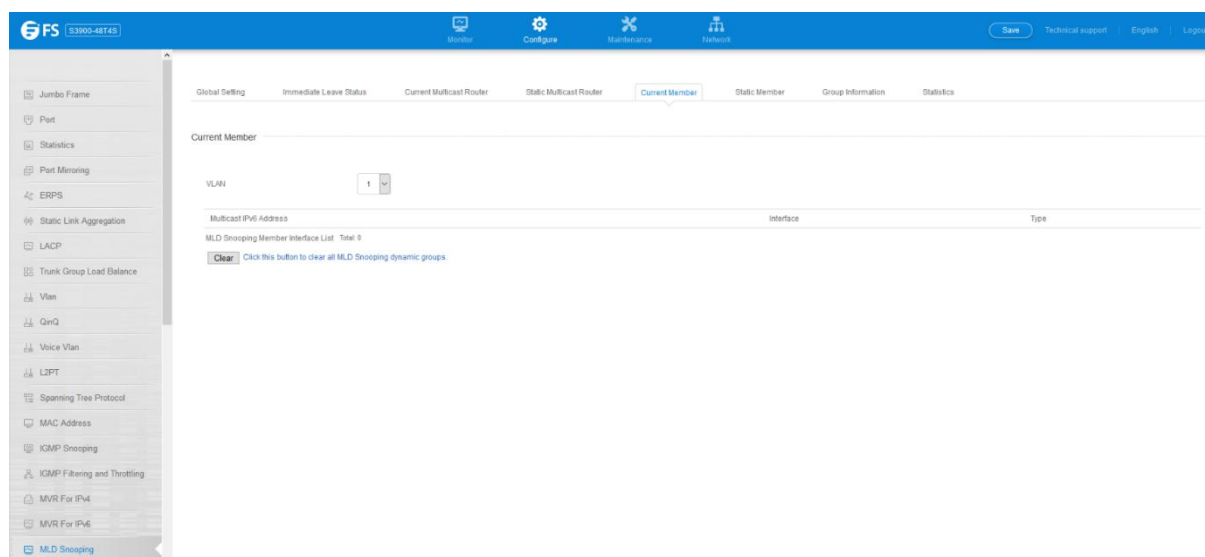
- **VLAN** – Selects the VLAN which is to propagate all IPv6 multicast traffic coming from the attached multicast router. (Range: 1-4094)
- **Interface** – Activates the Port or group scroll down list.



4.13.5 Current Member

Configure > MLD Snooping > Current Member page is used to statically show an IPv6 multicast service to an interface.

- **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- **Multicast IPv6 Address** – The IP address for a specific multicast service.
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port or Group** – Specifies the interface assigned to a multicast group.
- **Type (Show Current Member)** – Shows if this multicast stream was statically configured by the user, discovered by MLD Snooping, or is a data stream to which no other ports are subscribing (i.e., the stream is flooded onto VLAN instead of being trapped to the CPU for processing, or is being processed by MVR6).

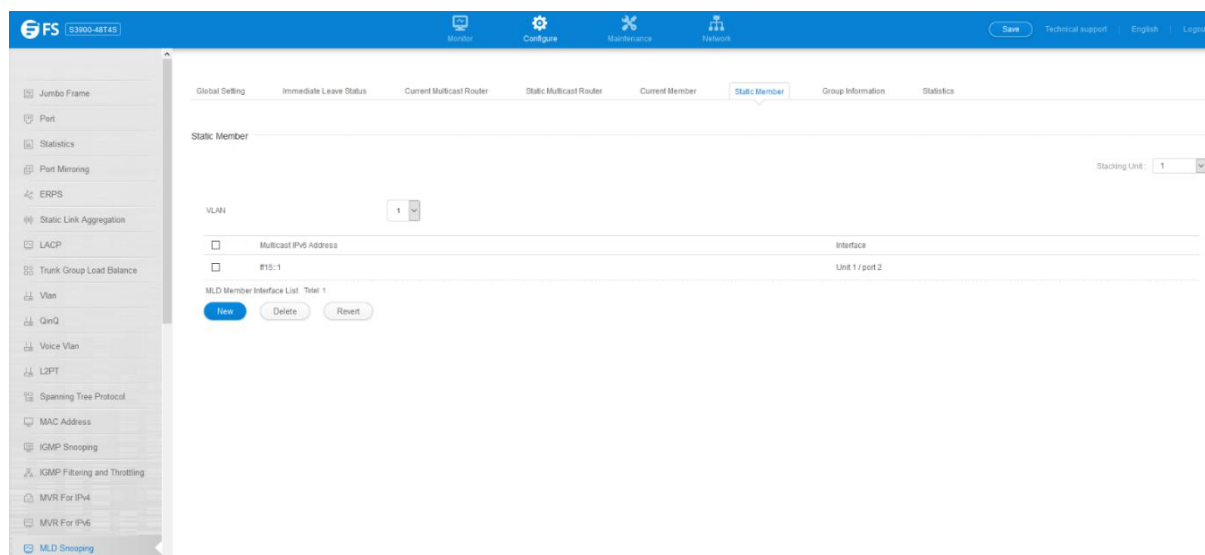


The screenshot shows the 'Current Member' configuration page for MLD Snooping. The left sidebar contains a navigation menu with options like Jumbo Frame, Port, Statistics, Port Mirroring, ERPS, Static Link Aggregation, LACP, Trunk Group Load Balance, Vlan, QinQ, Voice Vlan, L2PT, Spanning Tree Protocol, MAC Address, IGMP Snooping, IGMP Filtering and Throttling, MVR For IPv4, MVR For IPv6, and MLD Snooping. The main content area has tabs for Global Setting, Immediate Leave Status, Current Multicast Router, Static Multicast Router, Current Member (selected), Static Member, Group Information, and Statistics. Under 'Current Member', there is a 'VLAN' dropdown set to '1', a 'Multicast IPv6 Address' field, and an 'Interface' dropdown. Below these is a table titled 'MLD Snooping Member Interface List' with a 'Total: 0' count and a 'Clear' button. A link below the table says 'Click this button to clear all MLD Snooping dynamic groups.'

4.13.6 Static Member

Configure > MLD Snooping > Static Member page is used to statically add an IPv6 multicast service to an interface.

- **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- **Multicast IPv6 Address** – The IP address for a specific multicast service.
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port or Group** – Specifies the interface assigned to a multicast group.
- **Type** (Show Current Member) – Shows if this multicast stream was statically configured by the user, discovered by MLD Snooping, or is a data stream to which no other ports are subscribing (i.e., the stream is flooded onto VLAN instead of being trapped to the CPU for processing, or is being processed by MVR6).



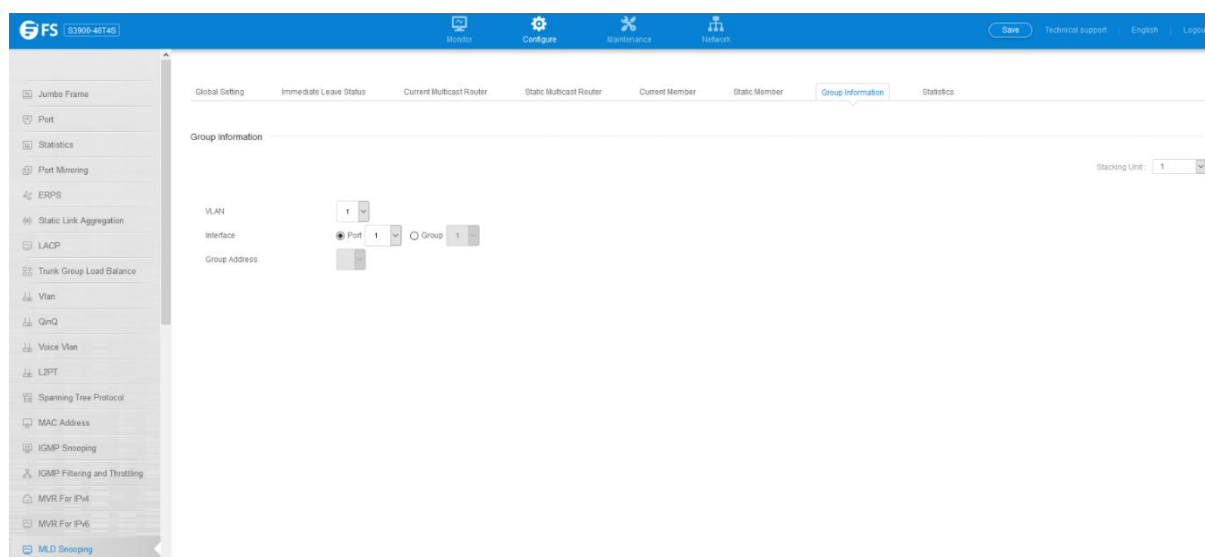
The screenshot shows the 'Static Member' configuration page for MLD Snooping. The left sidebar is the same as the previous screenshot. The main content area has tabs for Global Setting, Immediate Leave Status, Current Multicast Router, Static Multicast Router, Current Member, Static Member (selected), Group Information, and Statistics. Under 'Static Member', there is a 'Stacking Unit' dropdown set to '1'. Below this is a 'VLAN' dropdown set to '1'. There are two rows for configuration: the first row has a checkbox for 'Multicast IPv6 Address' and an 'Interface' dropdown; the second row has a checkbox for 'MIS: 1' and a dropdown set to 'Unit 1 / port 2'. Below these is a table titled 'MLD Member Interface List' with a 'Total: 1' count and buttons for 'New', 'Delete', and 'Revert'.



4.13.7 Group Information

Configure >MLD Snooping >Group Information page is used to display and set known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

- **VLAN** – VLAN identifier. (Range: 1-4094)
- **Interface** – Port or group identifier.
- **Group Address** – The IP address for a specific multicast service.
- **Type** – The means by which each group was learned – MLD Snooping or Multicast Data.
- **Filter Mode** – The filter mode is used to summarize the total listening state of a multicast address to a minimum set such that all nodes' listening states are respected. In Include mode, the router only uses the request list, indicating that the reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the hosts' source-list. In Exclude mode, the router uses both the request list and exclude list, indicating that the reception of packets sent to the given multicast address is requested from all IP source addresses, except for those listed in the exclude source-list and for any other sources where the source timer status has expired.
- **Filter Timer Elapse** – The Filter timer is only used when a specific multicast address is in Exclude mode. It represents the time for the multicast address filter mode to expire and change to Include mode.
- **Request List** – Sources included on the router's request list.
- **Exclude List** – Sources included on the router's exclude list.



4.13.8 Statistics

Configure >MLD Snooping >Statistics pages is used to display MLD Snooping protocol related statistics for the specified interface.

- **Domain ID** – An independent multicast domain. (Range: 1-5)

- **VLAN** – VLAN identifier. (Range: 1-4093)
- **Port** – Port identifier. (Range: 1-28)
- **Group** – group identifier. (Range: 1-12)

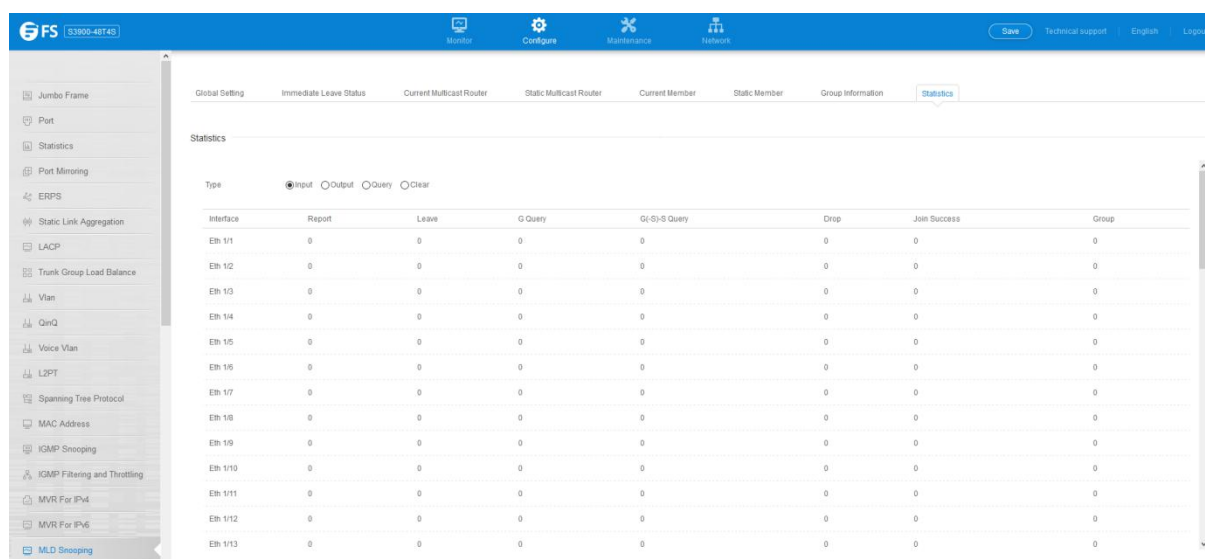
Query Statistics

- **Querier IP Address** – The IP address of the querier on this interface.
- **Querier Expire Time** – The time after which this querier is assumed to have expired.
- **General Query Received** – The number of general queries received on this interface.
- **General Query Sent** – The number of general queries sent from this interface.
- **Specific Query Received** – The number of specific queries received on this interface.
- **Specific Query Sent** – The number of specific queries sent from this interface.
- **Number of Reports Sent** – The number of reports sent from this interface.
- **Number of Leaves Sent** – The number of leaves sent from this interface. VLAN, Port, and group Statistics Input Statistics
- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of MVR groups active on this interface.

Output Statistics

- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of MVR groups active on this interface.

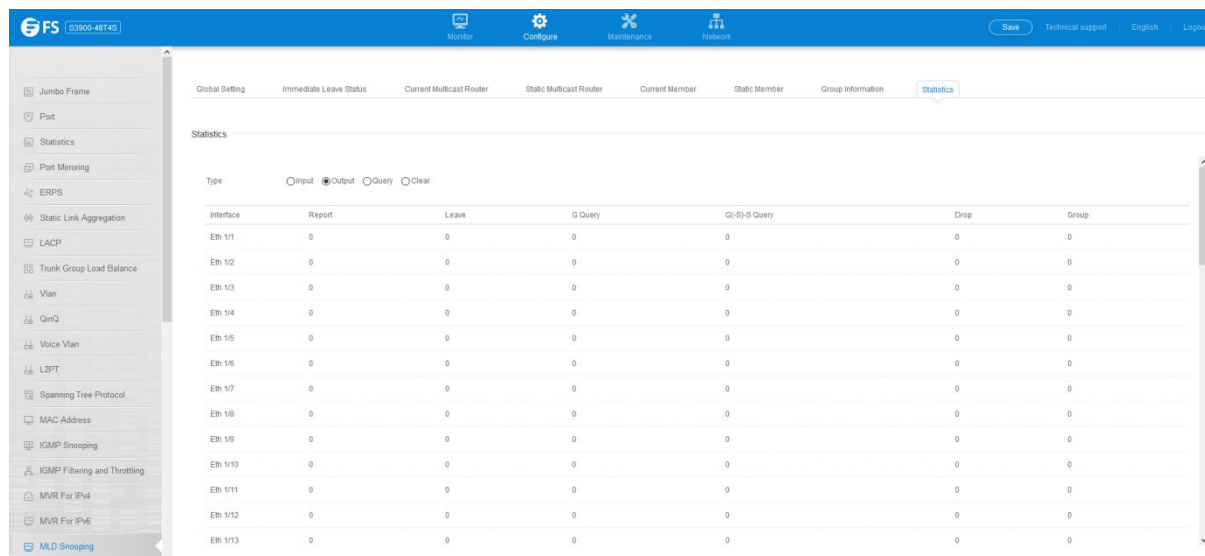
To display statistics for MLD Snooping input:



The screenshot shows the FS S3900-48T4S web management interface. The left sidebar contains a navigation menu with options like Jumbo Frame, Port, Statistics, Port Mirroring, ERPS, Static Link Aggregation, LACP, Trunk Group Load Balance, Vlan, QinQ, Voice Vlan, LPT, Spanning Tree Protocol, MAC Address, IGMP Snooping, IGMP Filtering and Throttling, MVR For IPv4, MVR For IPv6, and MLD Snooping. The main content area is titled 'Statistics' and displays a table of statistics for MLD Snooping input. The table has columns for Interface, Report, Leave, G Query, G(-S)-S Query, Drop, Join Success, and Group. The data is filtered by Type: Input. The table shows statistics for interfaces Eth 1/1 through Eth 1/13, all with values of 0.

Interface	Report	Leave	G Query	G(-S)-S Query	Drop	Join Success	Group
Eth 1/1	0	0	0	0	0	0	0
Eth 1/2	0	0	0	0	0	0	0
Eth 1/3	0	0	0	0	0	0	0
Eth 1/4	0	0	0	0	0	0	0
Eth 1/5	0	0	0	0	0	0	0
Eth 1/6	0	0	0	0	0	0	0
Eth 1/7	0	0	0	0	0	0	0
Eth 1/8	0	0	0	0	0	0	0
Eth 1/9	0	0	0	0	0	0	0
Eth 1/10	0	0	0	0	0	0	0
Eth 1/11	0	0	0	0	0	0	0
Eth 1/12	0	0	0	0	0	0	0
Eth 1/13	0	0	0	0	0	0	0

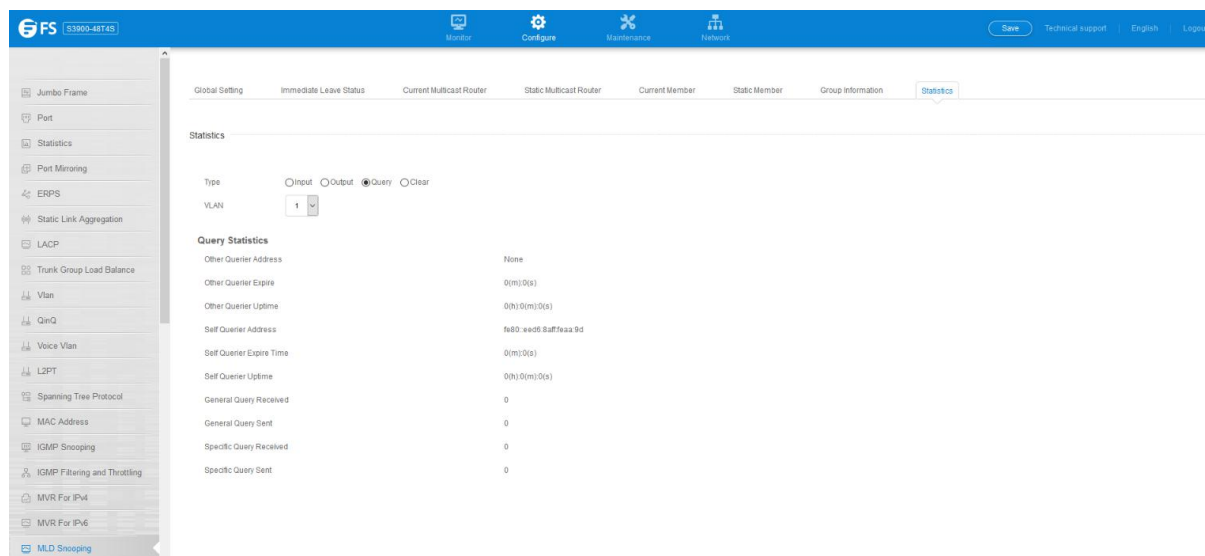
To display statistics for MLD Snooping output:



The screenshot shows the FS S3900-48T4S web management interface. The left sidebar contains a menu with various configuration options, including Jumbo Frame, Port, Statistics, Port Mirroring, ERPS, Static Link Aggregation, LACP, Trunk Group Load Balance, Vlan, QinQ, Voice Vlan, L2PT, Spanning Tree Protocol, MAC Address, IGMP Snooping, IGMP Filtering and Throttling, MVR For IPv4, MVR For IPv6, and MLD Snooping. The main content area is titled 'Statistics' and displays a table of MLD Snooping output statistics. The table has columns for Interface, Report, Leave, G Query, G:G-S Query, Drop, and Group. The data shows zero values for all metrics across all interfaces (Eth 1/1 to Eth 1/13).

Interface	Report	Leave	G Query	G:G-S Query	Drop	Group
Eth 1/1	0	0	0	0	0	0
Eth 1/2	0	0	0	0	0	0
Eth 1/3	0	0	0	0	0	0
Eth 1/4	0	0	0	0	0	0
Eth 1/5	0	0	0	0	0	0
Eth 1/6	0	0	0	0	0	0
Eth 1/7	0	0	0	0	0	0
Eth 1/8	0	0	0	0	0	0
Eth 1/9	0	0	0	0	0	0
Eth 1/10	0	0	0	0	0	0
Eth 1/11	0	0	0	0	0	0
Eth 1/12	0	0	0	0	0	0
Eth 1/13	0	0	0	0	0	0

To display statistics for MLD Snooping Query:



The screenshot shows the FS S3900-48T4S web management interface. The left sidebar contains a menu with various configuration options, including Jumbo Frame, Port, Statistics, Port Mirroring, ERPS, Static Link Aggregation, LACP, Trunk Group Load Balance, Vlan, QinQ, Voice Vlan, L2PT, Spanning Tree Protocol, MAC Address, IGMP Snooping, IGMP Filtering and Throttling, MVR For IPv4, MVR For IPv6, and MLD Snooping. The main content area is titled 'Statistics' and displays a table of MLD Snooping Query statistics. The table has columns for Other Querier Address, Other Querier Expire, Other Querier Uptime, Self Querier Address, Self Querier Expire Time, Self Querier Uptime, General Query Received, General Query Sent, Specific Query Received, and Specific Query Sent. The data shows zero values for all metrics across all interfaces (Eth 1/1 to Eth 1/13).

Other Querier Address	Other Querier Expire	Other Querier Uptime	Self Querier Address	Self Querier Expire Time	Self Querier Uptime	General Query Received	General Query Sent	Specific Query Received	Specific Query Sent
None	0(m)(0s)	0(h)(0(m)(0s)	fe80::e005:5aff:feaa:9d	0(m)(0s)	0(h)(0(m)(0s)	0	0	0	0

4.14 MVR For IPv4

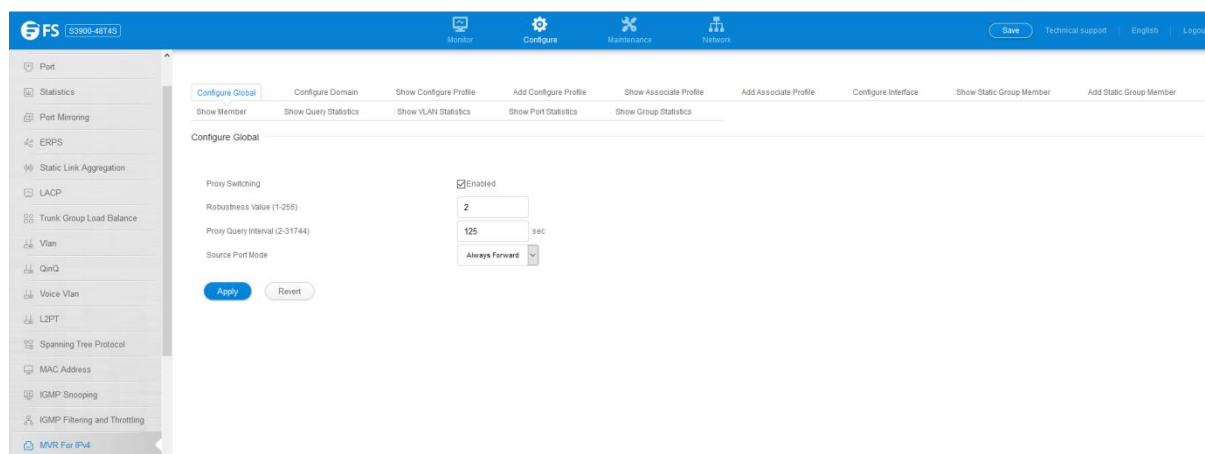
4.14.1 Configure Global

Configure >MVR For IPv4 >Configure Global page is used to configure proxy switching and the robustness variable.

- **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)
 - When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
 - Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be

configured on all downstream interfaces which require MVR proxy service.

- When the source port receives report and leave messages, it only forwards them to other source ports.
- When receiver ports receive any query messages, they are dropped.
- When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- When MVR proxy switching is disabled:
 - Any membership reports received from receiver/source ports are forwarded to all source ports.
 - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
 - When a receiver port receives a query message, it will be dropped.
- **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-255; Default: 2)
 - This parameter is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
 - This parameter only takes effect when MVR proxy switching is enabled.
- **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)
 - This parameter sets the general query interval at which active receiver ports send out general queries.
 - This interval is only effective when proxy switching is enabled.
- **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only forward multicast streams which the source port has dynamically joined.
 - **Always Forward** – By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
 - **Dynamic** – When dynamic mode is enabled, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.



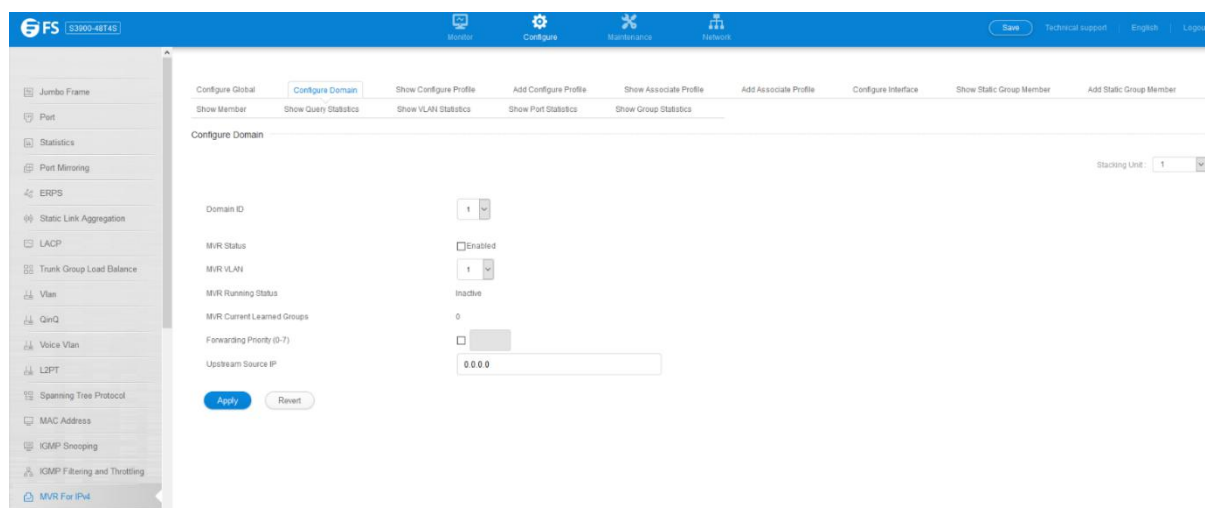
4.14.2 Configure Domain

Configure > MVR For IPv4 > Configure Domain page is used to enable MVR globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **MVR Status** – When MVR is enabled on the switch, any multicast data associated with an MVR group is sent from all designated

source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)

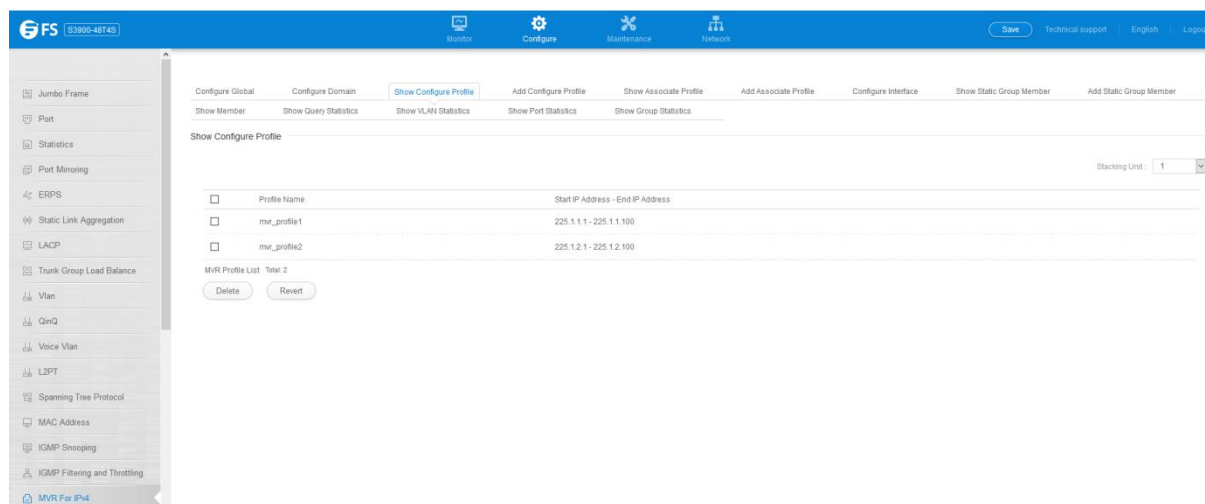
- **MVR VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR. MVR source ports should be configured as members of the MVR VLAN (see ["Adding Static Members to VLANs"](#)), but MVR receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- **MVR Running Status** – Indicates whether or not all necessary conditions in the MVR environment are satisfied. Running status is Active as long as MVR is enabled, the specified MVR VLAN exists, and a source port with a valid link has been configured (see ["Configuring MVR Interface Status"](#)).
- **MVR Current Learned Groups** – The number of MVR groups currently assigned to this domain.
- **Forwarding Priority** – The CoS priority assigned to all multicast traffic forwarded into this domain. (Range: 0-6, where 6 is the highest priority) This parameter can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.
- **Upstream Source IP** – The source IP address assigned to all MVR control packets sent upstream on the specified domain. By default, all MVR reports sent upstream use a null source IP address.



4.14.3 Show Configure Profile

Configure >MVR For IPv4 >Show Configure Profile page is used to display the multicast group address for required services to one or more MVR domains.

- **Profile Name** – The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
- **Start IP Address** – Starting IP address for an MVR multicast group.(Range: 224.0.1.0 - 239.255.255.255)
- **End IP Address** – Ending IP address for an MVR multicast group.(Range: 224.0.1.0 - 239.255.255.255)

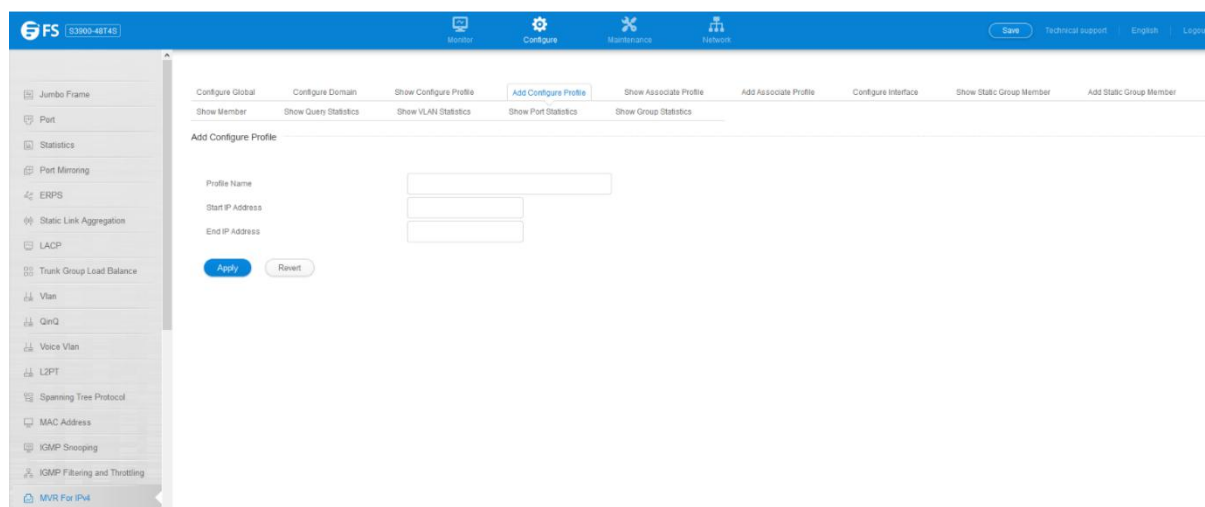


4.14.4 Add Configure Profile

Configure >MVR For IPv4 >Add Configure Profile page is used to assign the multicast group address for required services to one or more MVR domains.

- **Profile Name** – The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
- **Start IP Address** – Starting IP address for an MVR multicast group.(Range: 224.0.1.0 - 239.255.255.255)
- **End IP Address** – Ending IP address for an MVR multicast group.(Range: 224.0.1.0 - 239.255.255.255)

Associate Profile(Range: 1-21 characters)



4.14.5 Show Associate Profile

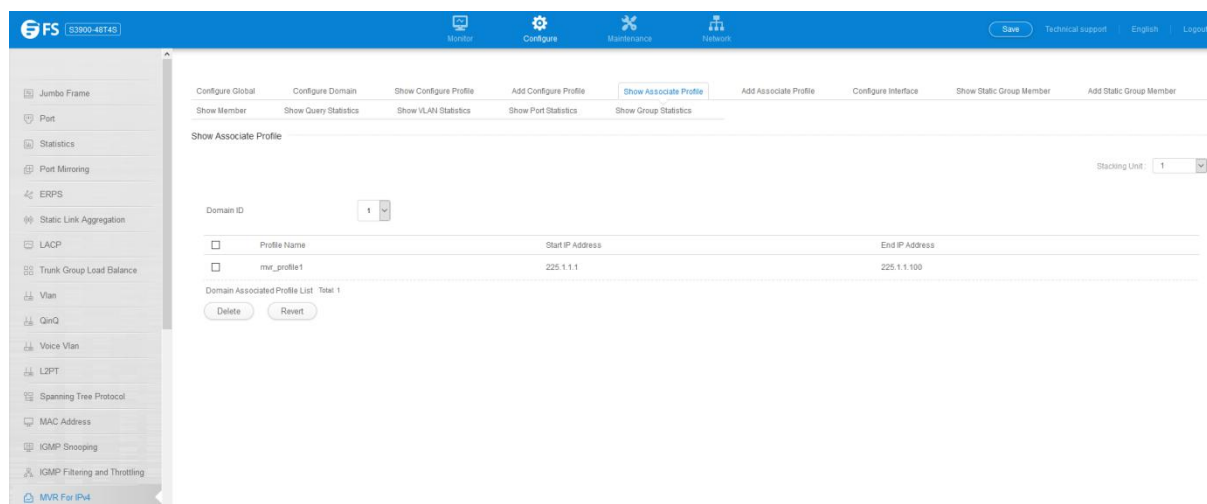
Configure >MVR For IPv4 >Show Associate Profile pages is used to show the multicast group address for required services to one or more MVR domains.

- **Profile Name** – The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
- **Start IP Address** – Starting IP address for an MVR multicast group.(Range: 224.0.1.0 - 239.255.255.255)
- **End IP Address** – Ending IP address for an MVR multicast group.(Range: 224.0.1.0 - 239.255.255.255)

Associate Profile

- **Domain ID** – An independent multicast domain. (Range: 1-5)

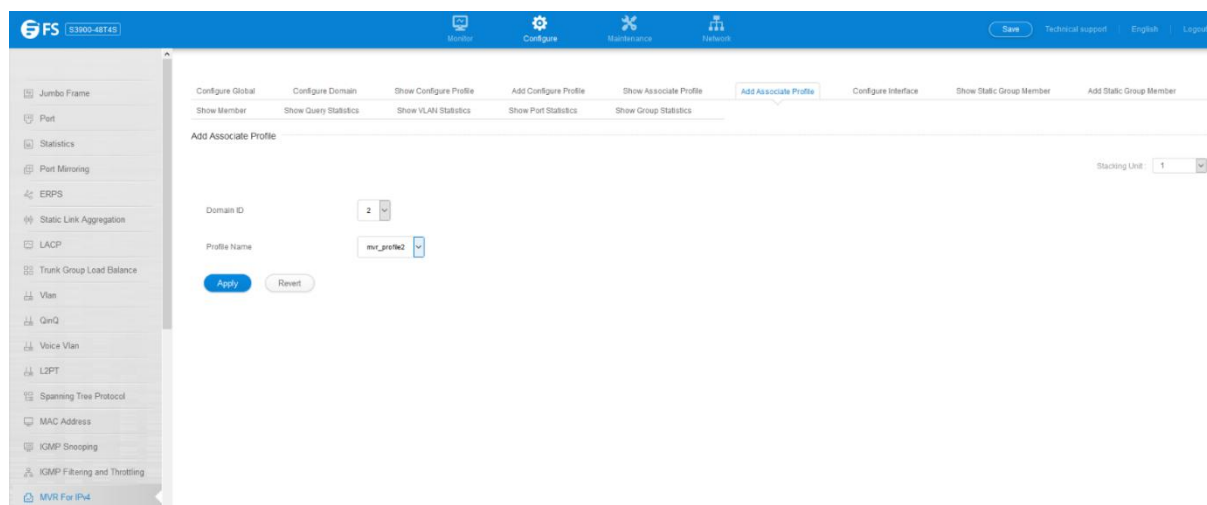
To show the MVR group address profiles assigned to a domain:



4.14.6 Add Associate Profile

Configure >MVR For IPv4 >Add Associate Profile page is used to assign the multicast group address for required services to one or more MVR domains.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Profile Name** – The name of a profile to be assigned to this domain.(Range: 1-21 characters)



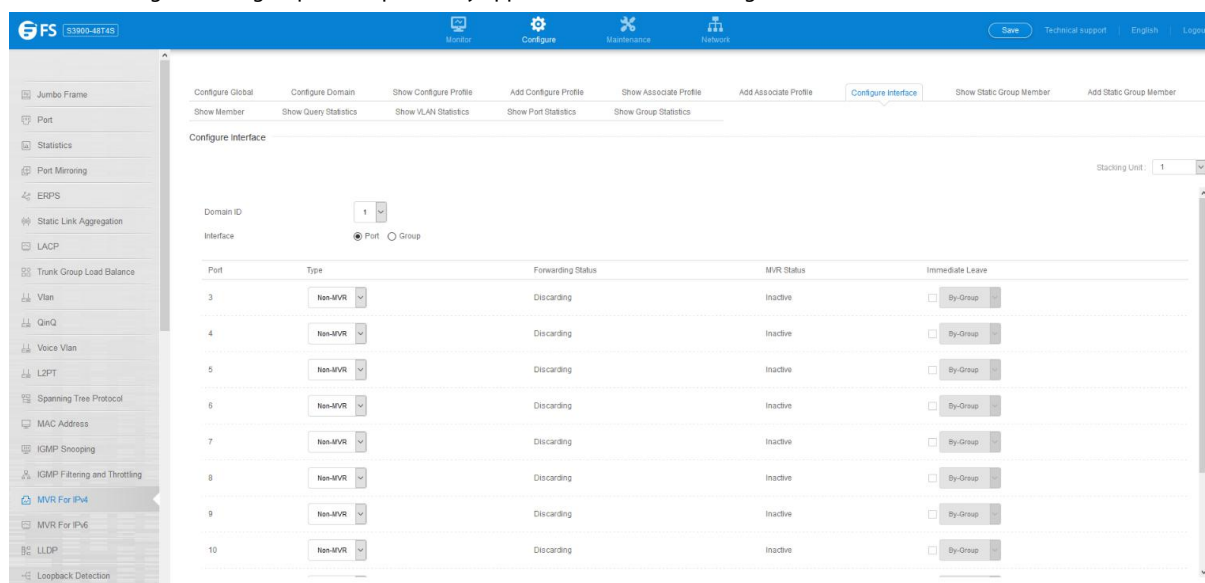
4.14.7 Configure Interface

Configure >MVR For IPv4 >Configure Interface page is used to configure each interface that participates in the MVR protocol as a source port or receiver port.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Port/Group** – Interface identifier.
- **Type** – The following interface types are supported:
 - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN. Note that the source port must be manually configured as a member of the MVR VLAN.
 - **Receiver** – A subscriber port that can receive multicast data sent through the MVR VLAN. Any port configured as an

receiver port will be dynamically added to the MVR VLAN when it forwards an IGMP report or join message from an attached host requesting any of the designated multicast services supported by the MVR VLAN. Just remember that only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned.

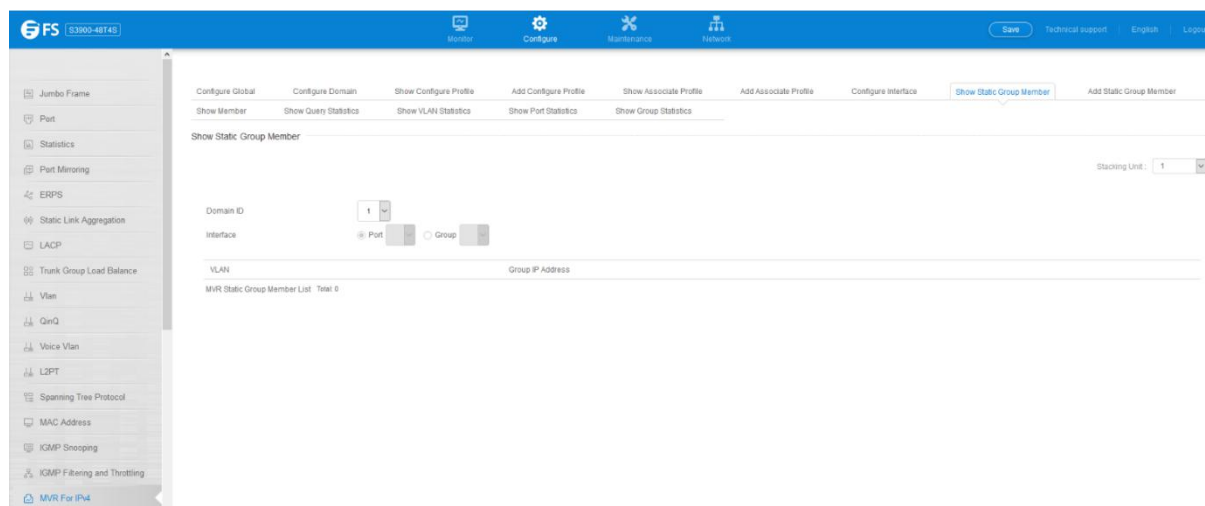
- **Non-MVR** – An interface that does not participate in the MVR VLAN. (This is the default type.)
- **Forwarding Status** – Shows if MVR traffic is being forwarded or discarded.
- **MVR Status** – Shows the MVR status. MVR status for source ports is “Active” if MVR is globally enabled on the switch. MVR status for receiver ports is “Active” only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.
- **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR receiver.)



4.14.8 Show Static Group Member

Configure > MVR For IPv4 > Show Static Group Member page is used to show static multicast groups for a port or trunk which will receive long-term multicast streams associated with a stable set of hosts.

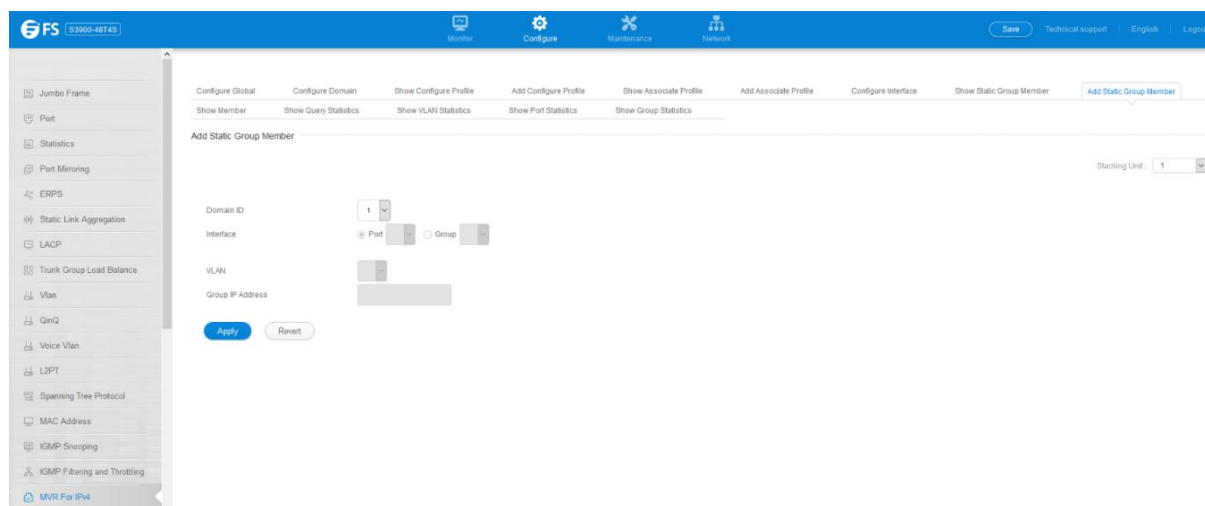
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Interface** – Port or group identifier.
- **VLAN** – VLAN identifier. (Range: 1-4093)
- **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.



4.14.9 Add Static Group Member

Configure >MVR For IPv4 > Add Static Group Member page is used to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Interface** – Port or group identifier.
- **VLAN** – VLAN identifier. (Range: 1-4093)
- **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.

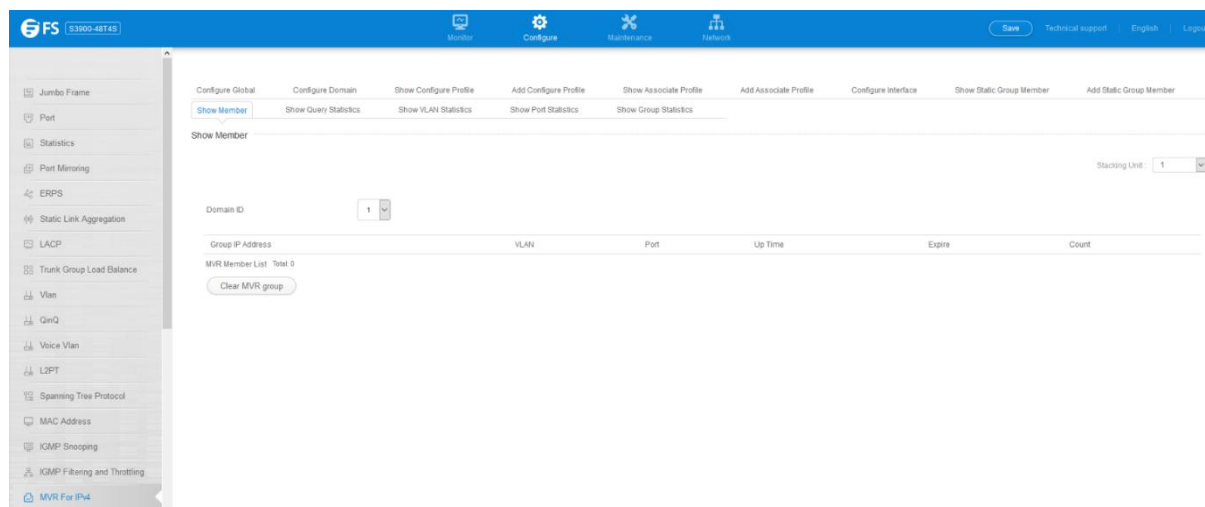


4.14.10 Show Member

Configure >MVR For IPv4 > Show Member page is used to show the multicast groups either statically or dynamically assigned to the MVR receiver groups on each interface.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Group IP Address** – Multicast groups assigned to the MVR VLAN.
- **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR VLAN if the group address has been statically assigned.

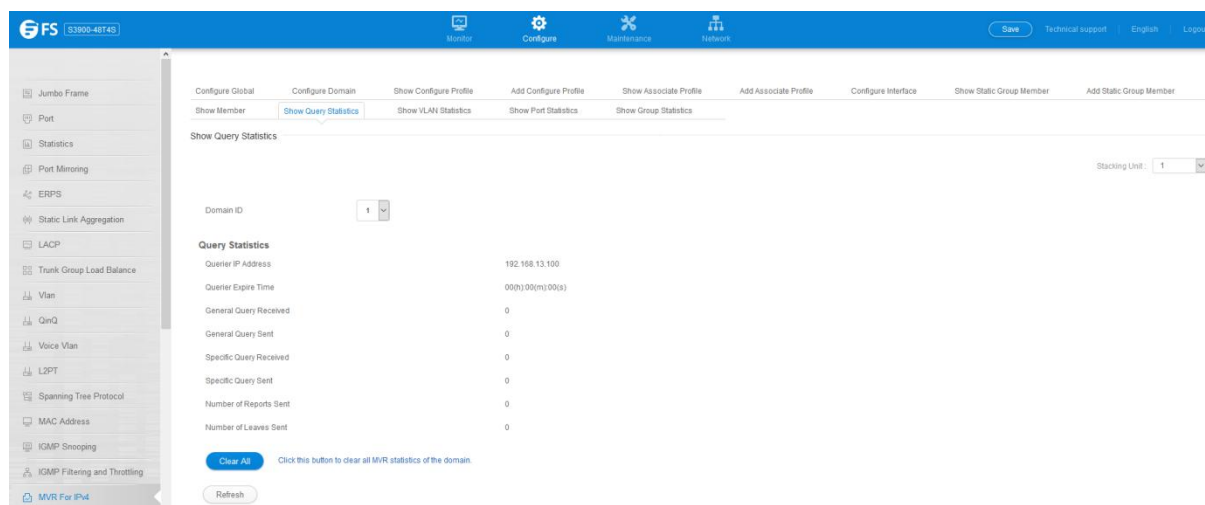
- **Port** – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN.
- **Up Time** – Time this service has been forwarded to attached clients.
- **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.
- **Count** – The number of multicast services currently being forwarded from the MVR VLAN.



4.14.11 Show Query Statistics

Configure > MVR For IPv4 > Show Query Statistics page is used to display MVR protocol related query statistics for the specified domain.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Querier IP Address** – The IP address of the querier on this interface.
- **Querier Expire Time** – The time after which this querier is assumed to have expired.
- **General Query Received** – The number of general queries received on this interface.
- **General Query Sent** – The number of general queries sent from this interface.
- **Specific Query Received** – The number of specific queries received on this interface.
- **Specific Query Sent** – The number of specific queries sent from this interface.
- **Number of Reports Sent** – The number of reports sent from this interface.
- **Number of Leaves Sent** – The number of leaves sent from this interface.



4.14.12 Show VLAN Statistics

Configure >MVR For IPv4 >Show VLAN Statistics page is used to display MVR protocol related statistics for the specified VLAN.

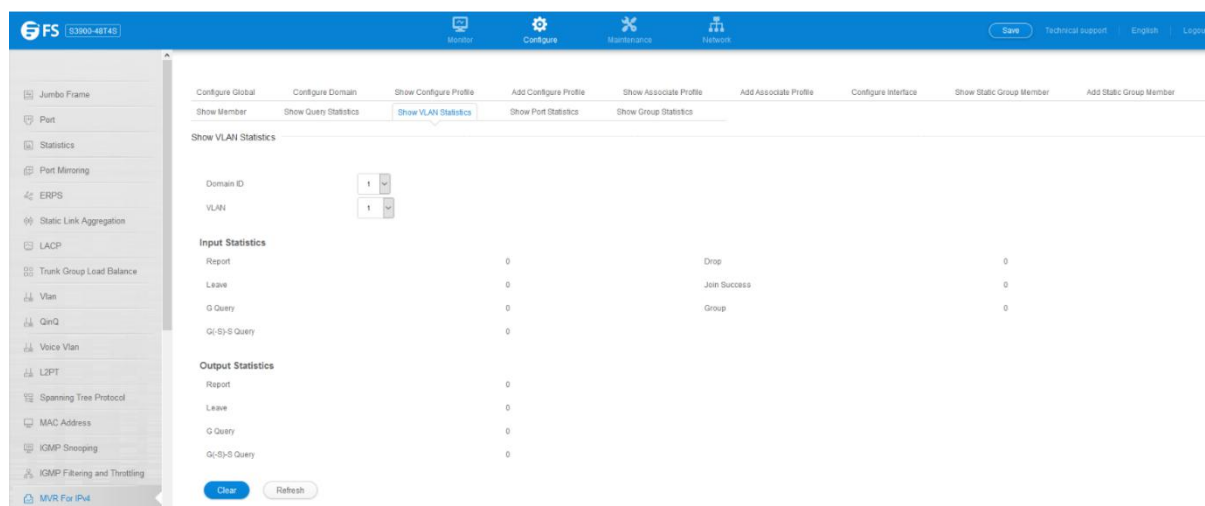
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **VLAN** – VLAN identifier. (Range: 1-4093)

Input Statistics

- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of MVR groups active on this interface.

Output Statistics

- **Report** – The number of IGMP membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.



4.14.13 Show Port Statistics

Configure >MVR For IPv4 >Show Port Statistics page is used to display MVR protocol related statistics for the specified interface.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Port** – Port identifier. (Range: 1-28)

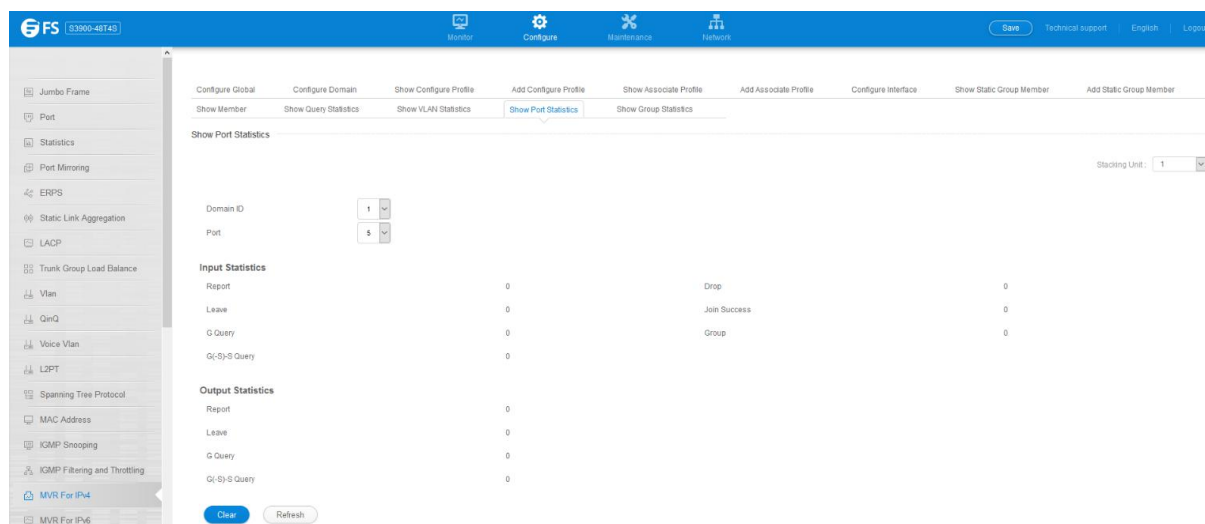
Input Statistics

- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.

- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of MVR groups active on this interface.

Output Statistics

- **Report** – The number of IGMP membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.



4.14.14 Show Group Statistics

Configure >MVR For IPv4 >Show Group Statistics page is used to display MVR protocol related statistics for the specified trunk group.

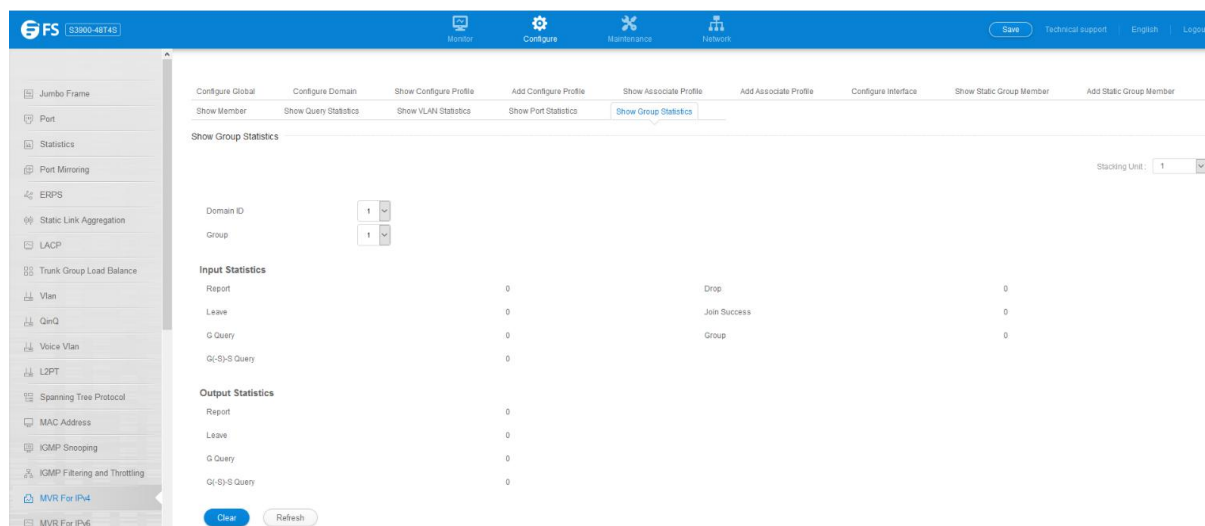
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Group** – Group identifier. (Range: 1-12)

Input Statistics

- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of MVR groups active on this interface.

Output Statistics

- **Report** – The number of IGMP membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.



4.15 MVR For IPv6

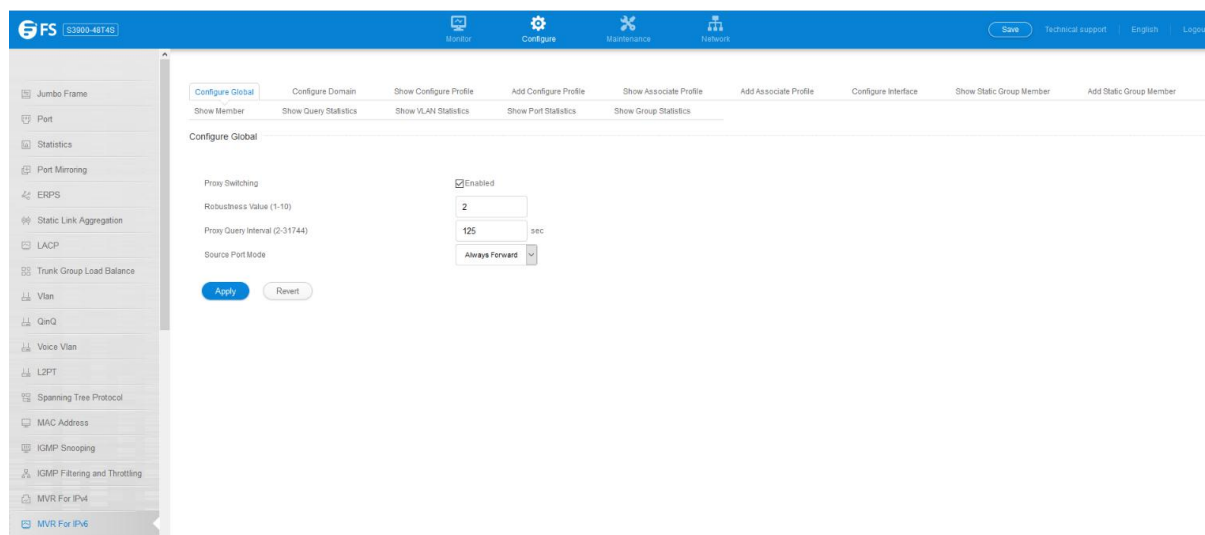
4.15.1 Configure Global

Configure > MVR For IPv6 > Configure Global page is used to configure proxy switching and the robustness variable.

- **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)
 - When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
 - Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
 - When the source port receives report and leave messages, it only forwards them to other source ports.
 - When receiver ports receive any query messages, they are dropped.
 - When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
 - When MVR proxy switching is disabled: Any membership reports received from receiver/source ports are forwarded to all source ports.
 - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
 - When a receiver port receives a query message, it will be dropped.
- **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-10; Default: 2)
 - This parameter is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
 - This parameter only takes effect when MVR6 proxy switching is enabled.
- **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)
 - This parameter sets the general query interval at which active receiver ports send out general queries.
 - This interval is only effective when proxy switching is enabled.
- **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only

forward multicast streams which the source port has dynamically joined.

- **Always Forward** – By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
- **Dynamic** – When dynamic mode is enabled, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.



4.15.2 Configure Domain

Configure >MVR For IPv6 >Configure Domain page is used to enable MVR6 globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.

- **Domain ID**– An independent multicast domain. (Range: 1-5)
- **MVR6 Status** – When MVR6 is enabled on the switch, any multicast data associated with an MVR6 group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- **MVR6 VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR6. MVR6 source ports should be configured as members of the MVR6 VLAN, but MVR6 receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- **MVR6 Running Status** – Indicates whether or not all necessary conditions in the MVR6 environment are satisfied. Running status is Active as long as MVR6 is enabled, the specified MVR6 VLAN exists, and a source port with a valid link has been configured.
- **MVR6 Current Learned Groups** – The number of MVR6 groups currently assigned to this domain.
- **Upstream Source IPv6** – The source IPv6 address assigned to all MVR6 control packets sent upstream on the specified domain. This parameter must be a full IPv6 address including the network prefix and host address bits. By default, all MVR6 reports sent upstream use a null source IP address.

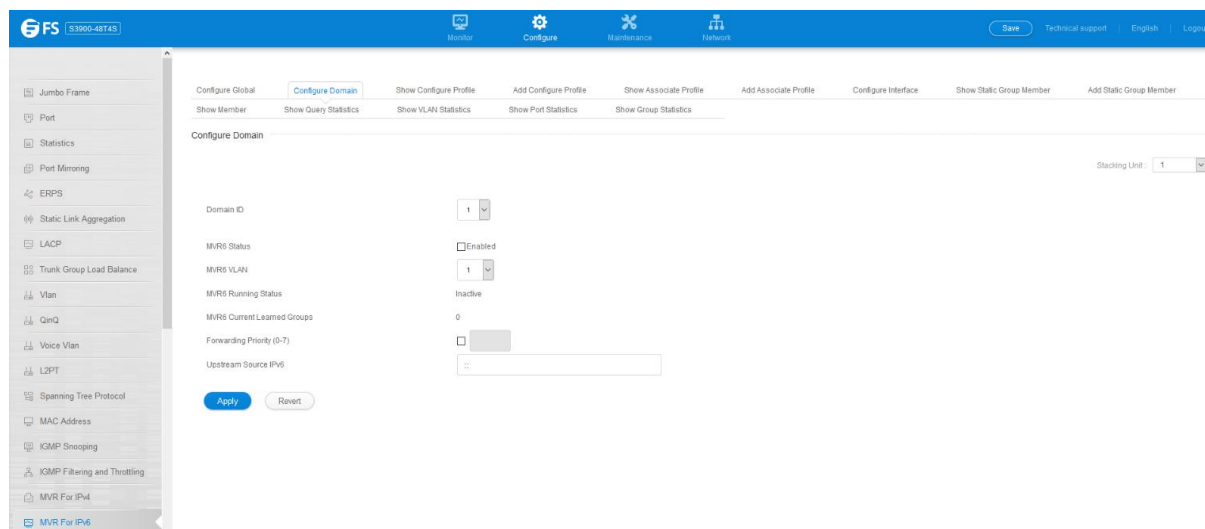
All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

To configure settings for an MVR6 domain:

1. Click Configure >MVR For IPv6 >Configure Domain.
2. Select a domain from the scroll-down list.
3. Enable MVR6 for the selected domain, select the MVR6 VLAN, set the forwarding priority to be assigned to all ingress multicast traffic,

and set the source IP address for all control packets sent upstream as required.

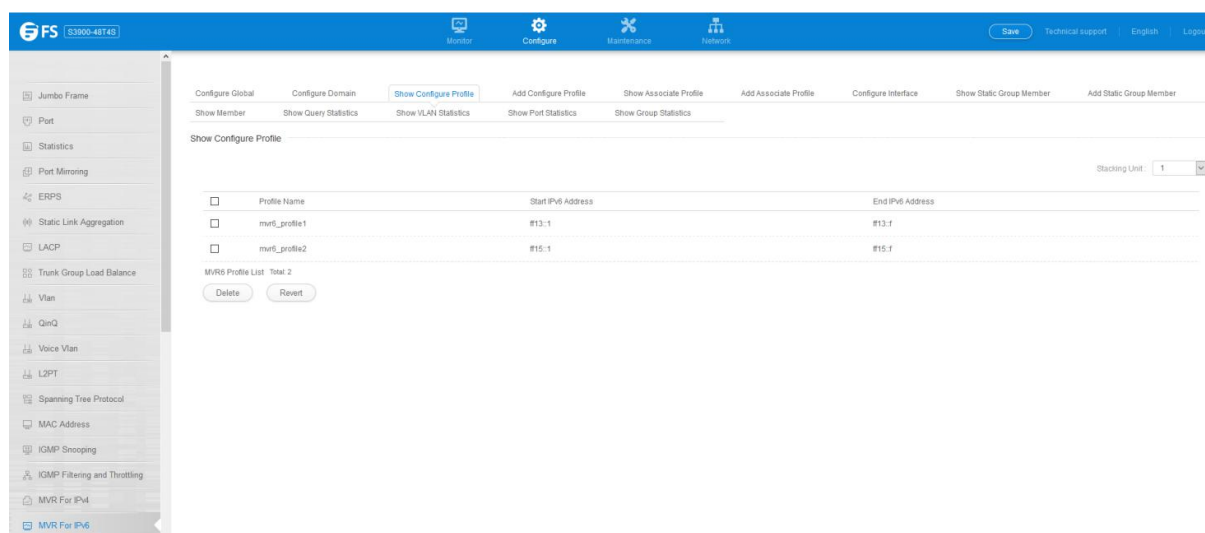
4. Click Apply.



4.15.3 Show Configure Profile

Configure >MVR For IPv6 >Show Configure Profile page is used to assign the multicast group address for required services to one or more MVR6 domains.

- **Profile Name** – The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)
- **Start IPv6 Address** – Starting IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.
- **End IPv6 Address** – Ending IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

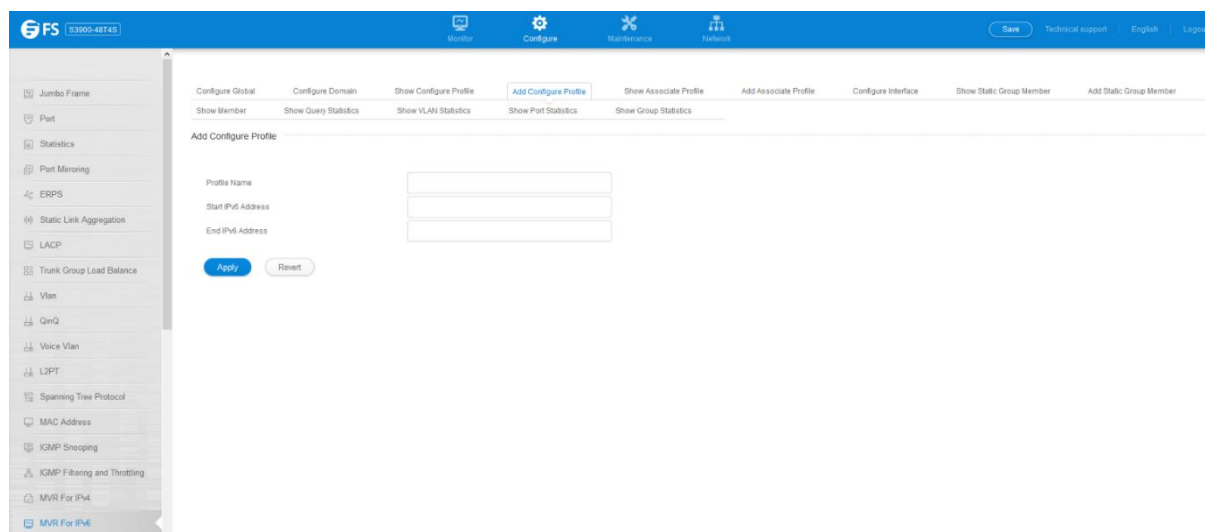


4.15.4 Add Configure Profile

Configure >MVR For IPv6 >Add Configure Profile page is used to assign the multicast group address for required services to one or more MVR6 domains.

- **Profile Name** – The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)

- **Start IPv6 Address** – Starting IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.
- **End IPv6 Address** – Ending IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

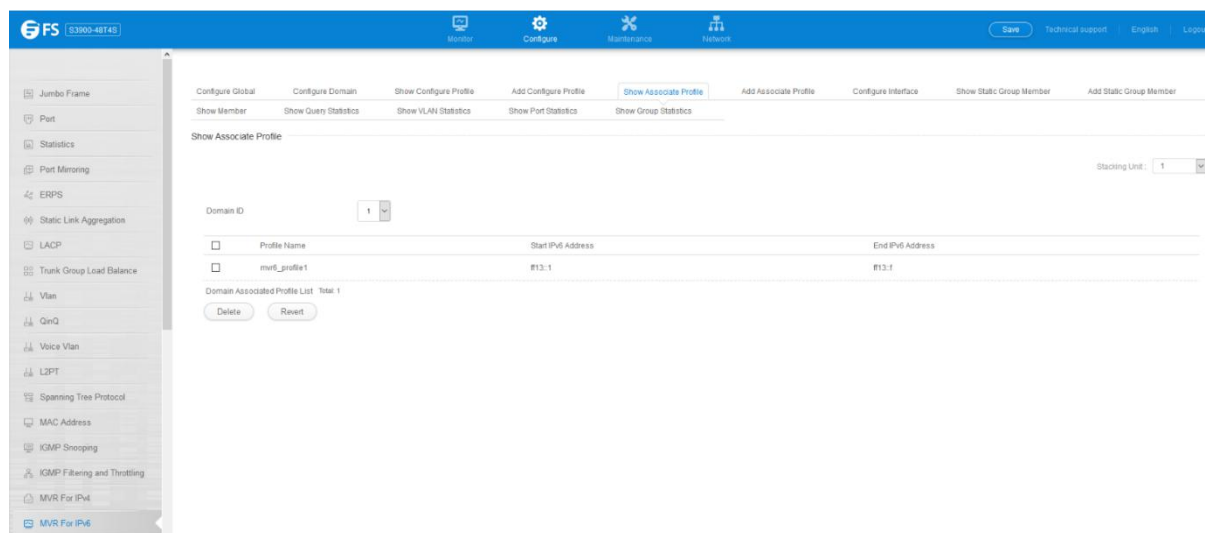


The screenshot shows the 'Add Configure Profile' page. The left sidebar contains a navigation menu with options like Jumbo Frame, Port, Statistics, Port Mirroring, ERPS, Static Link Aggregation, LACP, Trunk Group Load Balance, Vlan, QinQ, Voice Vlan, LLPT, Spanning Tree Protocol, MAC Address, IGMP Snooping, IGMP Filtering and Throttling, MVR For IPv4, and MVR For IPv6. The main content area has tabs for 'Add Configure Profile', 'Show Associate Profile', 'Add Associate Profile', 'Configure Interface', 'Show Static Group Member', and 'Add Static Group Member'. The 'Add Configure Profile' tab is active, showing input fields for 'Profile Name', 'Start IPv6 Address', and 'End IPv6 Address', along with 'Apply' and 'Revert' buttons.

4.15.5 Show Associate Profile

Configure >MVR For IPv6 >Show Associate Profile page is used to show the multicast group address for required services to one or more MVR6 domains.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Profile Name** – The name of a profile to be assigned to this domain.(Range: 1-20 characters)

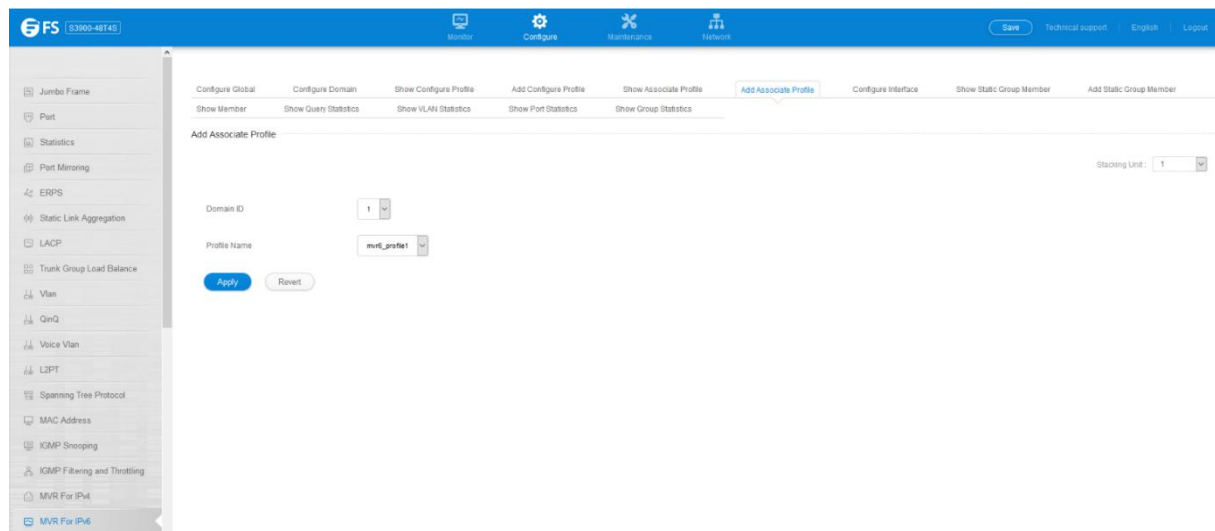


The screenshot shows the 'Show Associate Profile' page. The left sidebar is the same as in the previous screenshot. The main content area has tabs for 'Add Configure Profile', 'Show Associate Profile', 'Add Associate Profile', 'Configure Interface', 'Show Static Group Member', and 'Add Static Group Member'. The 'Show Associate Profile' tab is active. It shows a 'Domain ID' dropdown set to 1 and a 'Stacking Unit' dropdown set to 1. Below these, there is a table with columns for 'Profile Name', 'Start IPv6 Address', and 'End IPv6 Address'. The table contains one entry: 'mvr6_profile1' with 'ff13::1' for both Start and End IPv6 Address. Below the table, it says 'Domain Associated Profile List Total: 1' and has 'Delete' and 'Revert' buttons.

4.15.6 Add Associate Profile

Configure >MVR For IPv6 >Add Associate Profile page is used to assign the multicast group address for required services to one or more MVR6 domains.

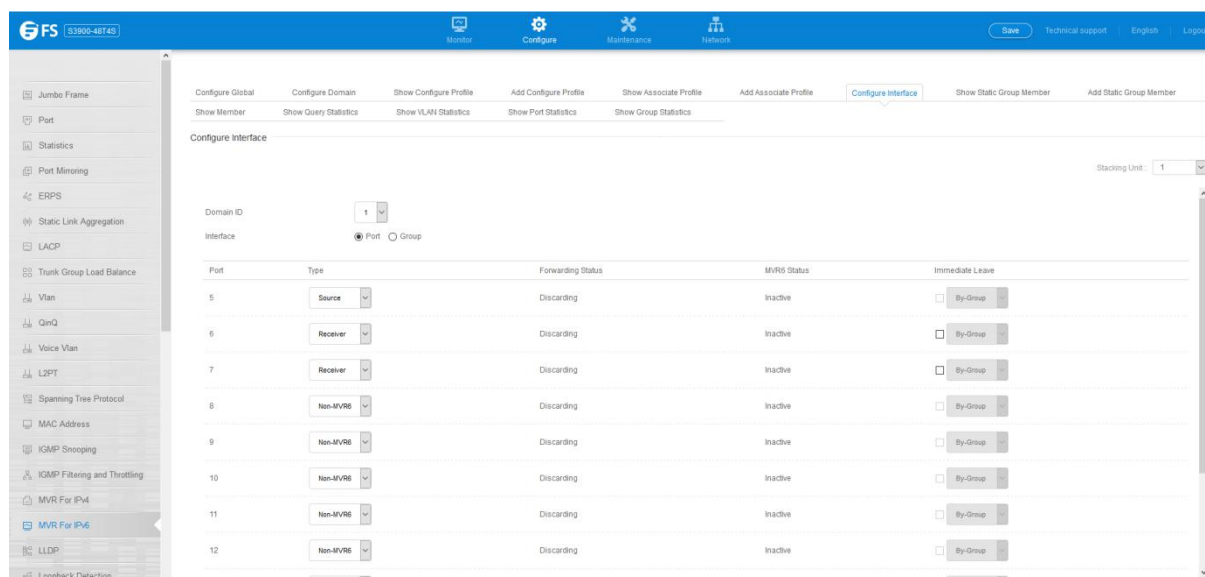
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Profile Name** – The name of a profile to be assigned to this domain.(Range: 1-20 characters)



4.15.7 Configure Interface

Configure >MVR For IPv6 >Configure Interface page is used to configure each interface that participates in the MVR6 protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

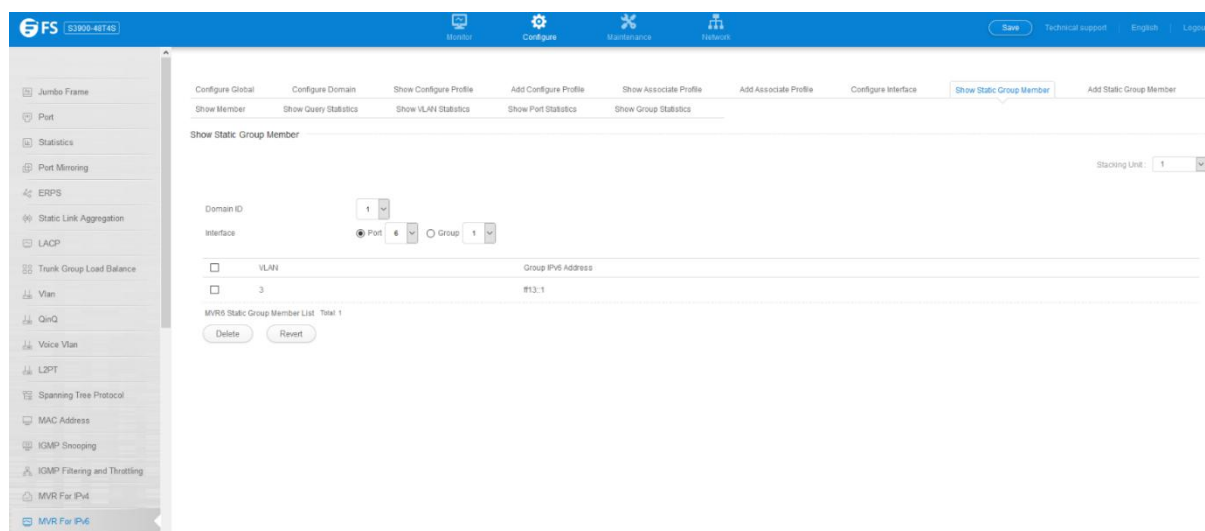
- **Domain ID** – An independent multicast domain. (Range: 1-5)\
- **Port/Group** – Interface identifier.
- **Type** – The following interface types are supported:
 - **Non-MVR6** – An interface that does not participate in the MVR6 VLAN. (This is the default type.)
 - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR6 VLAN. Note that the source port must be manually configured as a member of the MVR6 VLAN.
 - **Receiver** – A subscriber port that can receive multicast data sent through the MVR6 VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode.
- **Forwarding Status** – Shows if multicast traffic is being forwarded or blocked.
- **MVR6 Status** – Shows the MVR6 status. MVR6 status for source ports is “Active” if MVR6 is globally enabled on the switch. MVR6 status for receiver ports is “Active” only if there are subscribers receiving multicast traffic from one of the MVR6 groups, or a multicast group has been statically assigned to an interface.
- **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR6 receiver.)



4.15.8 Show Static Group Member

Configure >MVR For IPv6 >Show Static Group Member page is used to show static bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Interface** – Port or group identifier.
- **VLAN** – VLAN identifier. (Range: 1-4093)
- **Group IPv6 Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR6 group range configured on the Configure General page.

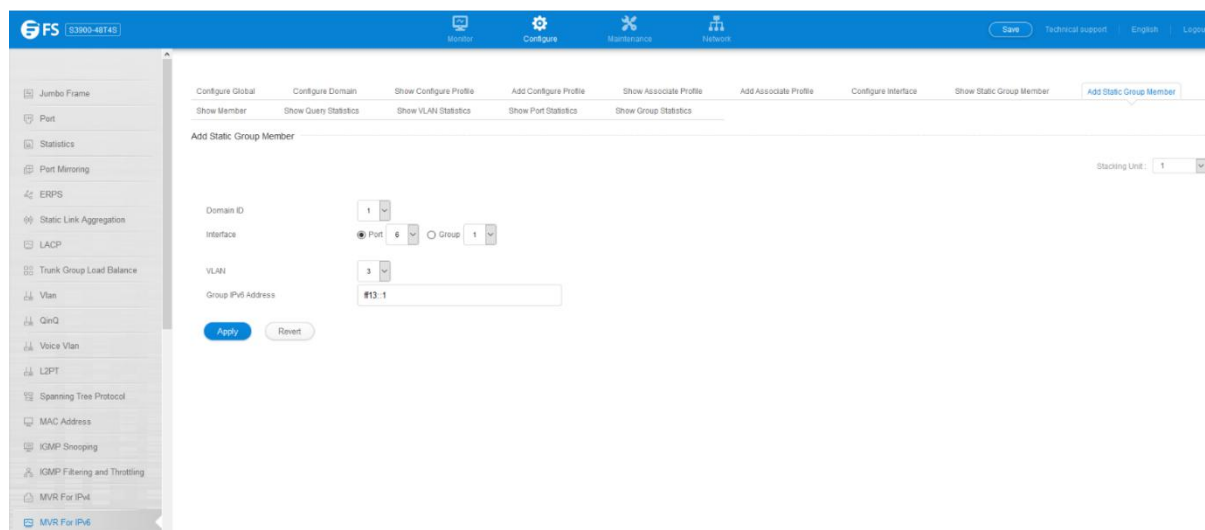


4.15.9 Add Static Group Member

Configure >MVR For IPv6 >Add Static Group Member page is used to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Interface** – Port or group identifier.
- **VLAN** – VLAN identifier. (Range: 1-4093)
- **Group IPv6 Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR6

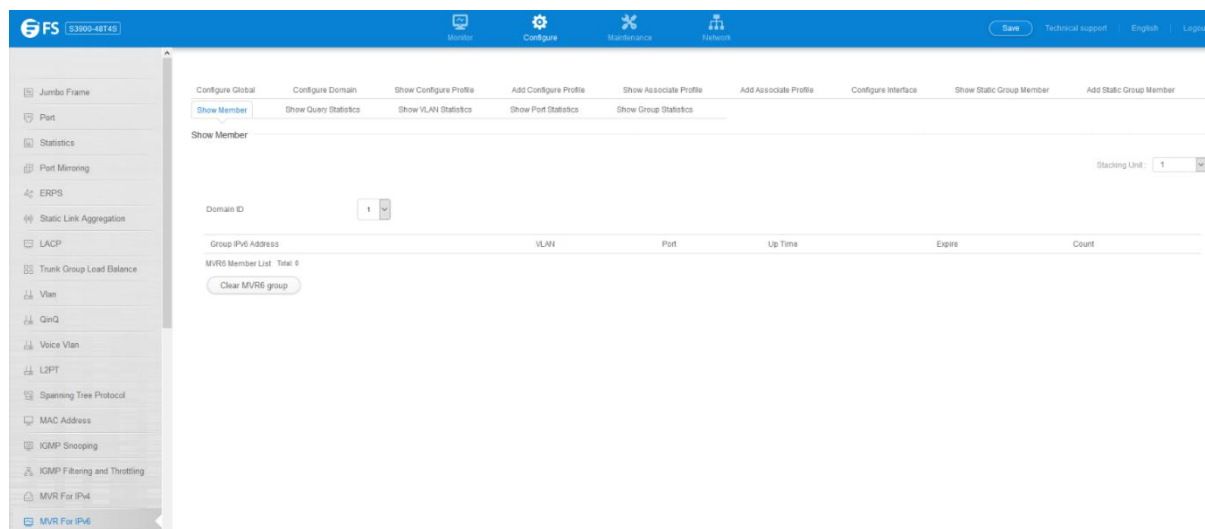
group range configured on the Configure General page.



4.15.10 Show Member

Configure >MVR For IPv6 >Show Member page is used to show the multicast groups either statically or dynamically assigned to the MVR6 receiver groups on each interface.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Group IPv6 Address** – Multicast groups assigned to the MVR6 VLAN.
- **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR6 VLAN if the group address has been statically assigned.
- **Port** – Indicates the source address of the multicast service, or displays an asterisk if the group address has been statically assigned (these entries are marked as “Source”). Also shows the interfaces with subscribers for multicast services provided through the MVR6 VLAN (these entries are marked as “Receiver”).
- **Up Time** – Time this service has been forwarded to attached clients.
- **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.
- **Count** – The number of multicast services currently being forwarded from the MVR6 VLAN.

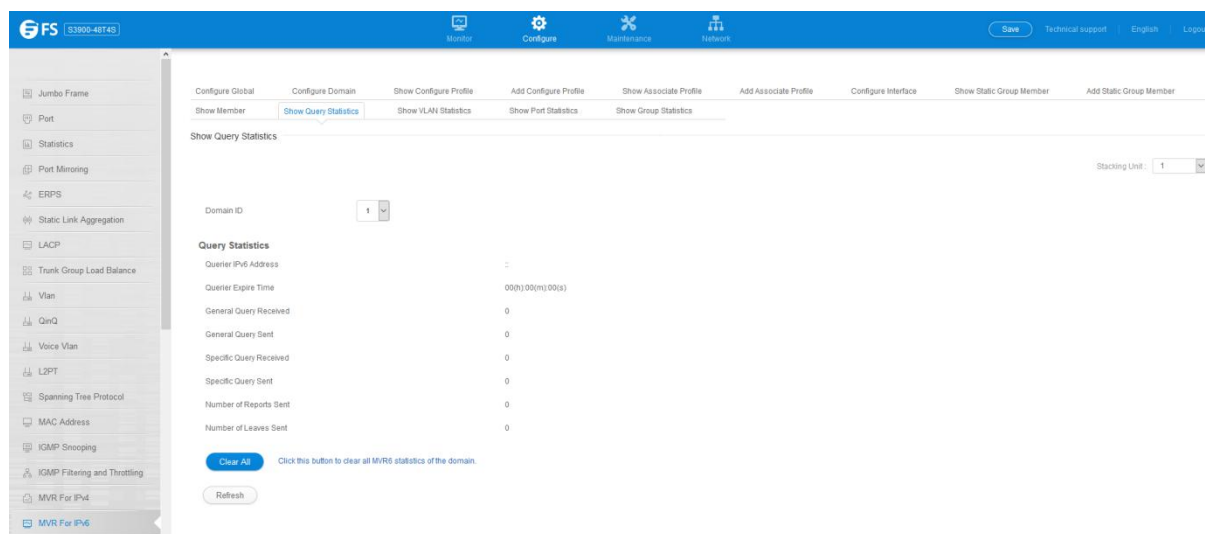


4.15.11 Show Query Statistics

Configure >MVR For IPv6 >Show Query Statistics page is used to display MVR6 protocol-related query statistics for the specified

domain.

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Querier IPv6 Address** – The IP address of the querier on this interface.
- **Querier Expire Time** – The time after which this querier is assumed to have expired.
- **General Query Received** – The number of general queries received on this interface.
- **General Query Sent** – The number of general queries sent from this interface.
- **Specific Query Received** – The number of specific queries received on this interface.
- **Specific Query Sent** – The number of specific queries sent from this interface.
- **Number of Reports Sent** – The number of reports sent from this interface.
- **Number of Leaves Sent** – The number of leaves sent from this interface.



4.15.12 Show VLAN Statistics

Configure > MVR For IPv6 > Show VLAN Statistics page is used to display MVR6 protocol-related statistics for the specified VLAN.

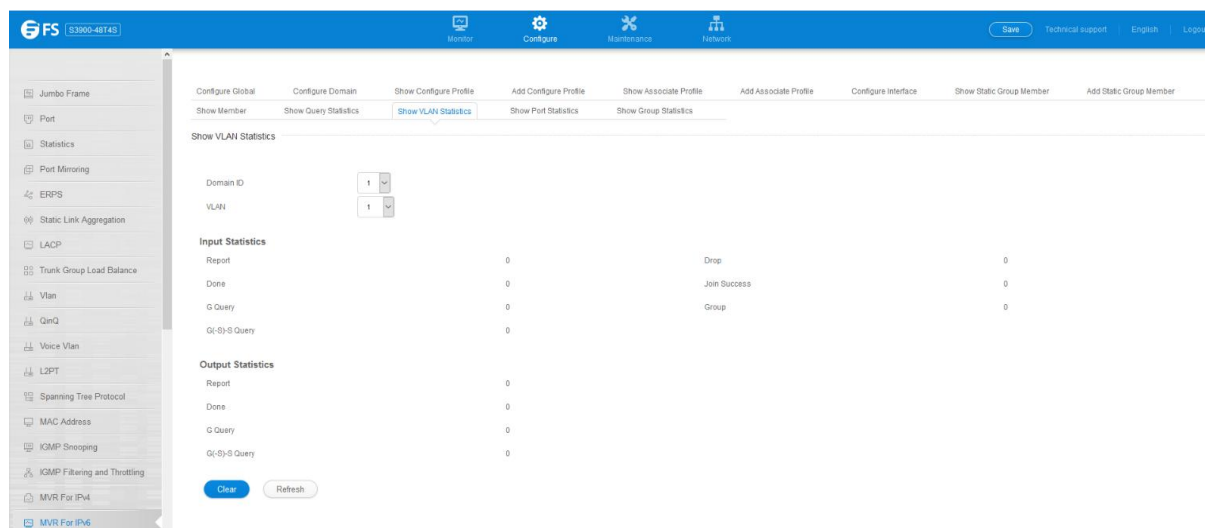
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **VLAN** – VLAN identifier. (Range: 1-4093)

Input Statistics

- **Report** – The number of MLD membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of MVR6 groups active on this interface.

Output Statistics

- **Report** – The number of MLD membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.



4.15.13 Show Port Statistics

Configure > MVR For IPv6 > Show Port Statistics page is used to display MVR6 protocol-related statistics for the specified interface.

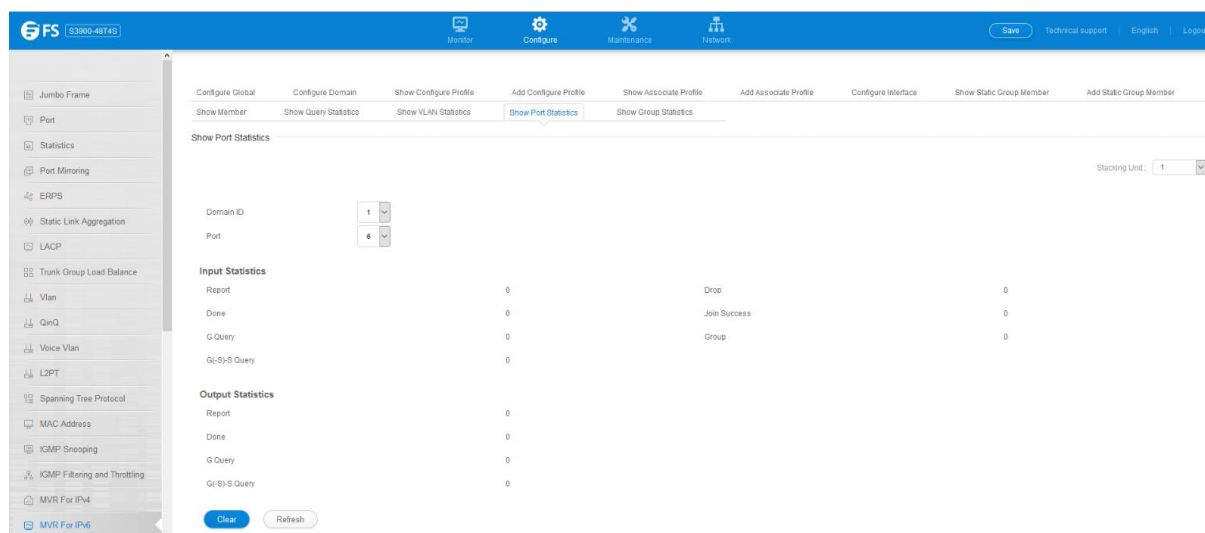
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Port** – Port identifier. (Range: 1-12)

Input Statistics

- **Report** – The number of MLD membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of MVR6 groups active on this interface.

Output Statistics

- **Report** – The number of MLD membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.



4.15.14 Show Group Statistics

Configure > MVR For IPv6 > Show Trunk Statistics page is used to display MVR6 protocol-related statistics for the specified trunk group.

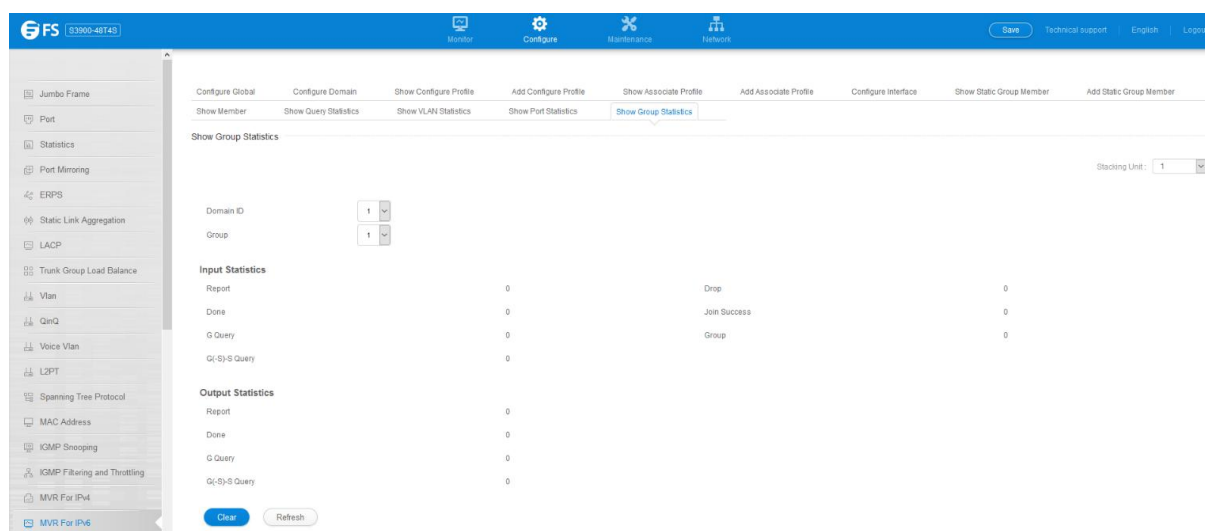
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Group** – Group identifier. (Range: 1-12)

Input Statistics

- **Report** – The number of MLD membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of MVR6 groups active on this interface.

Output Statistics

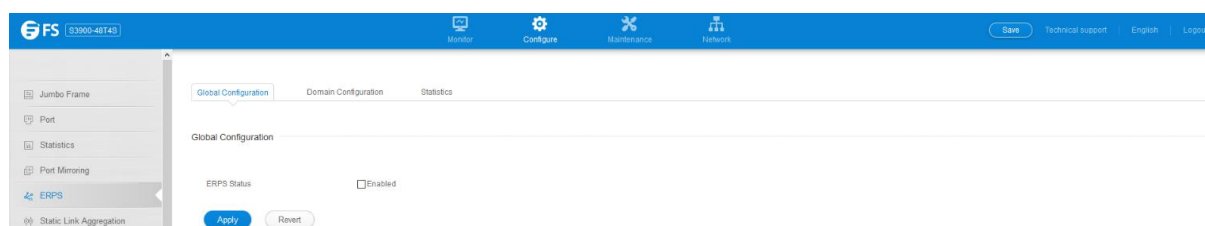
- **Report** – The number of MLD membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.



4.15.15 Global Configuration

Configure >ERPS >Global Configuration page is used to globally enable or disable ERPS on the switch.

- **ERPS Status** – Enables ERPS on the switch. (Default: Disabled) ERPS must be enabled globally on the switch before it can be enabled on an ERPS ring.



4.16 LLDP

4.16.1 Global Configuration

Configure >LLDP >Global Configuration page is used to set attributes for general functions such as globally enabling LLDP on the switch, setting the message age out time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.

- **LLDP** – Enables LLDP globally on the switch. (Default: Enabled)
- **Transmission Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- **Hold Time Multiplier** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4) The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner. TTL in seconds is based on the following rule: minimum value ((Transmission Interval * Hold time Multiplier), or 65535). Therefore, the default TTL is $4 * 30 = 120$ seconds.
- **Delay Interval** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds)

The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

This attribute must comply with the rule: $(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$

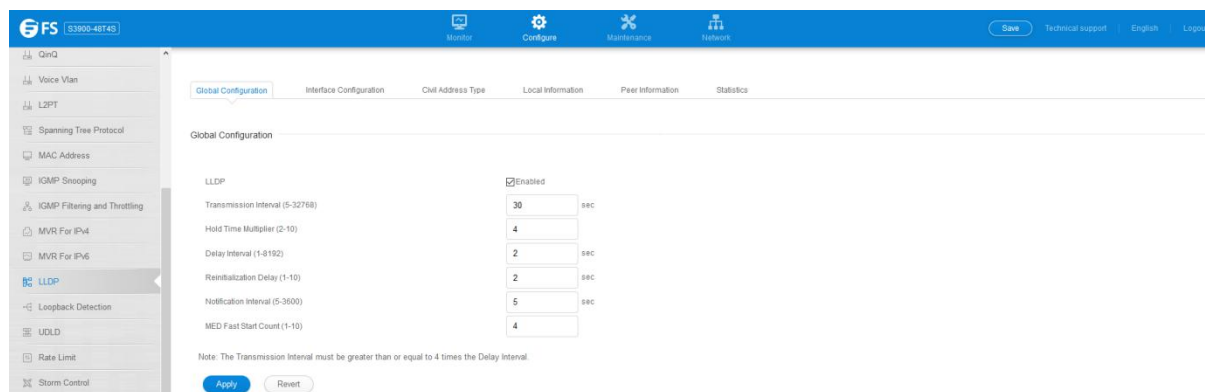
- **Reinitialization Delay** – Configures the delay before attempting to reinitialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds)

When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

- **Notification Interval** – Configures the allowed interval for sending SNMP notifications about LLDP MIB changes. (Range: 5-3600 seconds; Default: 5 seconds)

This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management. Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

- **MED Fast Start Count** – Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDPMED Fast Start mechanism. (Range: 1-10 packets; Default: 4 packets) The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDPMED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.



4.16.2 Interface Configuration

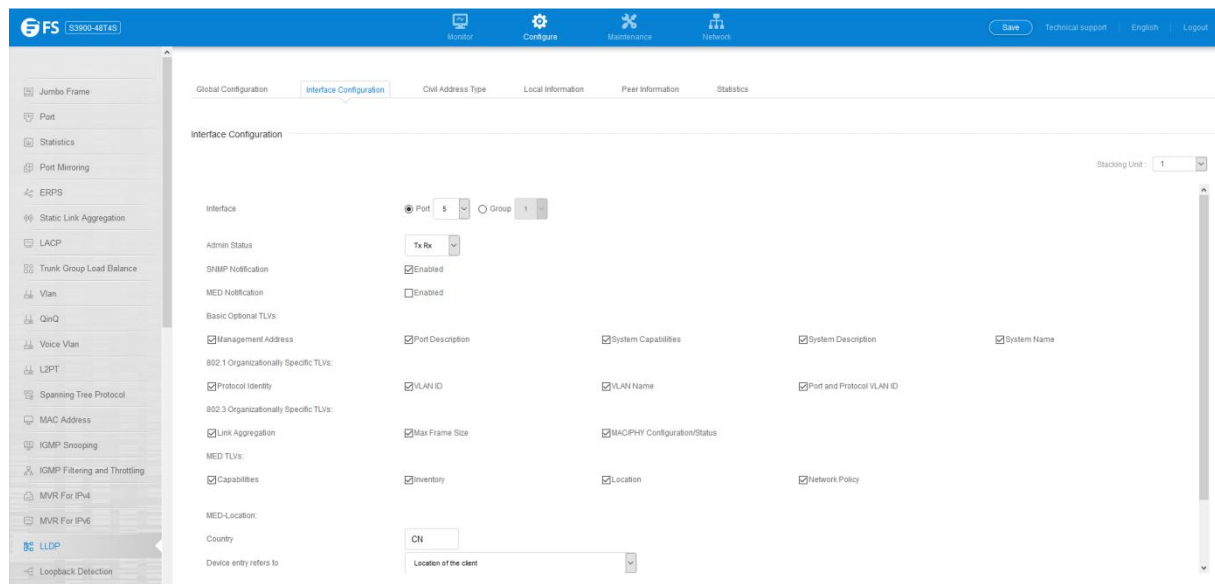
Configure >LLDP >Interface Configuration page is used to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, whether SNMP notifications are sent, and the type of information advertised.

- **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)
- **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP and LLDP-MED changes. (Default: Disabled)
This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/ TIA-1057), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs. For information on defining SNMP trap destinations, Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.
- **MED Notification** – Enables the transmission of SNMP trap notifications about LLDP-MED changes. (Default: Disabled)
- **Basic Optional TLVs** – Configures basic information included in the TLV field of advertised messages.
 - **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this

address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV. Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

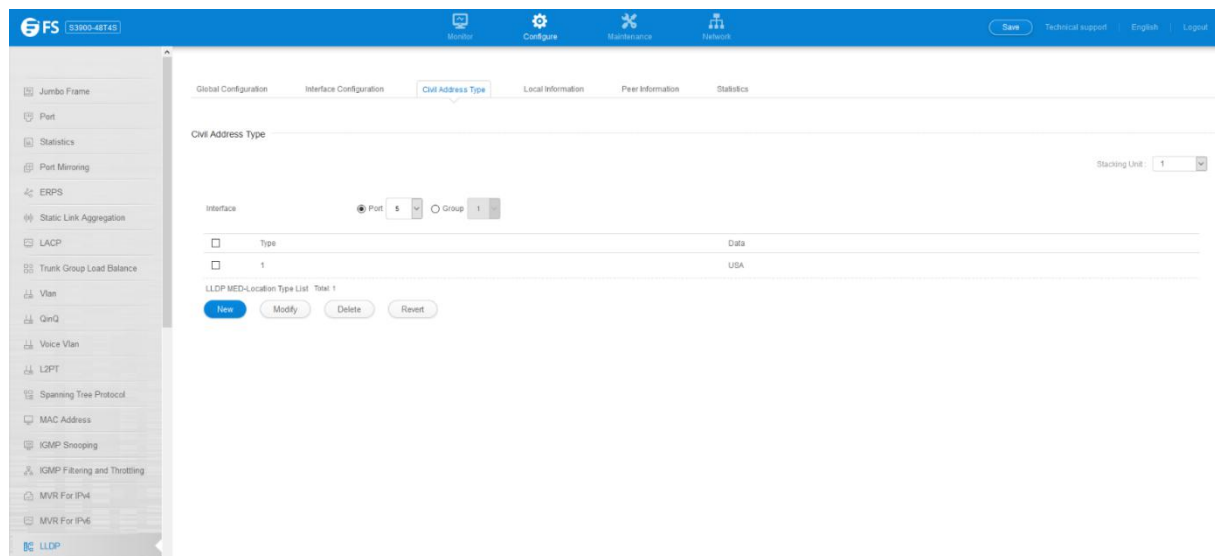
- **Port Description** – The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.
- **System Capabilities** – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.
- **System Description** – The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.
- **System Name** – The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name. To configure the system name.
- 802.1 Organizationally Specific TLVs – Configures IEEE 802.1 information included in the TLV field of advertised messages.
 - **Protocol Identity** – The protocols that are accessible through this interface.
 - **VLAN ID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.
 - **VLAN Name** – The name of all VLANs to which this interface has been assigned.
 - **Port and Protocol VLAN ID** – The port-based protocol VLANs configured on this interface.
- 802.3 Organizationally Specific TLVs – Configures IEEE 802.3 information included in the TLV field of advertised messages.
 - **Link Aggregation** – The link aggregation capabilities, aggregation status of the link, and the IEEE 802.3 aggregated port identifier if this interface is currently a link aggregation member.
 - **Max Frame Size** – The maximum frame size.
 - **MAC/PHY Configuration/Status** – The MAC/PHY configuration and status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.
- **MED TLVs** – Configures general information included in the MED TLV field of advertised messages.
 - **Capabilities** – This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.
 - **Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.
 - **Location** – This option advertises location identification details.
 - **Network Policy** – This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.
- **MED-Location Civic Address** – Configures information for the location of the attached device included in the MED TLV field of advertised messages, including the country and the device type.
 - **Country** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)
 - **Device entry refers to** – The type of device to which the location applies:
 - Location of DHCP server.
 - Location of network element closest to client.
 - Location of client. (This is the default.)



4.16.3 Civil Address Type

Configure > LLDP > Civil Address Type page is used to specify the physical location of the device attached to an interface.

- **CA-Type** – Descriptor of the data civic address value. (Range: 0-255)
- **CA-Value** – Description of a location. (Range: 1-32 characters)




4.16.4 Local Information

Configure >LLDP >Local Information page is used to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

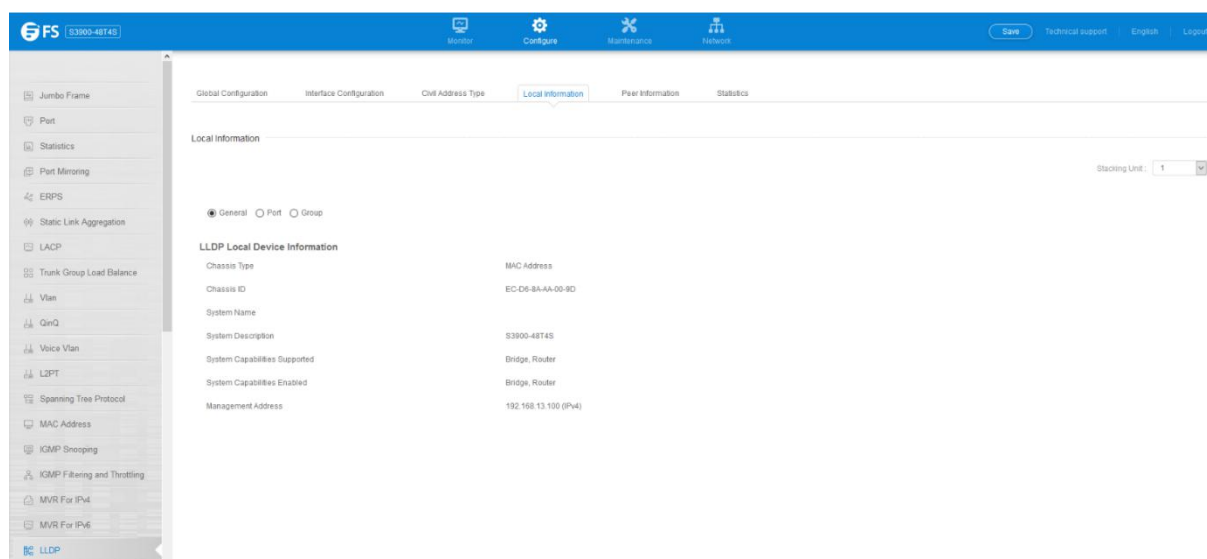
- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.

ID Basis	Reference
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	locally assigned

- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **System Name** – A string that indicates the system's administratively assigned name.
- **System Description** – A textual description of the network entity. This field is also displayed by the **show system** command.
- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

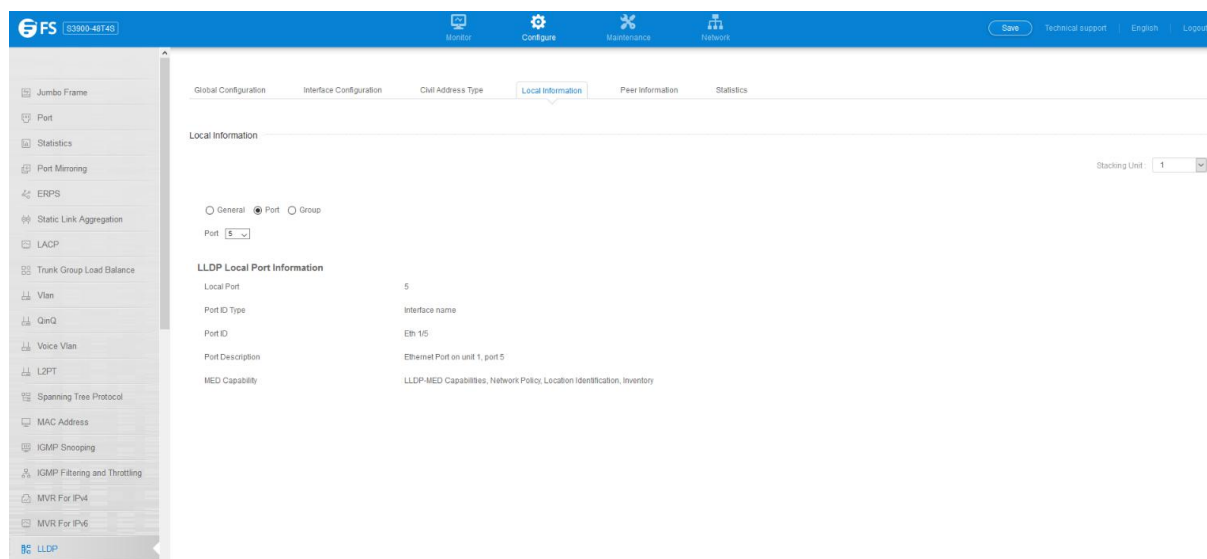
- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table.
- **Management Address** – The management address associated with the local system. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.



Interface Settings

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

- **Port/Group ID** – A string that contains the specific identifier for the port or trunk from which this LLDPDU was transmitted.



4.16.5 Peer Information

Configure >LLDP >Peer Information Group page is used to display information about devices connected directly to the switch's ports which are advertising information through LLDP, or to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **System Name** – A string that indicates the system's administratively assigned name.

Port Details

- **Port** – Port identifier on local switch.
- **Remote Index** – Index of remote device attached to this port.

- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **System Name** – A string that indicates the system's assigned name.
- **System Description** – A textual description of the network entity.
- **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field.

ID Basis	Reference
Interface alias	IfAlias (IETF RFC 2863)
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	agent circuit ID (IETF RFC 3046)
Locally assigned	locally assigned

- **Port Description** – A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.
- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled.
- **Management Address List** – The management addresses for this device. Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Port Details – 802.1 Extension Information

- **Remote Port VID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.
- **Remote Port-Protocol VLAN List** – The port-based protocol VLANs configured on this interface, whether the given port (associated with the remote system) supports port-based protocol VLANs, and whether the port-based protocol VLANs are enabled on the given port associated with the remote system.
- **Remote VLAN Name List** – VLAN names associated with a port.
- **Remote Protocol Identity List** – Information about particular protocols that are accessible through a port. This object represents an arbitrary local integer value used by this agent to identify a particular protocol identity, and an octet string used to identify the protocols associated with a port of the remote system.

Port Details – 802.3 Extension Port Information

- **Remote Port Auto-Neg Supported** – Shows whether the given port (associated with remote system) supports auto-negotiation.
- **Remote Port Auto-Neg Adv-Capability** – The value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) which is associated with a port on the remote system.

Bit	Capability
0	other or unknown
1	10BASE-T half duplex mode
2	10BASE-T full duplex mode
3	100BASE-T4
4	100BASE-TX half duplex mode
5	100BASE-TX full duplex mode
6	100BASE-T2 half duplex mode
7	100BASE-T2 full duplex mode
8	PAUSE for full-duplex links
9	Asymmetric PAUSE for full-duplex links
10	Symmetric PAUSE for full-duplex links
11	Asymmetric and Symmetric PAUSE for full-duplex links
12	1000BASE-X, -LX, -SX, -CX half duplex mode
13	1000BASE-X, -LX, -SX, -CX full duplex mode
14	1000BASE-T half duplex mode
15	1000BASE-T full duplex mode

- **Remote Port Auto-Neg Status** – Shows whether port auto negotiation is enabled on a port associated with the remote system.
- **Remote Port MAU Type** – An integer value that indicates the operational MAU type of the sending device. This object contains the integer value derived from the list position of the corresponding dot3MauType as listed in IETF RFC 3636 and is equal to the last number in the respective dot3MauType OID.

Port Details – 802.3 Extension Power Information

- **Remote Power Class** – The port Class of the given port associated with the remote system (PSE – Power Sourcing Equipment or PD – Powered Device).
- **Remote Power MDI Status** – Shows whether MDI power is enabled on the given port associated with the remote system.
- **Remote Power Pairs** – “Signal” means that the signal pairs only are in use, and “Spare” means that the spare pairs only are in use.
- **Remote Power MDI Supported** – Shows whether MDI power is supported on the given port associated with the remote system.
- **Remote Power Pair Controllable** – Indicates whether the pair selection can be controlled for sourcing power on the given port associated with the remote system.
- **Remote Power Classification** – This classification is used to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points and others, will be classified according to their power requirements.

Port Details – 802.3 Extension Trunk Information

- **Remote Link Aggregation Capable** – Shows if the remote port is not in link aggregation state and/or it does not support link aggregation.
- **Remote Link Aggregation Status** – The current aggregation status of the link.
- **Remote Link Port ID** – This object contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component associated with the remote system. If the remote port is not in link aggregation state and/or it does not support link aggregation, this value should be zero.

Port Details – 802.3 Extension Frame Information

- **Remote Max Frame Size** – An integer value indicating the maximum supported frame size in octets on the port component associated with the remote system.

Port Details – LLDP-MED Capability 8

- **Device Class** – Any of the following categories of endpoint devices:
 - Class 1 – The most basic class of endpoint devices.
 - Class 2 – Endpoint devices that supports media stream capabilities.
 - Class 3 – Endpoint devices that directly supports end users of the IP communication systems.
 - Network Connectivity Device – Devices that provide access to the IEEE 802 based LAN infrastructure for LLDP-MED endpoint devices. These may be any LAN access device including LAN switch/router, IEEE 802.1 bridge, IEEE 802.3 repeater, IEEE 802.11 wireless access point, or any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.
- **Supported Capabilities** – The supported set of capabilities that define the primary function(s) of the port:
 - LLDP-MED Capabilities
 - Network Policy
 - Location Identification
 - Extended Power via MDI – PSE
 - Extended Power via MDI – PD
 - Inventory
- **Current Capabilities** – The set of capabilities that define the primary function(s) of the port which are currently enabled.

Port Details – Network Policy 8

- **Application Type** – The primary application(s) defined for this network policy:
 - Voice
 - Voice Signaling
 - Guest Signaling
 - Guest Voice Signaling
 - Softphone Voice
 - Video Conferencing
 - Streaming Video
 - Video Signaling
- **Tagged Flag** – Indicates whether the specified application type is using a tagged or untagged VLAN.
- **Layer 2 Priority** – The Layer 2 priority to be used for the specified application type. This field may specify one of eight priority levels (0-7), where a value of 0 represents use of the default priority.
- **Unknown Policy Flag** – Indicates that an endpoint device wants to explicitly advertise that this policy is required by the device, but is currently unknown.
- **VLAN ID** – The VLAN identifier (VID) for the port as defined in IEEE 802.1Q. A value of zero indicates that the port is using priority tagged frames, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
- **DSCP Value** – The DSCP value to be used to provide Diffserv node behavior for the specified application type. This field may contain one of 64 code point values (0-63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

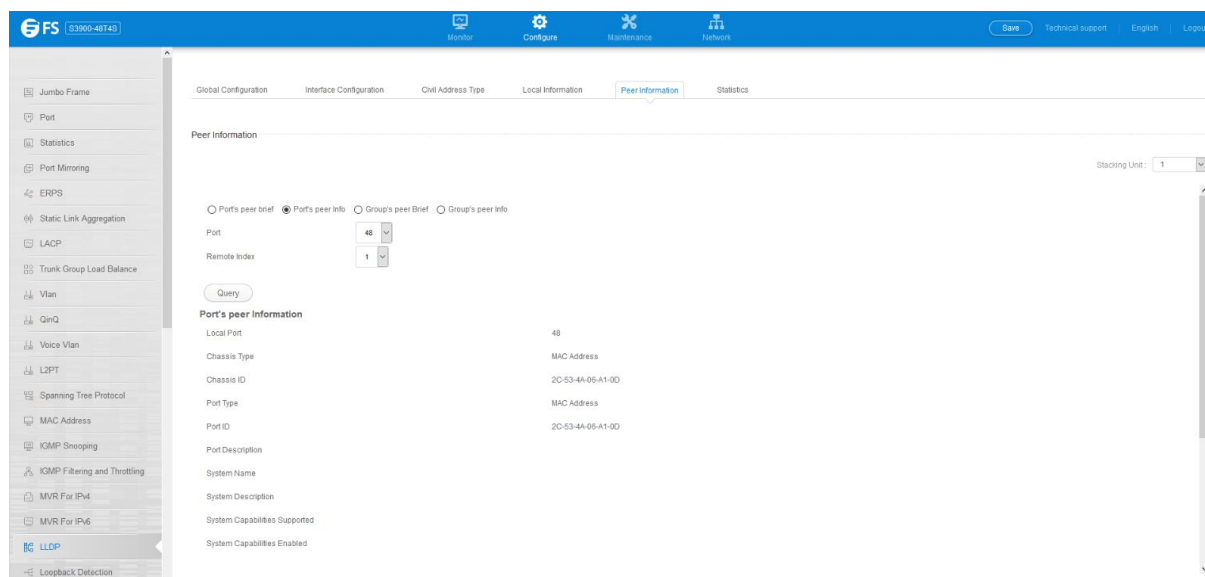
Port Details – Location Identification 8

- **Location Data Format** – Any of these location ID data formats:
 - Coordinate-based LCI9 – Defined in RFC 3825, includes latitude resolution, latitude, longitude resolution, longitude, altitude type, altitude resolution, altitude, and datum.
 - Civic Address LCI9 – Includes What, Country code, CA type, CA length and CA value.

- **ECS ELIN** – Emergency Call Service Emergency Location Identification Number supports traditional PSAP-based Emergency Call Service in North America.
- **Country Code** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)
- **What** – The type of device to which the location applies as described for the field entry.

Port Details – Inventory8

- **Hardware Revision** – The hardware revision of the end-point device.
- **Software Revision** – The software revision of the end-point device.
- **Manufacture Name** – The manufacturer of the end-point device
- **Asset ID** – The asset identifier of the end-point device. End-point devices are typically assigned asset identifiers to facilitate inventory management and assets tracking.
- **Firmware Revision** – The firmware revision of the end-point device.
- **Serial Number** – The serial number of the end-point device.
- **Model Name** – The model name of the end-point device.
- **Asset ID** – The asset identifier of the end-point device.



4.16.6 Statistics

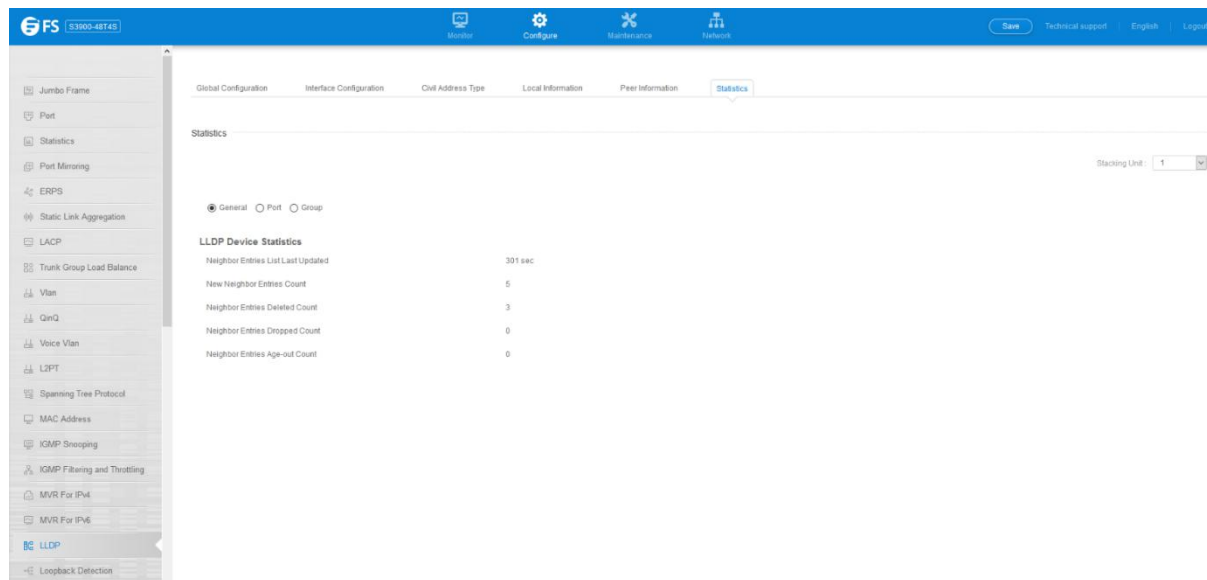
Configure >LLDP >Show Statistics page is used to display statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

- **Neighbor Entries List Last Updated** – The time the LLDP neighbor entry list was last updated.
- **New Neighbor Entries Count** – The number of LLDP neighbors for which the remote TTL has not yet expired.
- **Neighbor Entries Deleted Count** – The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.
- **Neighbor Entries Dropped Count** – The number of times which the remote database on this switch dropped an LLDPDU because of insufficient resources.
- **Neighbor Entries Age-out Count** – The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Port/Trunk

- **Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.
- **Frames Invalid** – A count of all LLDPDUs received with one or more detectable errors.

- **Frames Received** – Number of LLDP PDUs received.
- **Frames Sent** – Number of LLDP PDUs transmitted.
- **TLVs Unrecognized** – A count of all TLVs not recognized by the receiving LLDP local agent.
- **TLVs Discarded** – A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.
- **Neighbor Ageouts** – A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

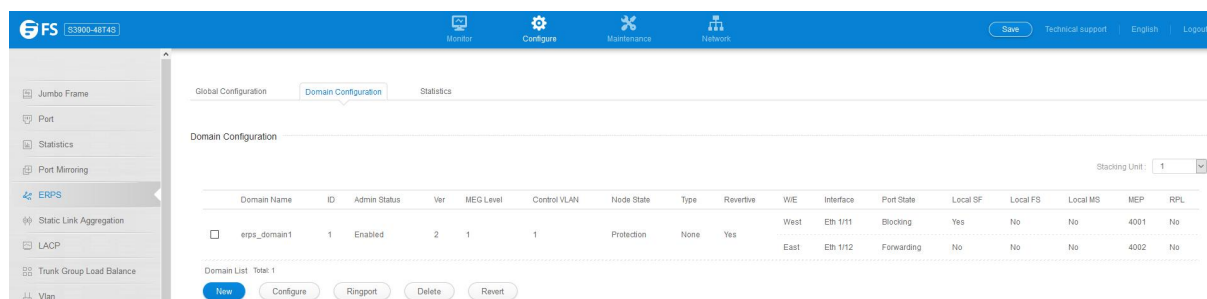


4.17 ERPS

Ethernet Ring Protection Switching (ERPS) is The ITU G.8032.

4.17.1 Domain Configuration

Configure > ERPS > Domain Configuration pages is used to add ERPS domain and configure domain details.





- **Domain Name** – Name of a configured ERPS ring.
- **Node State** – Shows the following ERPS states:
 - Init – The ERPS ring has started but has not yet determined the status of the ring.
 - Idle – If all nodes in a ring are in this state, it means that all the links in the ring are up. This state will switch to protection state if a link failure occurs.
 - Protection – If a node in this state, it means that a link failure has occurred. This state will switch to idle state if all the failed links recover.
- **MEG Level** – The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.
- **Admin Status** – Shows whether ERPS is enabled on the switch.
- **West Port** – Shows the west ring port for this node.
- **East Port** – Shows the east ring port for this node.
- **RPL Owner** – Shows if this node is the RPL owner.
- **Control VLAN** – Shows the Control VLAN ID.
- **Non ERPS Device Protection** – Shows if non-standard health-check packets are sent when in protection state.

Configure Details

- **Domain Name** – Name of a configured ERPS ring.
- **Admin Status** – Activates the current ERPS ring. Before enabling a ring, the global ERPS function should be enabled, the east and west ring ports configured on each node, the RPL owner specified, and the control VLAN configured. Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter idle state if no signal failures are detected.
- **MEG Level** – The maintenance entity group (MEG) level which provides a communication channel for ring automatic protection switching (R-APS) information. (Range: 0-7) This parameter is used to ensure that received R-APS PDUs are directed for this ring. A unique level should be configured for each local ring if there are many R-APS PDUs passing through this switch.
- **Node ID** – A MAC address unique to the ring node. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- **Node State** – Refer to the parameters for the Show page.
- **West Port** – Connects to next ring node to the west. Each node must be connected to two neighbors on the ring. For convenience, the ports connected are referred to as east and west

ports. Alternatively, the closest neighbor to the east should be the next node in the ring in a clockwise direction, and the closest neighbor to the west should be the next node in the ring in a counter-clockwise direction. Note that a ring port cannot be configured as a member of a spanning tree, a dynamic trunk, or a static trunk. Once configured, this field shows the ring port for this node, and the interface state:

- **Blocking** – The transmission and reception of traffic is blocked and the forwarding of R-APS messages is blocked, but the transmission of locally generated R-APS messages is allowed and the reception of all R-APS messages is allowed.
- **Forwarding** – The transmission and reception of traffic is allowed; transmission, reception and forwarding of R-APS

messages is allowed.

- Down – The interface is not linked up.
- Unknown – The interface is not in a known state.
- **East Port** – Connects to next ring node to the east.
- **RPL Port** – If node is connected to the RPL, this shows by which interface.
- **RPL Owner** – Configures a ring node to be the Ring Protection Link (RPL) owner.
- **Holdoff Timer** – The hold-off timer is used to filter out intermittent link faults. Faults will only be reported to the ring protection mechanism if this timer expires. (Range: 0-10000 milliseconds, in steps of 100 milliseconds) In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer. When a new defect or more severe defect occurs (new Signal Failure), this event will not be reported immediately to the protection switching mechanism if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the timer expires, whether a defect still exists or not, the timer will be checked. If one does exist, that defect will be reported to the protection switching mechanism. The reported defect need not be the same one that started the timer.
- **Guard Timer** – The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process, giving time for old messages still circulating on the ring to expire. (Range: 10-2000 milliseconds, in steps of 10 milliseconds) The guard timer duration should be greater than the maximum expected forwarding delay for an R-APS message to pass around the ring. A side-effect of the guard timer is that during its duration, a node will be unaware of new or existing ring requests transmitted from other nodes.
- **WTR Timer** – The wait-to-restore timer is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. (Range: 5-12 minutes) If the switch goes into ring protection state due to a signal failure, after the failure condition is cleared, the RPL owner will start the wait-to-restore timer and wait until it expires to verify that the ring has

stabilized before blocking the RPL and returning to the Idle (normal operating) state.

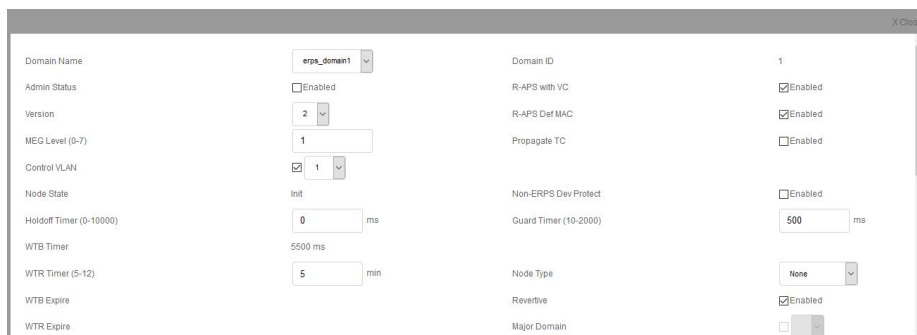
- **Control VLAN** – A dedicated VLAN used for sending and receiving E-APS protocol messages. (Range: 1-4093) Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN, add the ring ports for the east and west interface as tagged members to this VLAN, and then use this parameter to add it to the ring. The following restrictions are recommended to avoid creating a loop in the network or other problems which may occur under some situations:
 - The Control VLAN must not be configured as a Layer 3 interface (with an IP address), a dynamic VLAN (with GVRP enabled), nor as a private VLAN.
 - In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN.
 - Also, the ring ports of the Control VLAN must be tagged. Once the ring has been activated, the configuration of the control VLAN cannot be modified. Use the Admin Status parameter to stop the ERPS ring before making any configuration changes to the control VLAN.
- **Propagate TC** – Enables propagation of topology change messages from a secondary ring to the primary ring. (Default: Disabled) When a secondary ring detects a topology change, it can pass a message about this event to the major ring. When the major ring receives this kind of message from a secondary ring, it can clear the MAC addresses on its ring ports to help the secondary ring restore its connections more quickly through protection switching.

When the MAC addresses are cleared, data traffic may flood onto the major ring. The data traffic will become stable after the MAC addresses are learned again. The major ring will not be broken, but the bandwidth of data traffic on the major ring may suffer for a short period of time due to this flooding behavior.

- **Sub Domain** – A secondary ERPS ring which uses this primary ring for sending control packets.
- **Major Domain** – The ERPS ring used for sending control packets. This switch can support up to two rings. However, ERPS control packets can only be sent on one ring. This parameter is used to indicate that the current ring is a secondary ring, and to specify the major ring which will be used to send ERPS control packets. The Ring Protection Link (RPL) is always the west port. So the

physical port on a secondary ring must be the west port. In other words, if a domain has two physical ring ports, this ring can only be a major ring, not a secondary ring (or sub-domain) which can have only one physical ring port. The major domain therefore cannot be set if the east port is already configured.

- **Non-ERPS Device Protection** – Sends non-standard health-check packets when an owner node enters protection state without any link down event having been detected through Signal Fault messages. (Default: Disabled)



Domain Name	erps_domain1	Domain ID	1
Admin Status	<input type="checkbox"/> Enabled	R-APS with VC	<input checked="" type="checkbox"/> Enabled
Version	2	R-APS Def MAC	<input checked="" type="checkbox"/> Enabled
MEG Level (0-7)	1	Propagate TC	<input type="checkbox"/> Enabled
Control VLAN	<input checked="" type="checkbox"/> 1	Non-ERPS Dev Protect	<input type="checkbox"/> Enabled
Node State	Init	Guard Timer (10-2000)	500 ms
Holdoff Timer (0-10000)	0 ms	Node Type	None
WTB Timer	5500 ms	Revertive	<input checked="" type="checkbox"/> Enabled
WTR Timer (5-12)	5 min	Major Domain	<input type="checkbox"/> Major
WTB Expire			
WTR Expire			

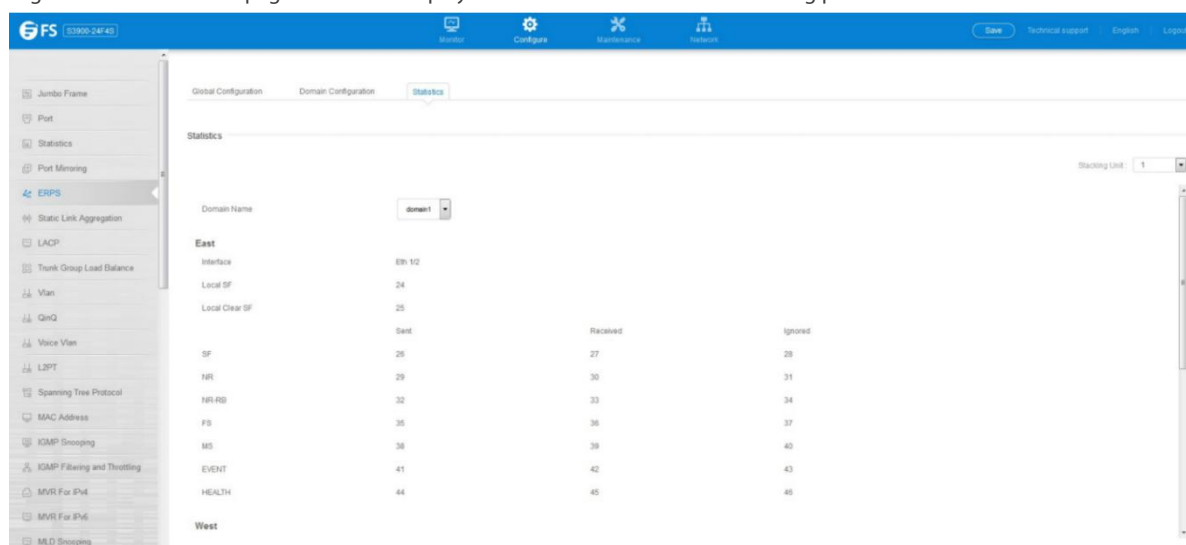
Press Ringport button to configure force or manual mode on ring ports.



Domain Name	erps_domain1
Operation	Forced-switch West
<input type="button" value="Apply"/>	

4.17.2 Statistics

Configure >ERPS >Statistics pages is used to display or clear statistics information on ring ports.



Statistics		Stacking Unit
Domain Name	domain1	1
East		
Interface	Eth 1/2	
Local SF	24	
Local Clear SF	25	
	Sent	Received
SF	26	27
NR	29	30
NR RB	32	33
FS	35	36
MS	38	39
EVENT	41	42
HEALTH	44	45
		Ignored
		28
		31
		34
		37
		40
		43
		46
West		

4.18 Loopback Detection

Configure >Loopback Detection page is used to configure loopback detection on an interface.

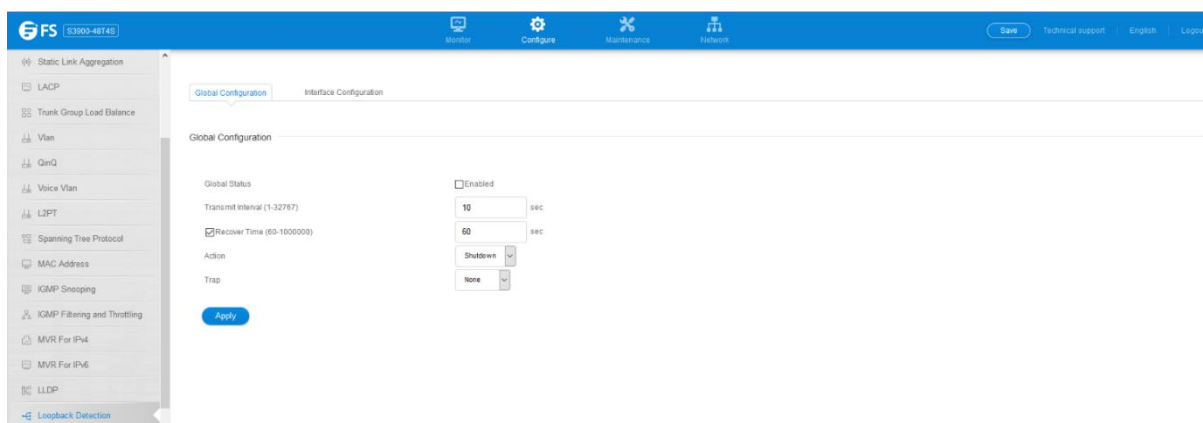
When loopback detection is enabled and a port or group receives it's own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode.

This loopback state can be released manually or automatically. If the interface is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

- The interface receives any other BPDU except for its own, or;
- The interfaces's link status changes to link down and then link up again, or;
- The interface ceases to receive its own BPDUs in a forward delay interval.

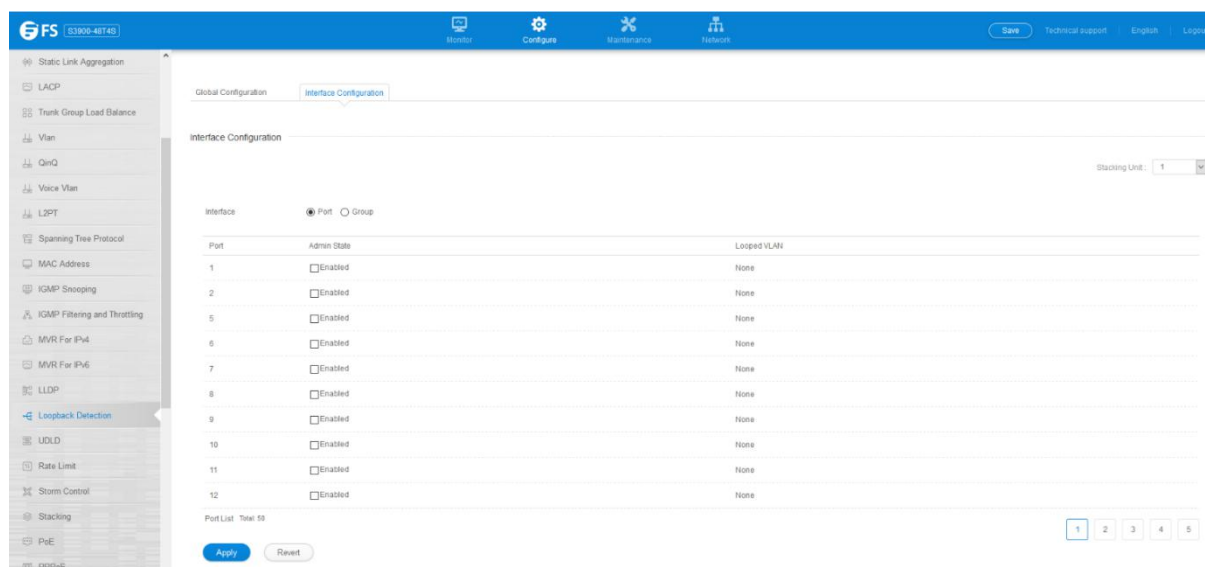
4.18.1 Global Configuration

- **Status** – Enables loopback detection on this interface. (Default: Enabled)
- **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)
- **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)
- **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.
- **Action** – Sets the response for loopback detection to block user traffic or shut down the interface. (Default: Block)
- **Transmit Interval** – The duration to shut down the interface. (Range: 1-32767 seconds; Default: 60 seconds) If an interface is shut down due to a detected loopback, and the release mode is set to “Auto,” the selected interface will be automatically enabled when the shutdown interval has expired. If an interface is shut down due to a detected loopback, and the release mode is set to “Manual,” the interface can be re-enabled using the Release button.



4.18.2 Interface Configuration

Enable/disable port loopback detection



4.19 UDLD

The switch can be configured to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back.

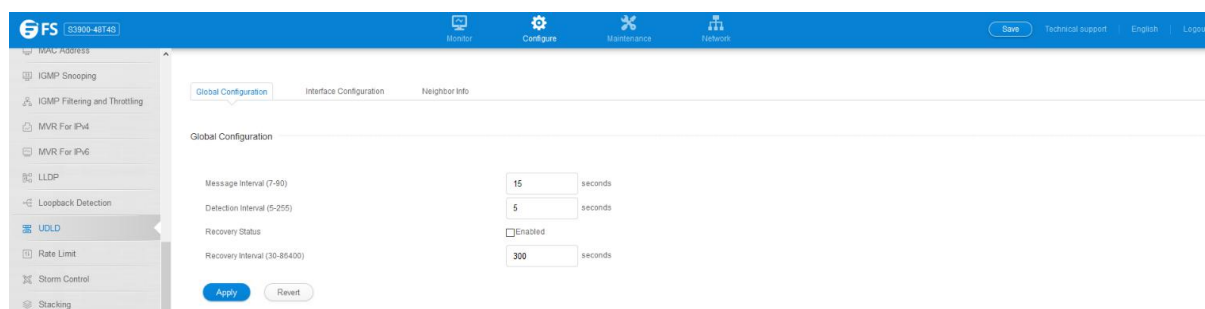
4.19.1 Global Configuration

Configure >UDLD >Global Configuration page is used to configure the UniDirectional Link Detection message probe interval, detection interval, and recovery interval.

- **Message Interval** – Configures the message interval between UDLD probe messages for ports in the advertisement phase and determined to be bidirectional. (Range: 7-90 seconds; Default: 15 seconds) UDLD probe messages are sent after linkup or detection phases. During the detection phase, messages are exchanged at the maximum rate of one per second. After that, if the protocol reaches a stable state and determines that the link is bidirectional, the message interval is increased to a configurable value based on a curve known as M1(t), a time-based function described in RFC 5171. If the link is deemed anything other than bidirectional at the end of the detection phase, this curve becomes a flat line with a fixed value of Mfast (7 seconds). If the link is instead deemed bidirectional, the curve will use Mfast for the first four subsequent message transmissions and then transition to an Mslow value for all other steady-state transmissions. Mslow is the value configured by this command.
- **Detection Interval** – Sets the amount of time the switch remains in detection state after discovering a neighbor. (Range: 5-255 seconds; Default: 5 seconds) When a neighbor device is discovered by UDLD, the switch enters “detection state” and remains in this state for specified detection-interval. After the detection-interval expires, the switch tries to decide whether or the link is unidirectional based on the information collected during the “detection state.”
- **Recovery Status** – Configures the switch to automatically recover from UDLD disabled port state after a period specified by the Recovery Interval. (Default: Disabled)

When automatic recovery state is changed, any ports shut down by UDLD will be reset.

- **Recovery Interval** – Specifies the period after which to automatically recover from UDLD disabled port state. (Range: 30-86400 seconds; Default: 7 seconds) When the recovery interval is changed, any ports shut down by UDLD will be reset.



4.19.2 Interface Configuration

Configure >UDLD >Interface Configuration page is used to enable UDLD and aggressive mode which reduces the shut-down delay after loss of bidirectional connectivity is detected.

- Port – Port identifier. (Range: 1-28/52)
- UDLD – Enables UDLD on a port. (Default: Disabled)
 - UDLD requires that all the devices connected to the same LAN segment be running the protocol in order for a potential mis-configuration to be detected and for prompt corrective action to be taken.
 - Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-synch neighbor, it (re)starts the detection process on its side of the connection and sends N echo messages in reply. (This mechanism implicitly assumes that N packets are sufficient to get through a link and reach the other end, even though some of them might get dropped during the transmission.) Since this behavior must be the same on all the neighbors, the sender of the echoes expects to receive an echo in reply. If the detection process ends without the proper echo information being received, the link is

considered to be unidirectional.

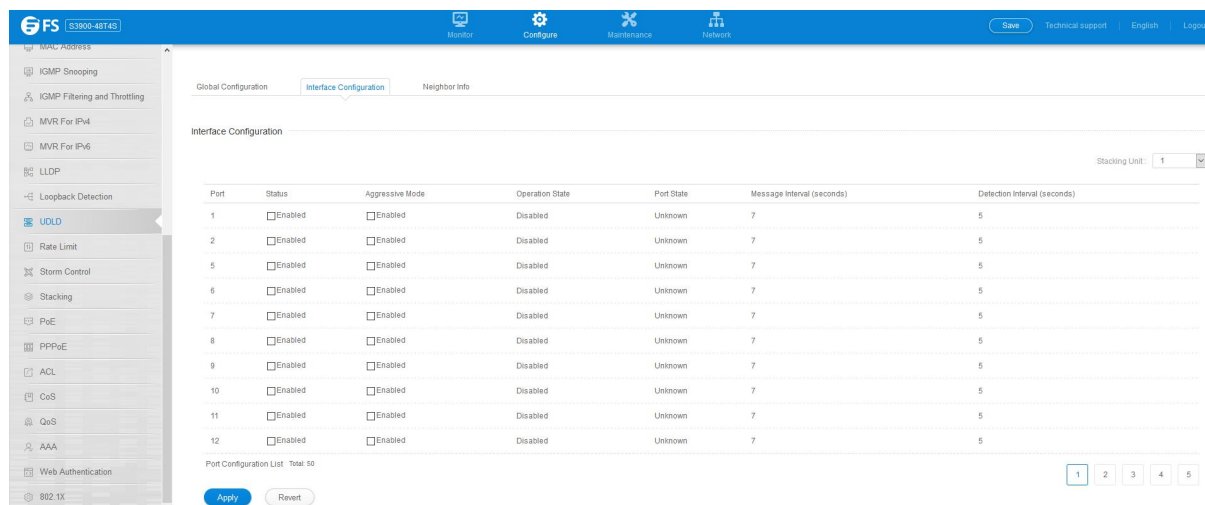
- Aggressive Mode – Reduces the shut-down delay after loss of bidirectional connectivity is detected. (Default: Disabled) UDLD can function in two modes: normal mode and aggressive mode.
 - In normal mode, determination of link status at the end of the detection process is always based on information received in UDLD messages: whether that's information about the exchange of proper neighbor identification or the absence of such. Hence, albeit bound by a timer, normal mode determinations are always based on gleaned information, and as such are "event-based." If no such information can be obtained (e.g., because of a bidirectional loss of connectivity), UDLD follows a conservative approach to minimize false positives during the detection process and deems a port to be in "undetermined" state. In other words, normal mode will shut down a port only if it can explicitly determine that

the associated link is faulty for an extended period of time.

- In aggressive mode, UDLD will also shut down a port if it loses bidirectional connectivity with the neighbor for the same extended period of time (as that mentioned above for normal mode) and subsequently fails repeated last-resort attempts to re-establish communication with the other end of the link. This mode of operation assumes that loss of communication with the neighbor is a meaningful network event in itself, and a symptom of a serious connectivity problem. Because this type of detection can be event-less, and lack of information cannot always be associated to an actual malfunction of the link, this mode is recommended only in certain scenarios (typically only on point-to-point links where no communication failure between two neighbors is admissible).
- Operation State – Shows the UDLD operational state (Disabled, Link down, Link up, Advertisement, Detection, Disabled port, Advertisement - Single neighbor, Advertisement - Multiple neighbors)
- Port State – Shows the UDLD port state (Unknown, Bidirectional, Unidirectional, Transmit-to-receive loop, Mismatch with neighbor state reported, Neighbor's echo is empty)

The state is Unknown if the link is down or not connected to a UDLD-capable device. The state is Bidirectional if the link has a normal two-way connection to a UDLD-capable device. All other states indicate mis-wiring.

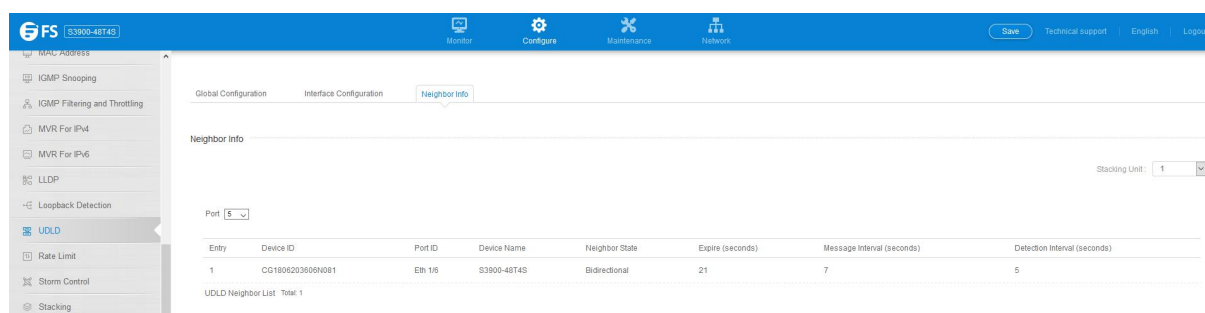
- **Message Interval** – The interval between UDLD probe messages used for the indicated operational state.
- **Detection Interval** – The period the switch remains in detection state after discovering a neighbor.



4.19.3 Neighbor Info

Configure >UDLD >Neighbor Info page is used to show UDLD neighbor information, including neighbor state, expiration time, and protocol intervals.

- **Port** – Port identifier. (Range: 1-28/52)
- **Entry** – Table entry number uniquely identifying the neighbor device discovered by UDLD on a port interface.
- **Device ID** – Device identifier of neighbor sending the UDLD packet.
- **Port ID** – The physical port the UDLD packet is sent from.
- **Device Name** – The device name of this neighbor.
- **Neighbor State** – Link status of neighbor device (Values: unknown, neighborsEcholsEmpty, bidirectional, mismatchWithneighborStateReported, unidirectional).
- **Expire** – The amount of time remaining before this entry will expire.
- **Message Interval** – The interval between UDLD probe messages for ports in advertisement phase.
- **Detection Interval** – The period the switch remains in detection state after discovering a neighbor.

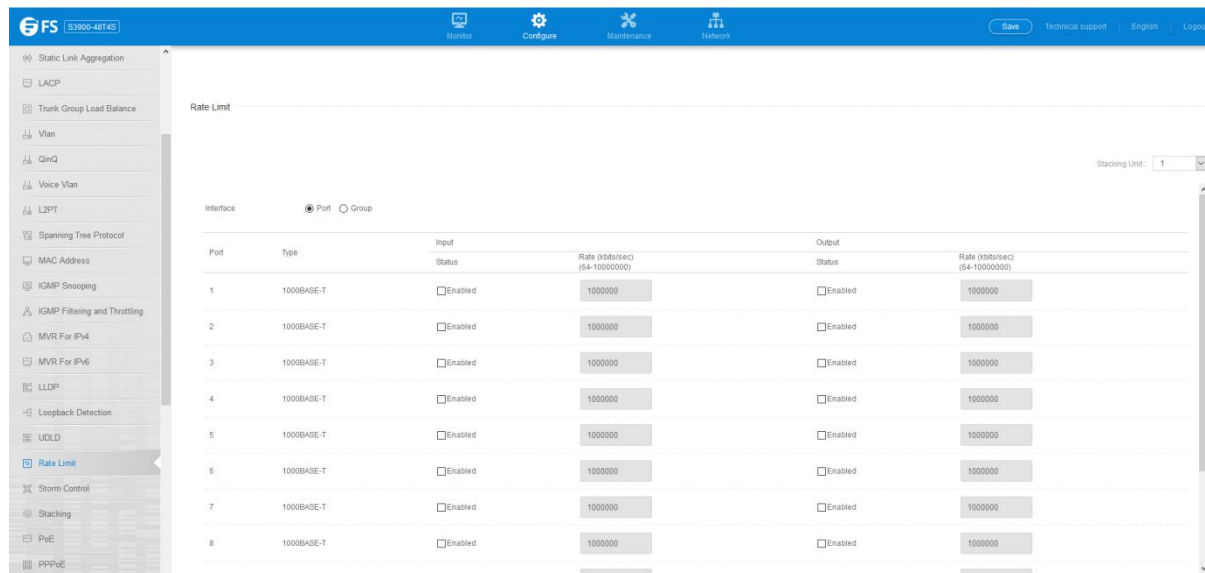


4.20 Rate Limit

Configure >Rate Limit page is used to apply rate limiting to ingress or egress ports. This function allows the network manager to control the maximum rate for traffic received or transmitted on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

- **Interface**– Displays the switch's ports or Groups.
- **Type** – Indicates the port type. (1000BASE-T, 10GBASE SFP+)
- **Status** – Enables or disables the rate limit. (Default: Disabled)
- **Rate** – Sets the rate limit level.(Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports;64 - 10,000,000 kbits per second for 10 Gigabit Ethernet ports)



Rate Limit

Stacking Unit: 1

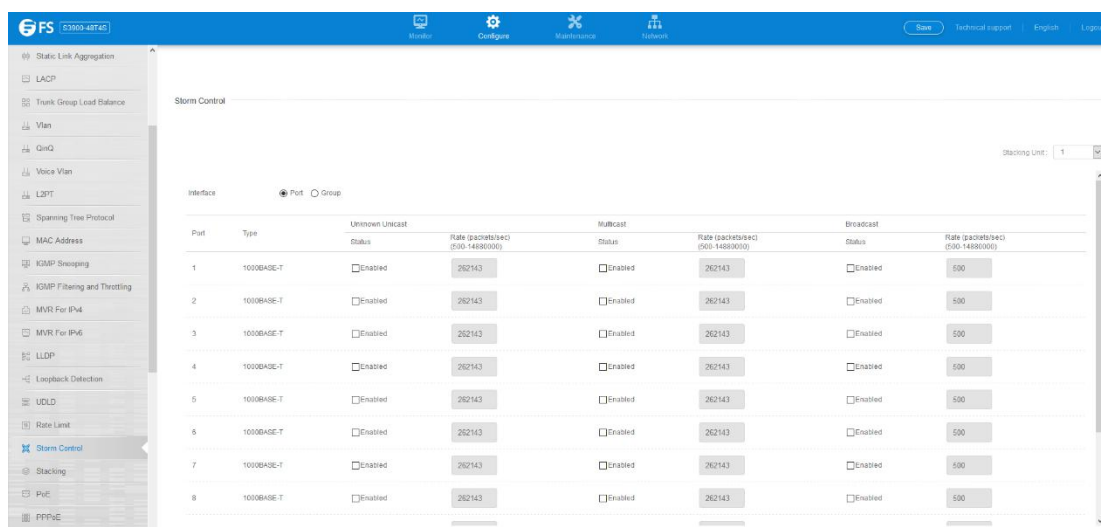
Interface: ☒ Port ☐ Group

Port	Type	Input Status	Rate (kbits/sec) (64-10000000)	Output Status	Rate (kbits/sec) (64-10000000)
1	1000BASE-T	<input checked="" type="checkbox"/> Enabled	1000000	<input checked="" type="checkbox"/> Enabled	1000000
2	1000BASE-T	<input checked="" type="checkbox"/> Enabled	1000000	<input checked="" type="checkbox"/> Enabled	1000000
3	1000BASE-T	<input checked="" type="checkbox"/> Enabled	1000000	<input checked="" type="checkbox"/> Enabled	1000000
4	1000BASE-T	<input checked="" type="checkbox"/> Enabled	1000000	<input checked="" type="checkbox"/> Enabled	1000000
5	1000BASE-T	<input checked="" type="checkbox"/> Enabled	1000000	<input checked="" type="checkbox"/> Enabled	1000000
6	1000BASE-T	<input checked="" type="checkbox"/> Enabled	1000000	<input checked="" type="checkbox"/> Enabled	1000000
7	1000BASE-T	<input checked="" type="checkbox"/> Enabled	1000000	<input checked="" type="checkbox"/> Enabled	1000000
8	1000BASE-T	<input checked="" type="checkbox"/> Enabled	1000000	<input checked="" type="checkbox"/> Enabled	1000000

4.21 Storm Control

Configure >Storm Control page is used to configure broadcast, multicast, and unknown unicast storm control thresholds.

- **Interface** – Displays a list of ports or groups.
- **Type** – Indicates interface type. (1000BASE-T or 10GBASE SFP)
- **Unknown Unicast** – Specifies storm control for unknown unicast traffic.
- **Multicast** – Specifies storm control for multicast traffic.
- **Broadcast** – Specifies storm control for broadcast traffic.
- **Status** – Enables or disables storm control. (Default: Enabled for broadcast storm control, disabled for multicast and unknown unicast storm control)
- **Rate** – Threshold level in Kilo bits per second.(Range: 64-10,000,000 Kbps; Default: 64 Kbps)



Storm Control

Stacking Unit: 1

Interface: ☒ Port ☐ Group

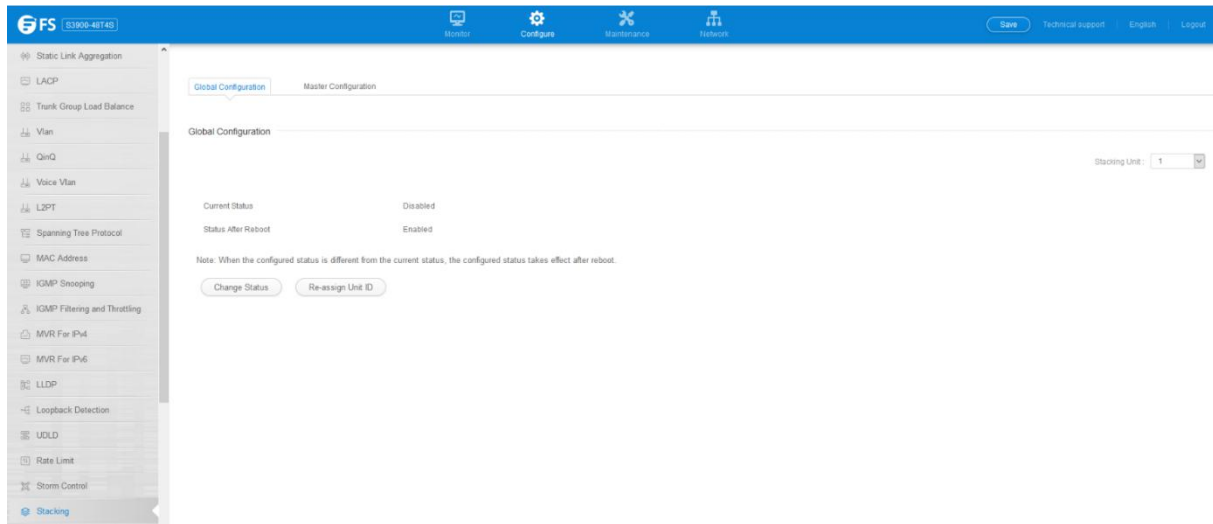
Port	Type	Unknown Unicast Status	Rate (packets/sec) (500-14883000)	Multicast Status	Rate (packets/sec) (500-14883000)	Broadcast Status	Rate (packets/sec) (500-14883000)
1	1000BASE-T	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	500
2	1000BASE-T	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	500
3	1000BASE-T	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	500
4	1000BASE-T	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	500
5	1000BASE-T	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	500
6	1000BASE-T	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	500
7	1000BASE-T	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	500
8	1000BASE-T	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	262143	<input checked="" type="checkbox"/> Enabled	500

4.22 Stacking

4.22.1 Global Configuration

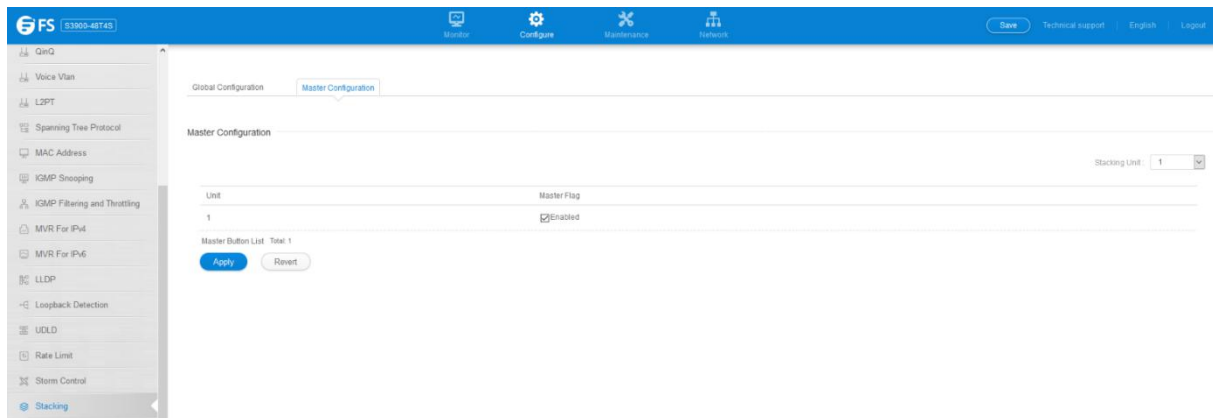
Configure >Stacking >Global Configuration page is used to convert switch mode between stacking and non-stacking and reset unit numbers.

Press Change Status button:



4.22.2 Master Configuration

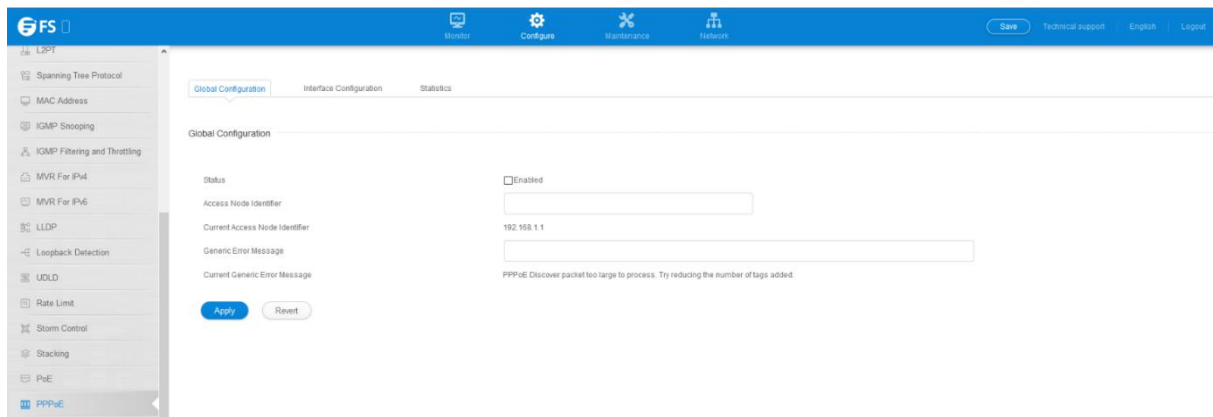
Configure >Stacking >Master Configuration page is used to set master button on the switch.



4.23 PPPoE

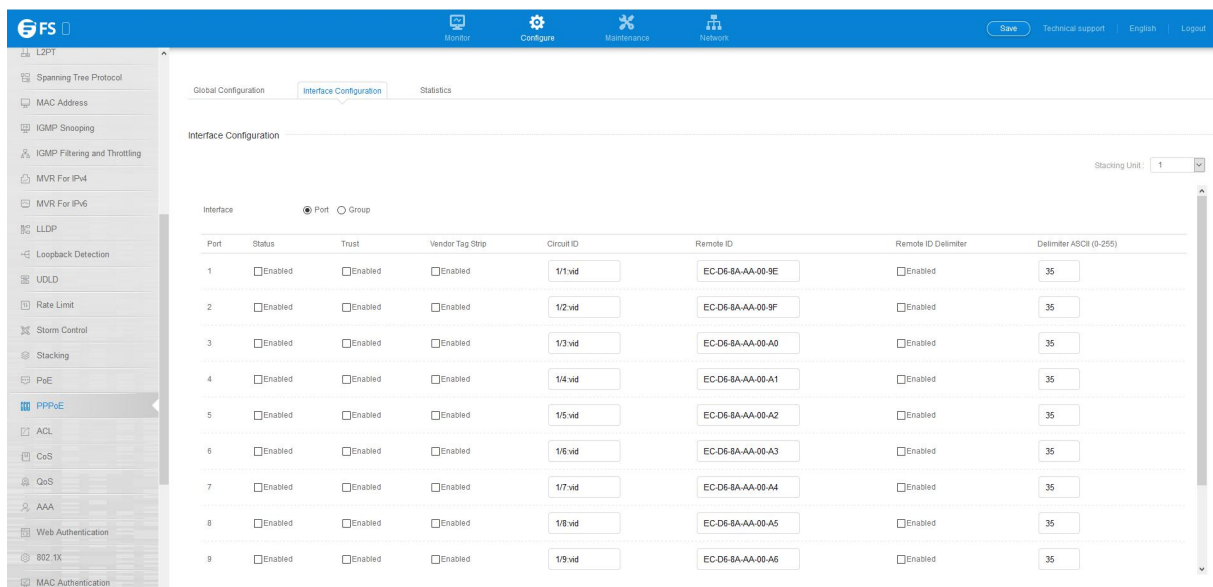
4.23.1 Global Configuration

Configure >PPPoE >Global configuration page is used to set the global configuration of PPPoE.



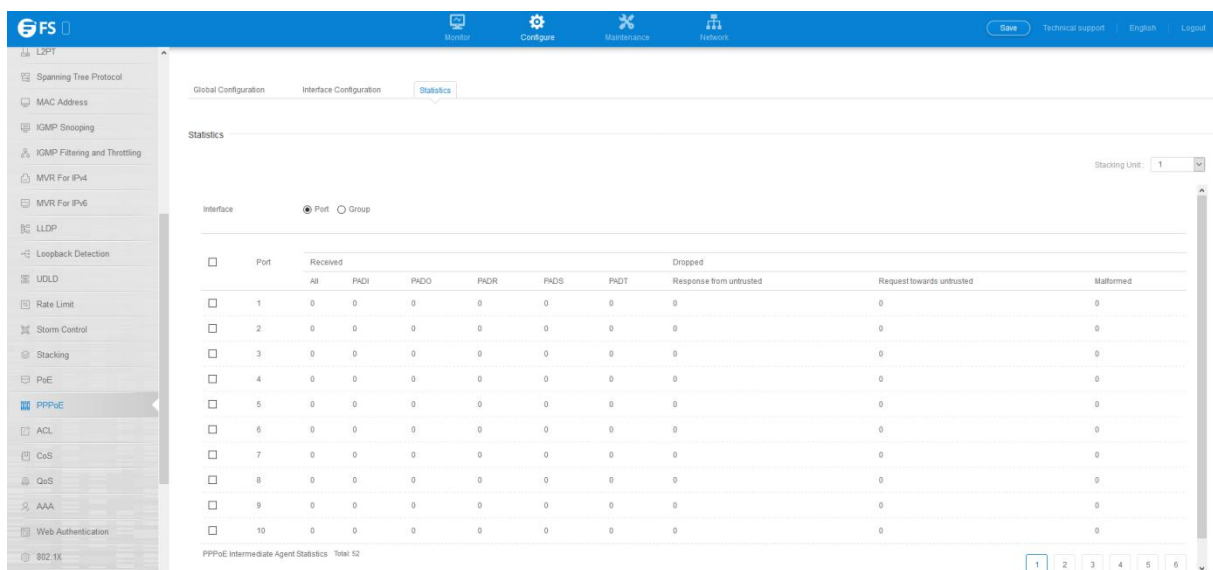
4.23.2 Interface Configuration

Configure > PPPoE > Interface Configuration page is used to set the parameters of interface for PPPoE.



4.23.3 Statistics

Configure > PPPoE > Statistics page is used to display the counters of PPPoE.

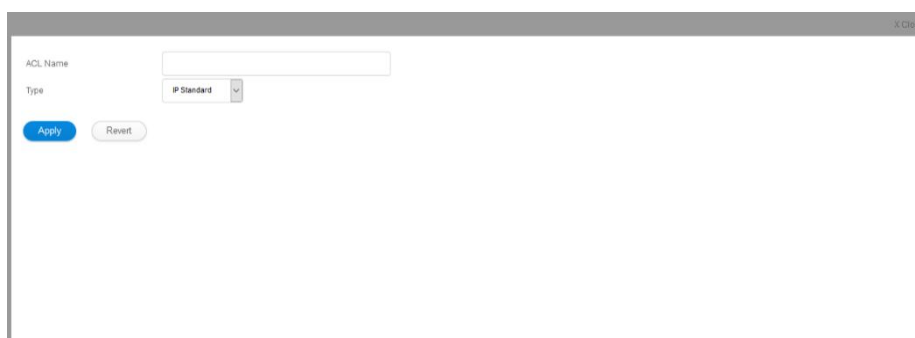
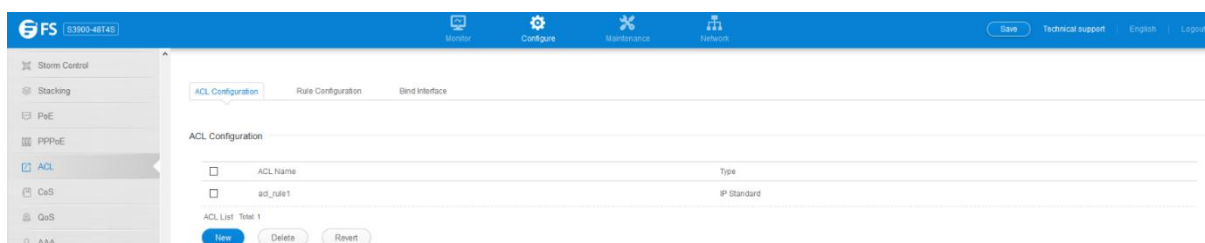


4.24 ACL

4.24.1 ACL Configuration

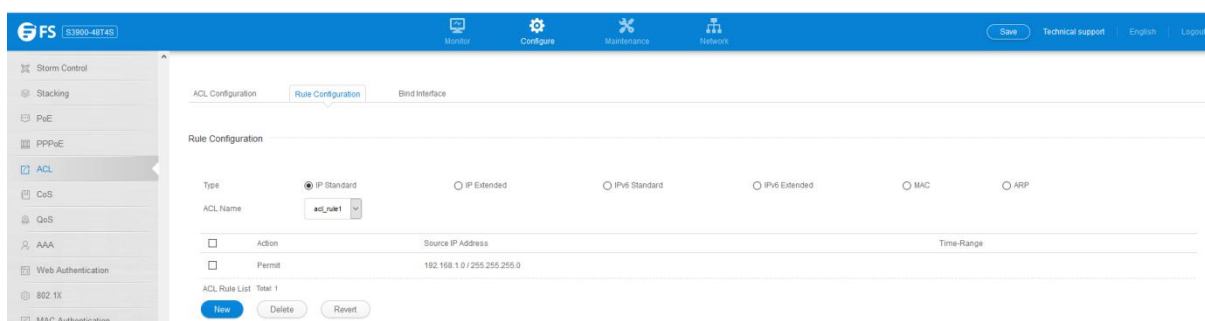
Configure >ACL >ACL Configuration page is used to configure ACL.

- **ACL Name** – Name of the ACL. (Maximum length: 32 characters)
- **Type** – The following filter modes are supported:
 - **IP Standard:** IPv4 ACL mode filters packets based on the source IPv4 address.
 - **IP Extended:** IPv4 ACL mode filters packets based on the source or destination IPv4 address, as well as the protocol type and protocol port number. If the “TCP” protocol is specified, then you can also filter packets based on the TCP control code.
 - **IPv6 Standard:** IPv6 ACL mode filters packets based on the source IPv6 address.
 - **IPv6 Extended:** IPv6 ACL mode filters packets based on the source or destination IP address, as well as DSCP, and the next header type.
 - **MAC** – MAC ACL mode filters packets based on the source or destination MAC address and the Ethernet frame type.
 - **ARP** – ARP ACL specifies static IP-to-MAC address bindings used for ARP inspection.



4.24.2 Rule Configuration

Configure >ACL >Rule Configuration page is used to configure the rule in acl.

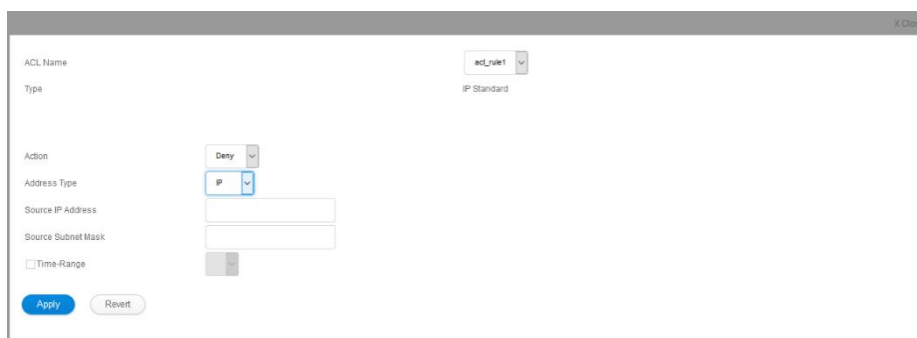


Standard Ipv4 ACL

Configure >ACL >Rule Configuration >IP Standard page is used to configure a Standard IPv4 ACL.

- **ACL Name** – Shows the names of ACLs.

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- **Source IP Address** – Source IP address.
- **Source Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- **Time Range** – Name of a time range.



Extended Ipv4 ACL

Configure > ACL > Rule Configuration > IP Extended page is used to configure an Extended IPv4 ACL.

- **ACL Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Specifies the source or destination IP address type. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Subnet Mask fields.

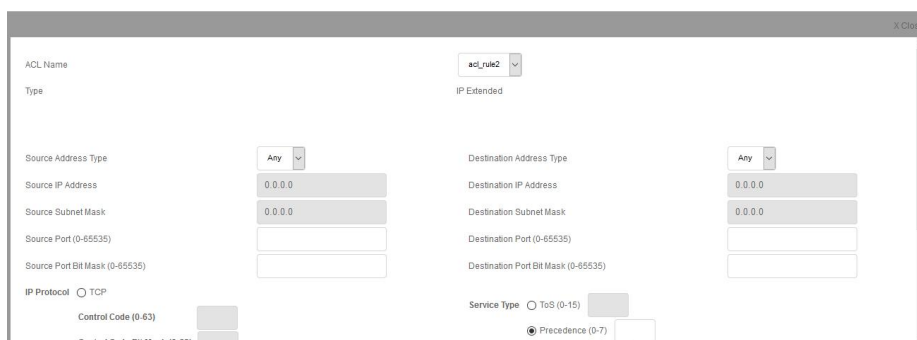
(Options: Any, Host, IP; Default: Any)

- **Source/Destination IP Address** – Source or destination IP address.
- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask.)
- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: Others)
- **Service Type** – Packet priority settings based on the following criteria:
 - **Precedence** – IP precedence level. (Range: 0-7)
 - **DSCP** – DSCP priority level. (Range: 0-63)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bit Mask** – Decimal number representing the code bits to match. (Range: 0-63) The control bit mask is a decimal number (for an equivalent binary bitmask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
 - 1 (fin) – Finish
 - 2 (syn) – Synchronize
 - 4 (rst) – Reset
 - 8 (psh) – Push

- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use control-code 2, control bit mask 2
- Both SYN and ACK valid, use control-code 18, control bit mask 18
- SYN valid and ACK invalid, use control-code 2, control bit mask 18
- **Time Range** – Name of a time range.



The screenshot shows the 'ACL Rule Configuration' window for an 'IP Extended' type ACL. The 'ACL Name' is 'acl_rule2'. The configuration fields include:

- Source Address Type:** Any
- Source IP Address:** 0.0.0.0
- Source Subnet Mask:** 0.0.0.0
- Source Port (0-65535):** (empty)
- Source Port Bit Mask (0-65535):** (empty)
- IP Protocol:** TCP
- Control Code (0-63):** (empty)
- Control Code Bit Mask (0-63):** (empty)
- Destination Address Type:** Any
- Destination IP Address:** 0.0.0.0
- Destination Subnet Mask:** 0.0.0.0
- Destination Port (0-65535):** (empty)
- Destination Port Bit Mask (0-65535):** (empty)
- Service Type:** ToS (0-15) (empty)
- Precedence (0-7):** (empty)

Standard Ipv6 ACL

Configure >ACL >Rule Configuration >IPv6 Standard page is used to configure a Standard IPv6 ACL.

- **ACL Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IPv6-Prefix” to specify a range of addresses.(Options: Any, Host, IPv6-Prefix; Default: Any)
- **Source IPv6 Address** – An IPv6 source address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- **Source Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e.,the network portion of the address). (Range: 0-128 bits)
- **Time Range** – Name of a time range.



The screenshot shows the 'IPv6 Standard' ACL Rule Configuration window. The 'ACL Name' is 'acl_rule3'. The configuration fields include:

- Action:** Permit
- Source Address Type:** Any
- Source IPv6 Address:** (empty)
- Source Prefix Length (0-128):** 0
- Time-Range:** (empty)

Buttons: Apply, Revert

Extended Ipv6 ACL

Configure >ACL >Rule Configuration >IPv6 Extended page is used to configure an Extended IPv6 ACL.

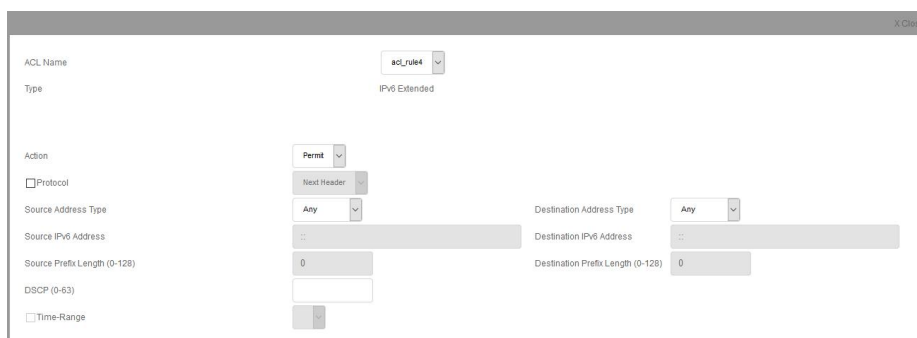
- **ACL Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.

- **Source/Destination Address Type** – Specifies the source or destination IP address type. Use “Any” to include all possible addresses, or “IPv6-Prefix” to specify a range of addresses. (Options: Any, IPv6-Prefix; Default: Any)
- **Source/Destination IPv6 Address** – An IPv6 address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- **Source/Destination Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix, i.e., the network portion of the address. (Range: 0-128 bits for the source address; 0-8 bits for the destination address)
- **DSCP** – DSCP traffic class. (Range: 0-63)
- **Next Header** – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, and includes these commonly used headers:

0 : Hop-by-Hop Options (RFC 2460)
 6 : TCP Upper-layer Header (RFC 1700)
 17 : UDP Upper-layer Header (RFC 1700)
 43 : Routing (RFC 2460)
 44 : Fragment (RFC 2460)
 50 : Encapsulating Security Payload (RFC 2406)
 51 : Authentication (RFC 2402)
 60 : Destination Options (RFC 2460)

- **Time Range** – Name of a time range.



The screenshot shows a web-based configuration window for an ACL rule. The 'ACL Name' is 'acl_rule4'. The 'Type' is 'IPv6 Extended'. The 'Action' is set to 'Permit'. The 'Protocol' checkbox is unchecked. The 'Source Address Type' is 'Any'. The 'Source IPv6 Address' field contains '::'. The 'Source Prefix Length (0-128)' is '0'. The 'DSCP (0-63)' field is empty. The 'Time-Range' checkbox is unchecked. The 'Destination Address Type' is 'Any'. The 'Destination IPv6 Address' field contains '::'. The 'Destination Prefix Length (0-128)' is '0'. There is a 'Next Header' dropdown menu set to 'Next Header'.

Mac ACL

Configure >ACL >Rule Configuration >MAC page is used to configure a MAC ACL based on hardware addresses, packet format, and Ethernet type.

- **ACL Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Bit Mask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination Bit Mask** – Hexadecimal mask for source or destination MAC address.
- **Packet Format** – This attribute includes the following packet types:
 - **Any** – Any Ethernet packet type.
 - **Untagged-eth2** – Untagged Ethernet II packets.

- **Untagged-802.3** – Untagged Ethernet 802.3 packets.
- **Tagged-eth2** – Tagged Ethernet II packets.
- **Tagged-802.3** – Tagged Ethernet 802.3 packets.
- **VID** – VLAN ID. (Range: 1-4094)
- **VID Bit Mask** – VLAN bit mask. (Range: 0-4095)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-ffff hex.) A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- **Ethernet Type Bit Mask** – Protocol bit mask. (Range: 600-ffff hex)
- **CoS** – CoS value. (Range: 0-7)
- **CoS Bit Mask** – CoS bit mask. (Range: 0-7)
- **Time Range** – Name of a time range.



Arp ACL

Configure > ACL > Rule Configuration > ARP page is used to configure ACLs based on ARP message addresses. ARP Inspection can then use these ACLs to filter suspicious traffic.

- **ACL Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Packet Type** – Indicates an ARP request, ARP response, or either type.

(Range: IP, Request, Response; Default: IP)

- **Source/Destination IP Address Type** – Specifies the source or destination IPv4 address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Mask fields.

(Options: Any, Host, IP; Default: Any)

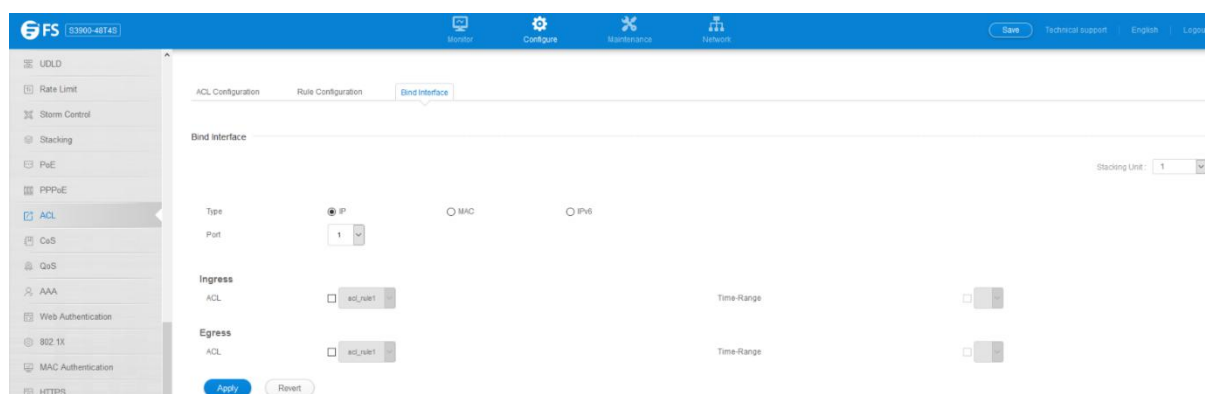
- **Source/Destination IP Address** – Source or destination IP address.
- **Source/Destination IP Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask.)
- **Source/Destination MAC Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Mask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination MAC Bit Mask** – Hexadecimal mask for source or destination MAC address.
- **Log when packet match** – Logs a packet when it matches the access control entry.



4.24.3 Bind Interface

Configure >ACL >Bind Interface page is used to bind the ports that need to filter traffic to the appropriate ACLs. You can assign one IP access list and one MAC access list to any port.

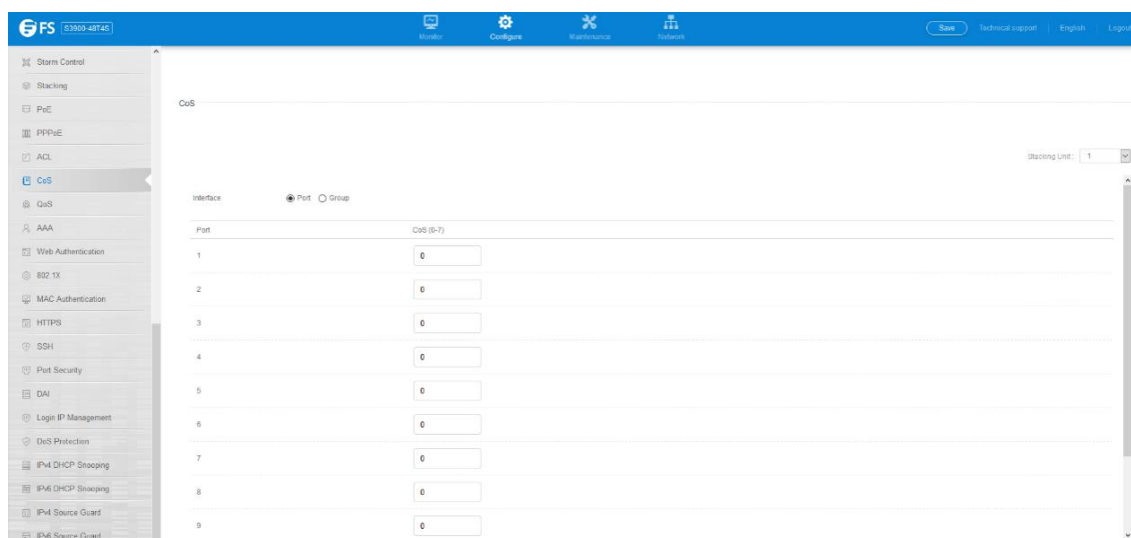
- **Type** – Selects the type of ACLs to bind to a port.
- **Port** – Port identifier.
- **ACL** – ACL used for ingress or egress packets.
- **Time Range** – Name of a time range.



4.25 CoS

Configure >Cos page is used to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

- **Port** – Displays a list of ports or trunks.
- **CoS** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)

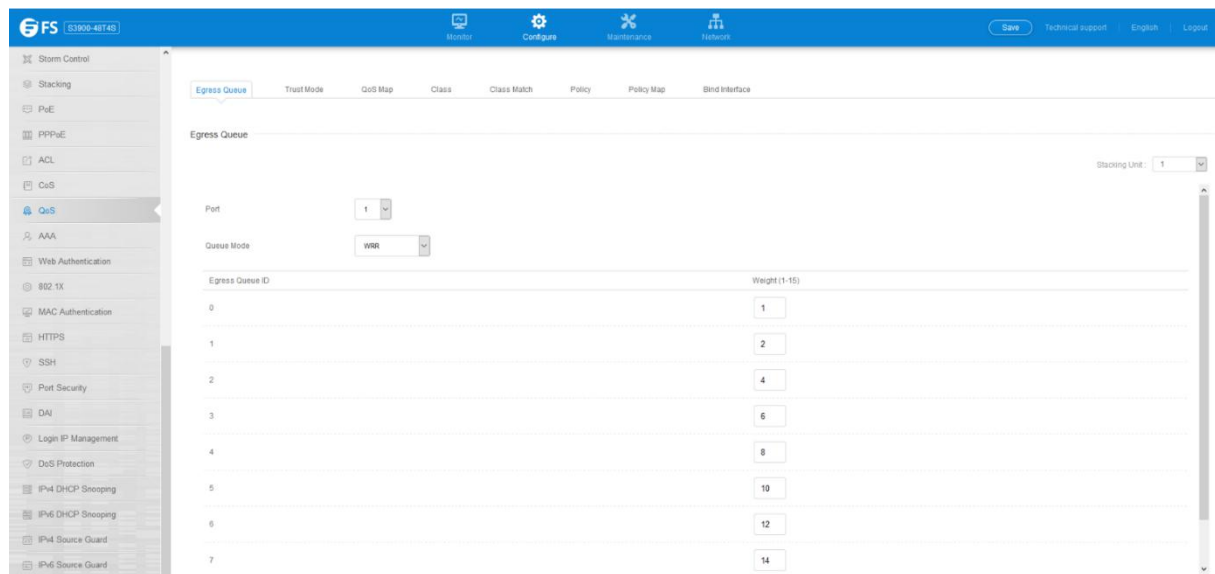


4.26 QoS

4.26.1 Egress Queue

Configure >QoS >Egress Queue page is used to set the queue mode for the egress queues on any interface. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, or Weighted Round-Robin (WRR) queuing which specifies a scheduling weight for each queue. It can also be configured to use a combination of strict and weighted queuing.

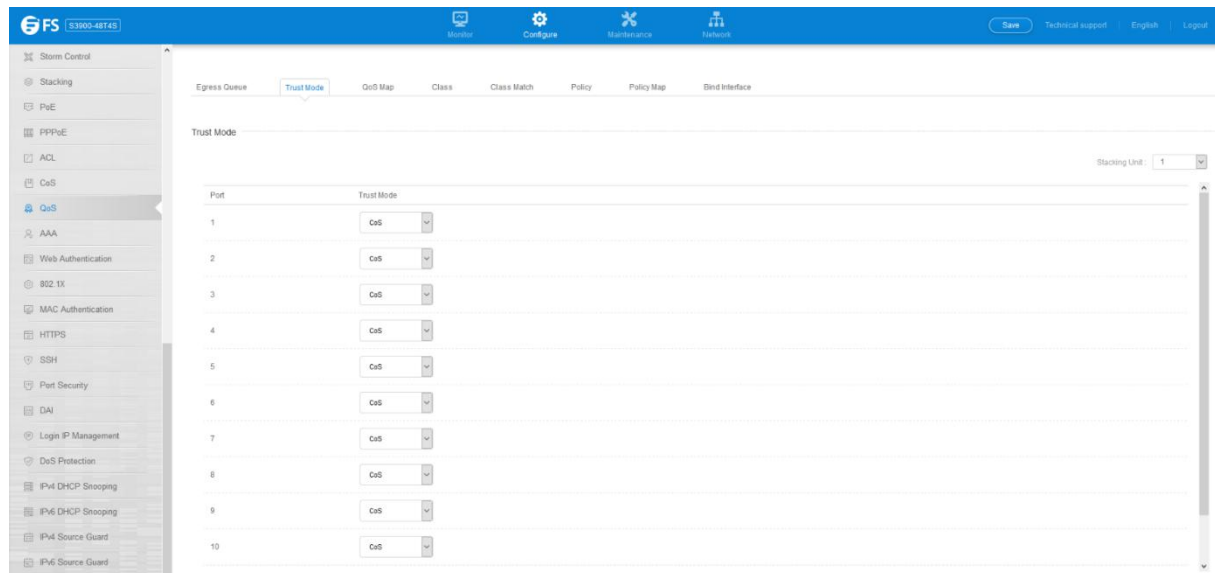
- **Queue Mode**
 - **Strict** – Services the egress queues in sequential order,transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.
 - **WRR** – Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights, and servicing each queue in around-robin fashion. (This is the default setting.)
 - **Strict and WRR** – Uses strict priority on the high-priority queues and WRR on the remaining queues.
- **Queue ID** – The ID of the priority queue. (Range: 0-7)
- **Strict Mode** – If “Strict and WRR” mode is selected, then a combination of strict service is used for the high priority queues and weighted service for the remaining queues. Use this parameter to specify the queues assigned to use strict priority. (Default: Disabled)
- **Weight** – Sets a weight for each queue which is used by the WRR scheduler. (Range: 1-255; Default: Weights 1, 2, 4, 6, 8, 10, 12 and 14are assigned to queues 0 - 7 respectively)



4.26.2 Trust Mode

The switch allows a choice between using DSCP or CoS priority processing methods. Configure >QoS >Trust Mode page is used to select the required processing method.

- **Port** – Port identifier. (Range: 1-28)
- **Trust Mode**
 - **CoS** – Maps layer 3/4 priorities using Class of Service values.(This is the default setting.)
 - **DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point values.



4.26.3 QoS Map

Configure >QoS >QoS Map page is used to map DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing.

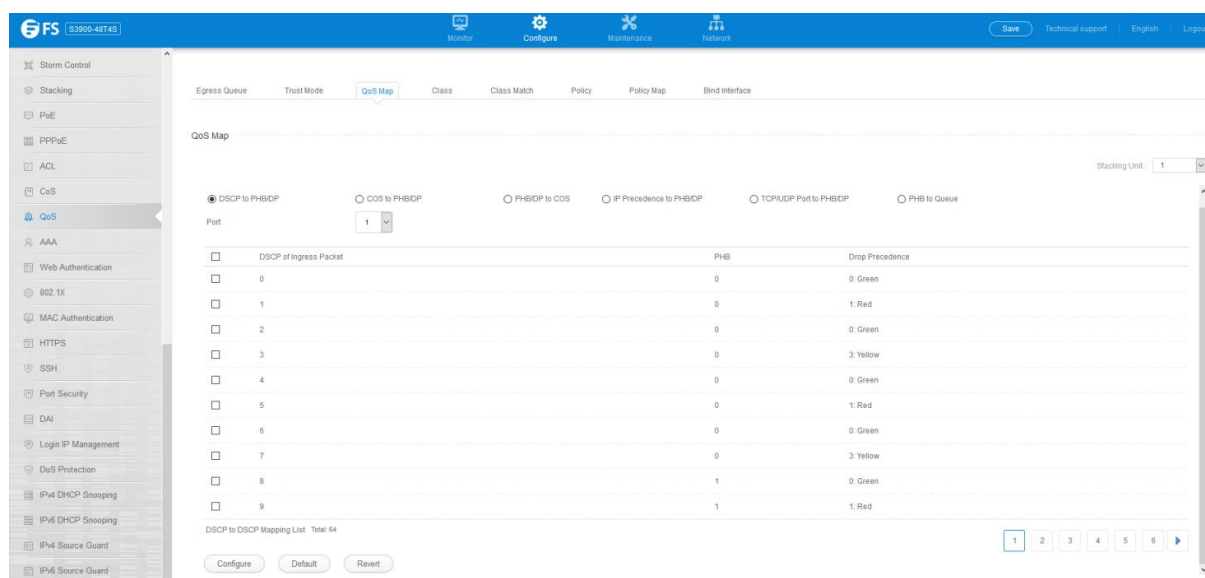
The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

DSCP to PHB/DP

- **Port** – Specifies a port.
- **DSCP** – DSCP value in ingress packets. (Range: 0-63)
- **PHB** – Per-hop behavior, or the priority used for this router hop.(Range: 0-7)
- **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)



To show the DHCP to PHB/DP precedence map:

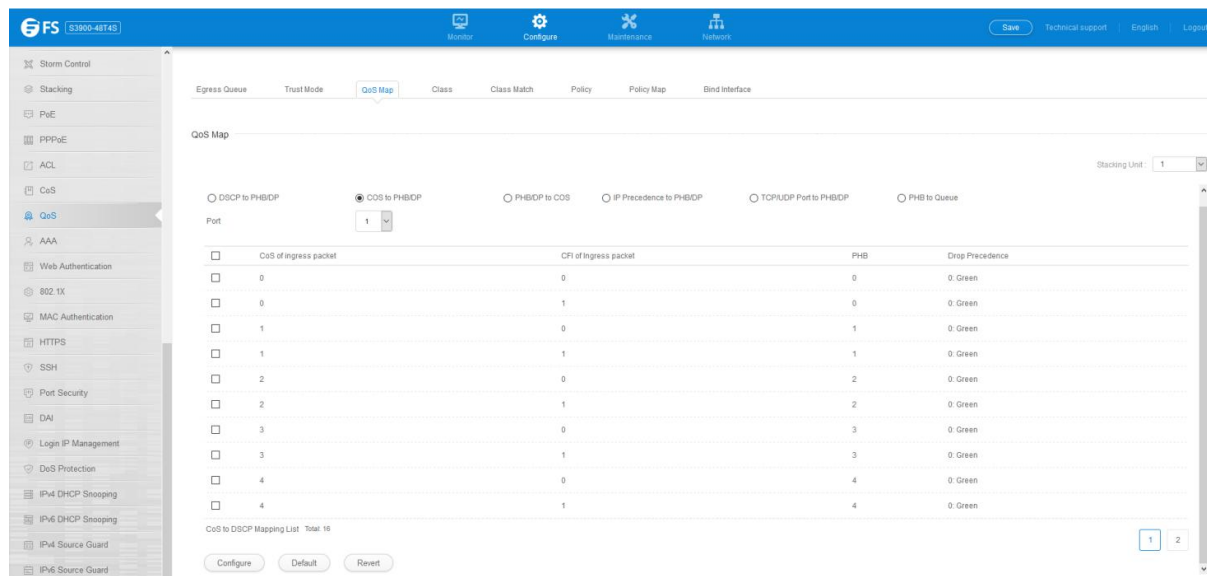


CoS to PHB/DP

- **Port** – Specifies a port.
- **CoS** – CoS value in ingress packets. (Range: 0-7)
- **CFI** – Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)
- **PHB** – Per-hop behavior, or the priority used for this router hop.(Range: 0-7)
- **Drop Precedence** – Drop precedence used in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)



To show the CoS to PHB/DP precedence map:



Port	CoS of ingress packet	CFI of Ingress packet	PHB	Drop Precedence
1	0	0	0	0: Green
1	0	1	0	0: Green
1	1	0	1	0: Green
1	1	1	1	0: Green
1	2	0	2	0: Green
1	2	1	2	0: Green
1	3	0	3	0: Green
1	3	1	3	0: Green
1	4	0	4	0: Green
1	4	1	4	0: Green

PHB/DP to CoS

PHB/DP to CoS page is used to map internal per-hop behavior and drop precedence value pairs to CoS values used in tagged egress packets on a Layer 2 interface.

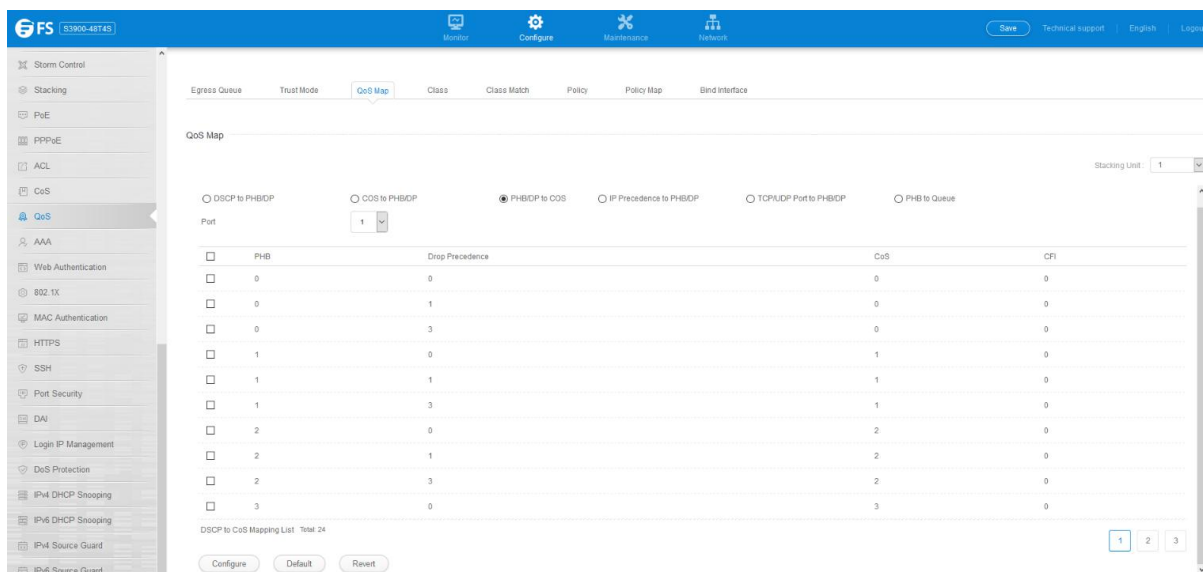
- **Port** – Specifies a port.
- **PHB** – Per-hop behavior, or the priority used for this router hop.

(Range: 0-7)

- **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)
- **CoS** – Class-of-Service value. (Range: 0-7)
- **CFI** – Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)



To show the PHB/DP to CoS precedence map:



IP Precedence to PHB/DP

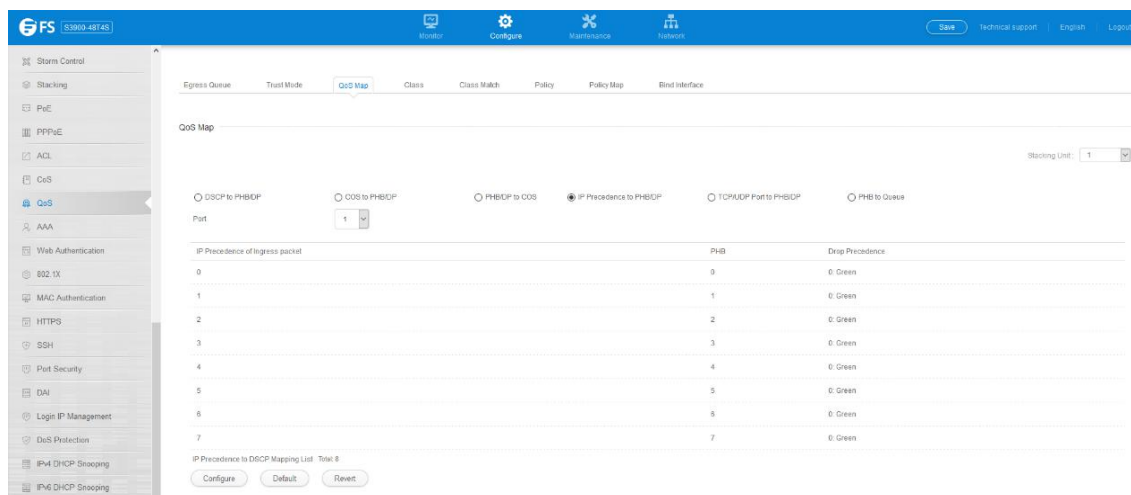
IP Precedence to PHB/DP page is used to map IP precedence values in incoming packets to per-hop behavior and drop precedence values for priority processing.

- **Port** – Specifies a port.
- **IP Precedence** – IP Precedence value in ingress packets. (Range: 0-7)
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

IP Precedence Value	0	1	2	3	4	5	6	7
Per-hop Behavior	0	1	2	3	4	5	6	7
Drop Precedence	0	0	0	0	0	0	0	0



To show the IP Precedence to PHB/DP precedence map:



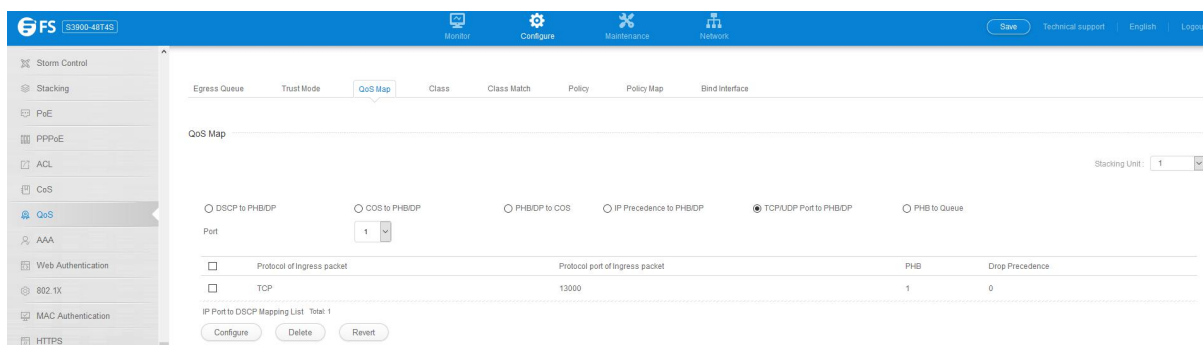
TCP/UDP Port to DSCP

TCP/UDP Port to DSCP page is used to map network applications designated by a TCP/UDP destination port number in the frame header to per-hop behavior and drop precedence values for internal priority processing.

- **Port** – Specifies a port.
- **IP Protocol**
 - **TCP** – Transport Control Protocol
 - **UDP** – User Datagram Protocol
- **Destination Port Number** – 16-bit TCP/UDP destination port number. (Range: 0-65535)
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)



To show the TCP/UDP Port to DSCP precedence map:



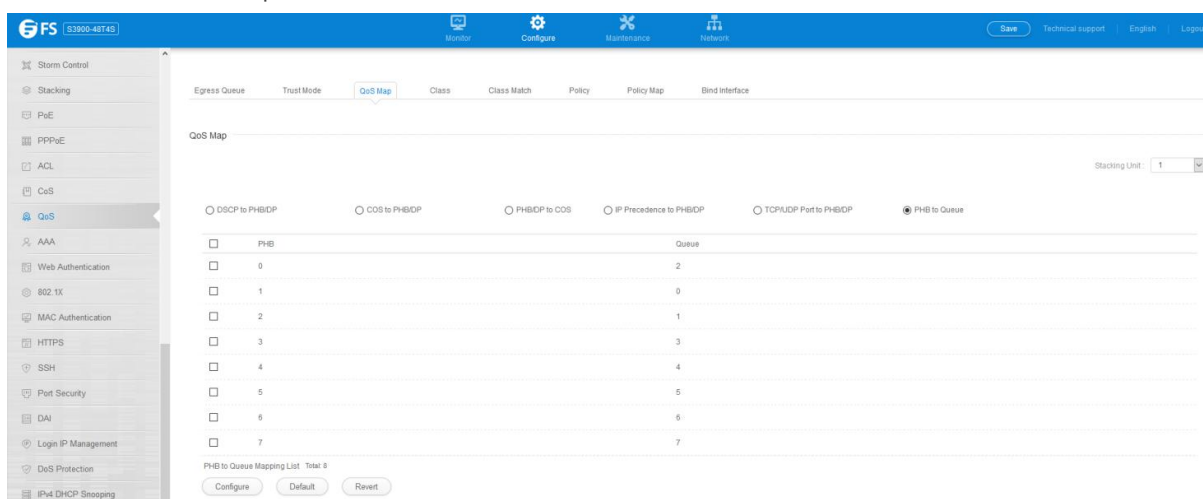
PHB to Queue

PHB to Queue page is used to specify the hardware output queues to use based on the internal per-hop behavior value.

- **PHB** – Per-hop behavior, or the priority used for this router hop.(Range: 0-7, where 7 is the highest priority)
- **Queue** – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)



To show the PHB to Queue map:



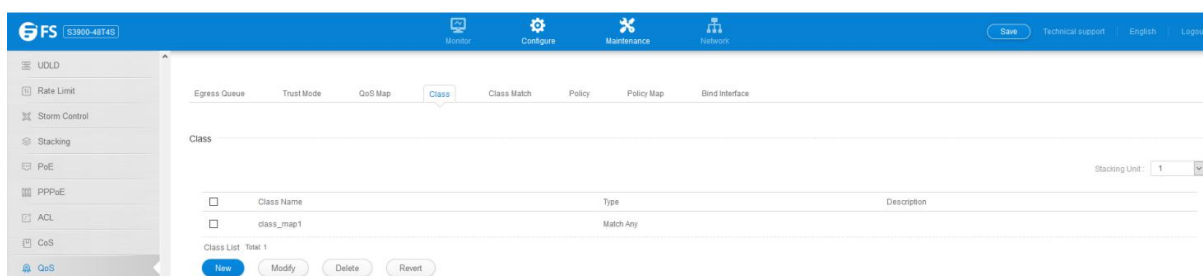
PHB	Queue
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

4.26.4 Class

A class map is used for matching packets to a specified class. Configure >QoS >Class page is used to configure a class map.

Add

- **Class Name** – Name of the class map. (Range: 1-32 characters)
- **Type** – The criteria specified by the match command.
 - **Match Any** – Match any condition within a class map.
- **Description** – A brief description of a class map. (Range: 1-64characters)



Class Name	Type	Description
class_map1	Match Any	



4.26.5 Class Match

To edit the rules for a class map:



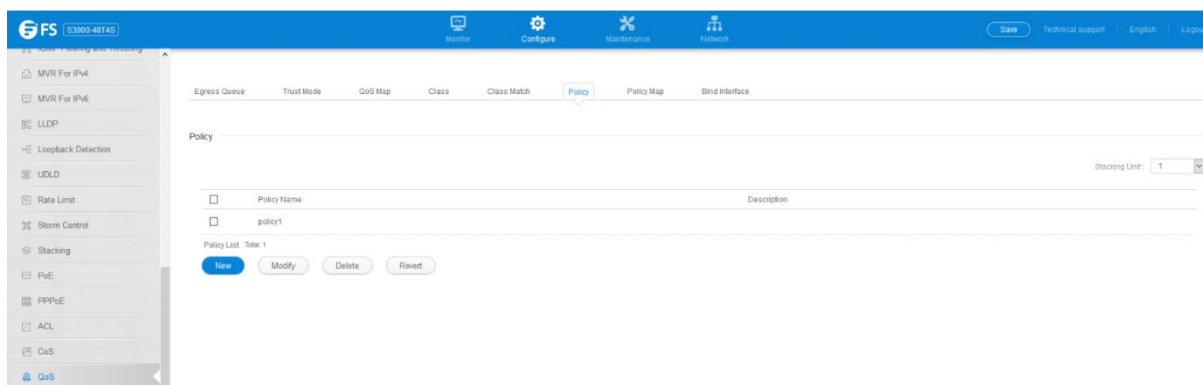
4.26.6 Policy

Configure > QoS > Policy page is used to create a policy map that can be attached to multiple interfaces. A policy map is used to group one or more class map statements, modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces.

Add

- **Policy Name** – Name of policy map. (Range: 1-32 characters)
- **Description** – A brief description of a policy map. (Range: 1-256 characters)

Add Rule



4.26.7 Policy Map

- **Policy Name** – Name of policy map.
- **Bound Class Name** – Name of a class map that defines a traffic classification upon which a policy can act.
- **Action** – This attribute is used to set an internal QoS value in hardware for matching packets. The PHB label is composed of five

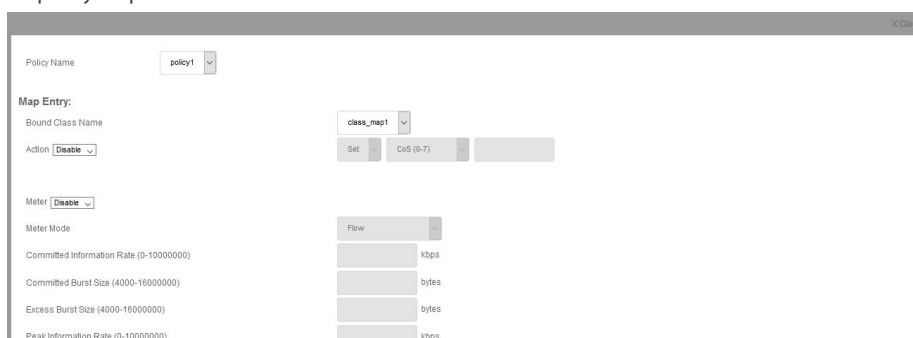
bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion with the srTCM and trTCM metering functions.

- **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
- **Meter Mode** – Selects one of the following policing methods.
- **Committed Information Rate (CIR)** – Rate in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)The rate cannot exceed the configured interface speed.
- **Committed Burst Size (BC)** – Burst in bytes.(Range: 64-16000000 at a granularity of 4k bytes)The burst size cannot exceed 16 Mbytes.
- **Excess Burst Size (BE)** – Burst in excess of committed burst size. (Range: 0-16000000 at a granularity of 4k bytes).The burst size cannot exceed 16 Mbytes.
- **Peak Information Rate (PIR)** – Rate in kilobits per second.(Range: 0-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower).

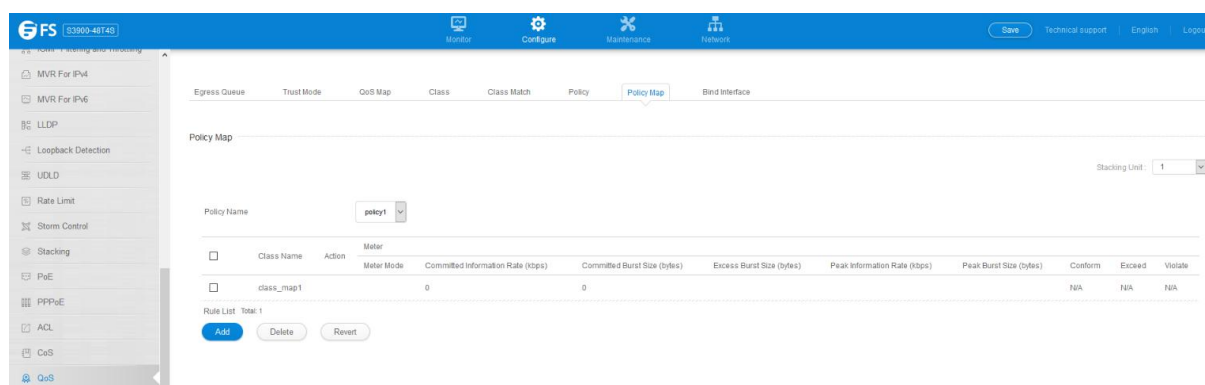
The rate cannot exceed the configured interface speed.

- **Peak Burst Size (BP)** – Burst size in bytes.(Range: 0-16000000 at a granularity of 4k bytes).The burst size cannot exceed 16 Mbytes.
- **Action for Conform**– Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.
- **Action for Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the excess burst size (BE) will be dropped or the DSCP service level will be reduced.
- **Action for Violate** – Specifies whether the traffic that exceeds the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

To edit the rules for a policy map:



To show the rules for a policy map:



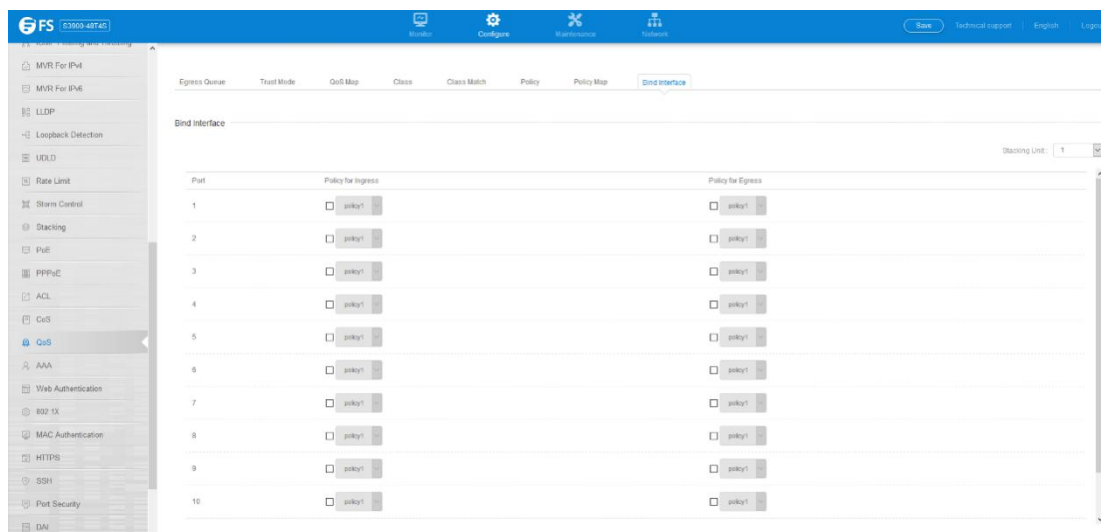
Class Name	Action	Meter	Meter Mode	Committed Information Rate (kbps)	Committed Burst Size (bytes)	Excess Burst Size (bytes)	Peak Information Rate (kbps)	Peak Burst Size (bytes)	Conform	Exceed	Violate
class_map1				0	0				N/A	N/A	N/A

4.26.8 Bind Interface

Configure >QoS >Bind Interface page is used to bind a policy map to a port.First define a class map, define a policy map, and bind the

service policy to the required interface.

- **Port** – Specifies a port.
- **Policy for Ingress**– Applies the selected rule to ingress traffic.
- **Policy for Egress**– Applies the selected rule to egress traffic.



4.27 AAA

4.27.1 Global Configuration

Configure > AAA > Global Configuration page to set global configuration.

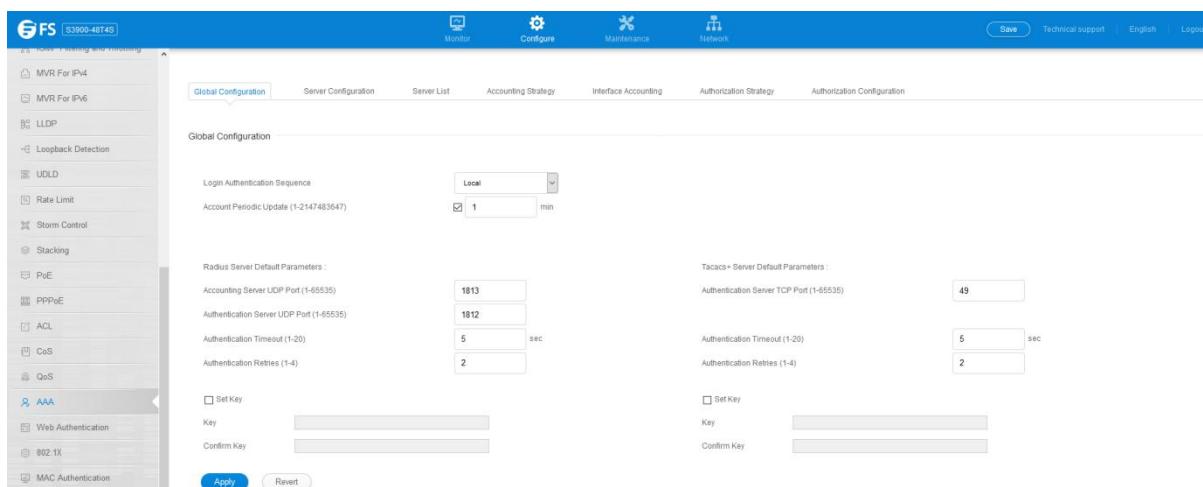
- **Authentication Sequence** –set the sequence of authentication. There are three method of authentication.

Local – User authentication is performed only locally by the switch.

RADIUS – User authentication is performed using a RADIUS server only.

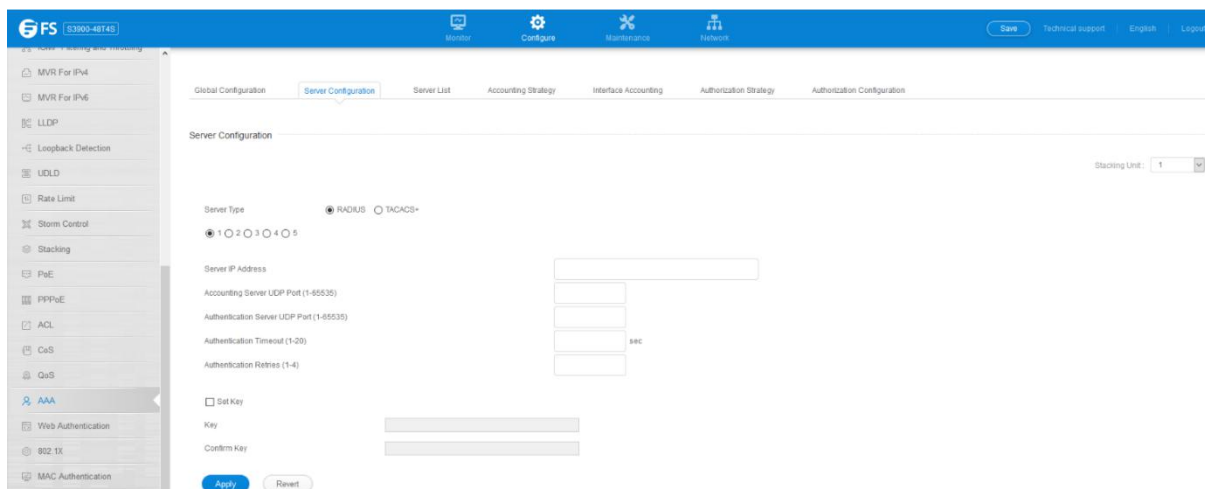
TACACS – User authentication is performed using a TACACS+ server only.

- **Radius Server Default Parameters:** if a radius server do not set these parameters, the default parameter will active.
- **Tacacs+ Server Default Parameters:** if the tacacs+ server do not set these parameters, the default parameter will active.



4.27.2 Server Configuration

Configure >AAA >Server configuration page is used to configure the parameters of RADIUS or TACACS+ server for AAA:



Global Configuration | **Server Configuration** | Server List | Accounting Strategy | Interface Accounting | Authorization Strategy | Authorization Configuration

Stacking Unit: 1

Server Type: ☒ RADIUS ☐ TACACS+

Server IP Address:

Accounting Server UDP Port (1-65535):

Authentication Server UDP Port (1-65535):

Authentication Timeout (1-20):

Authentication Retries (1-4):

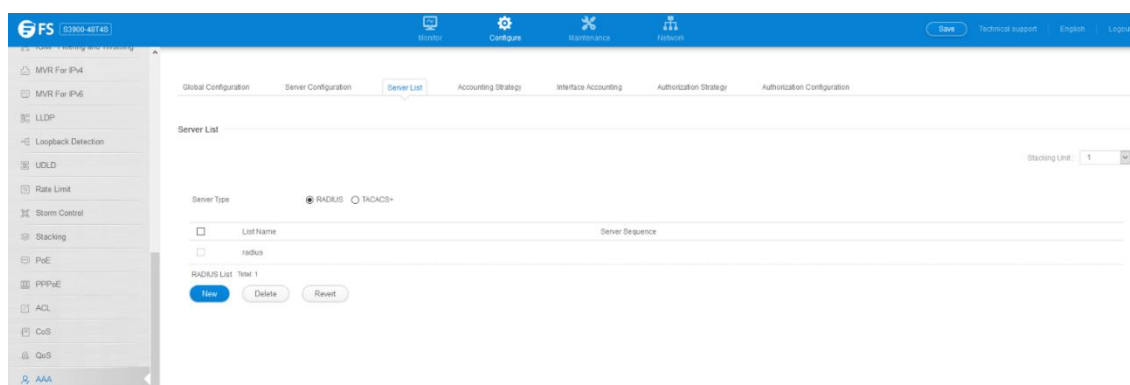
☐ Set Key

Key:

Confirm Key:

4.27.3 Server List

Configure >AAA >Server List page is used to configure the RADIUS or TACACS+ server groups to use for accounting and authorization:
Server list include a list of servers.



Global Configuration | Server Configuration | **Server List** | Accounting Strategy | Interface Accounting | Authorization Strategy | Authorization Configuration

Stacking Unit: 1

Server Type: ☒ RADIUS ☐ TACACS+

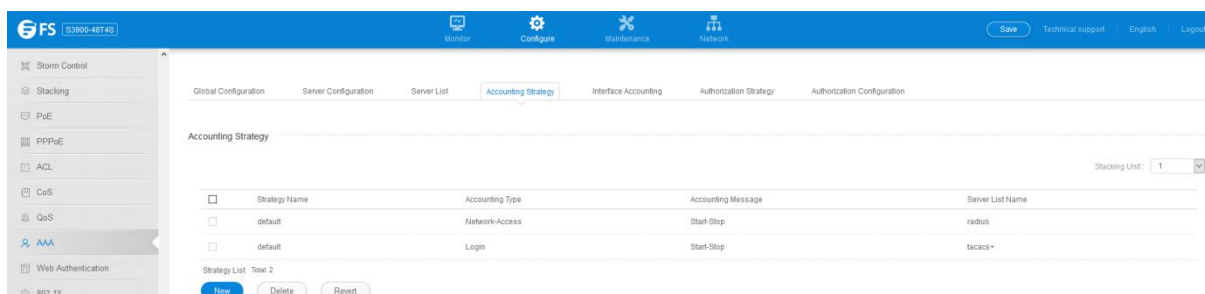
☐ List Name: Server Sequence:

☐ radius

RADIUS List: New 1

4.27.4 Accounting Strategy

Configure >AAA >Accounting Strategy page is used to configure the strategy for Accounting.



Global Configuration | Server Configuration | Server List | **Accounting Strategy** | Interface Accounting | Authorization Strategy | Authorization Configuration

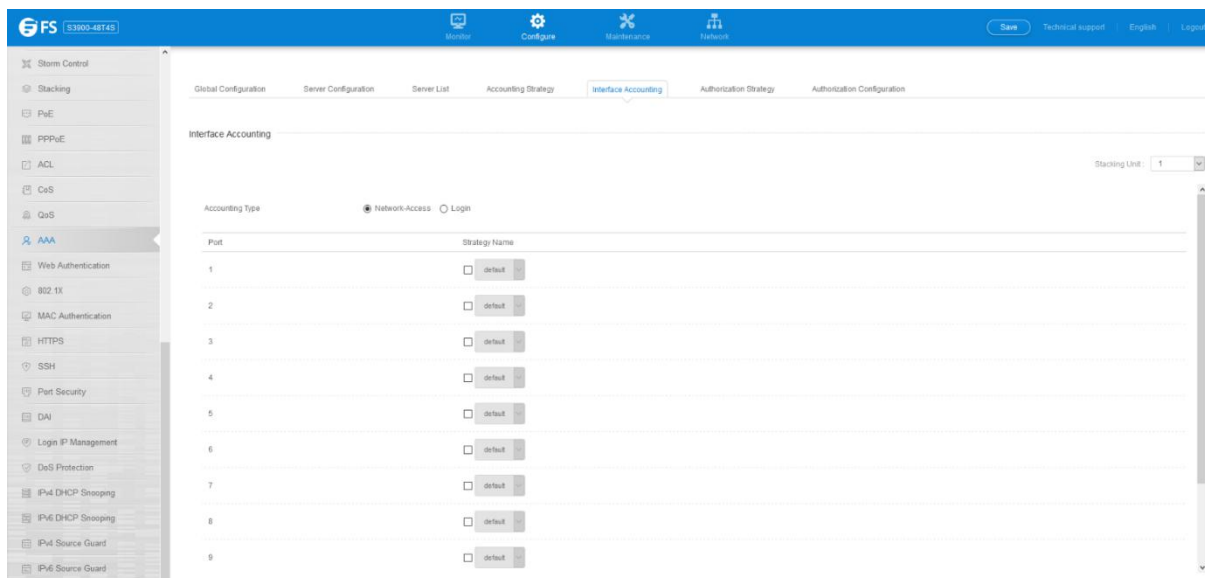
Stacking Unit: 1

Strategy Name	Accounting Type	Accounting Message	Server List Name
default	Network-Access	Start-Stop	radius
default	Login	Start-Stop	tacacs+

Strategy List: Total 2

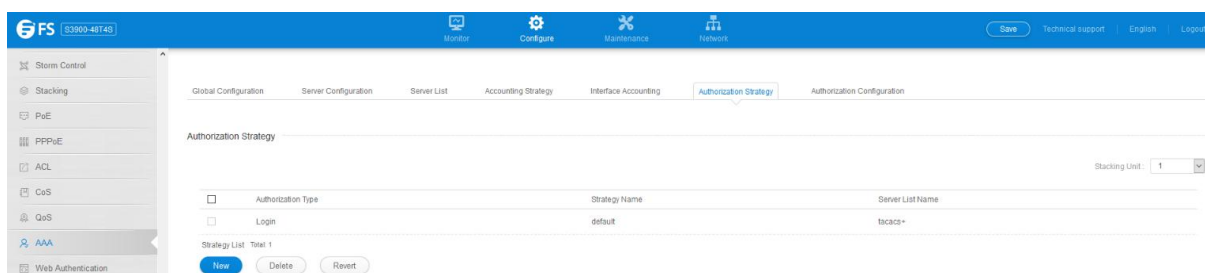
4.27.5 Interface Accounting

Configure >AAA >Interface Accounting page is used to configure the strategy used on the interface.



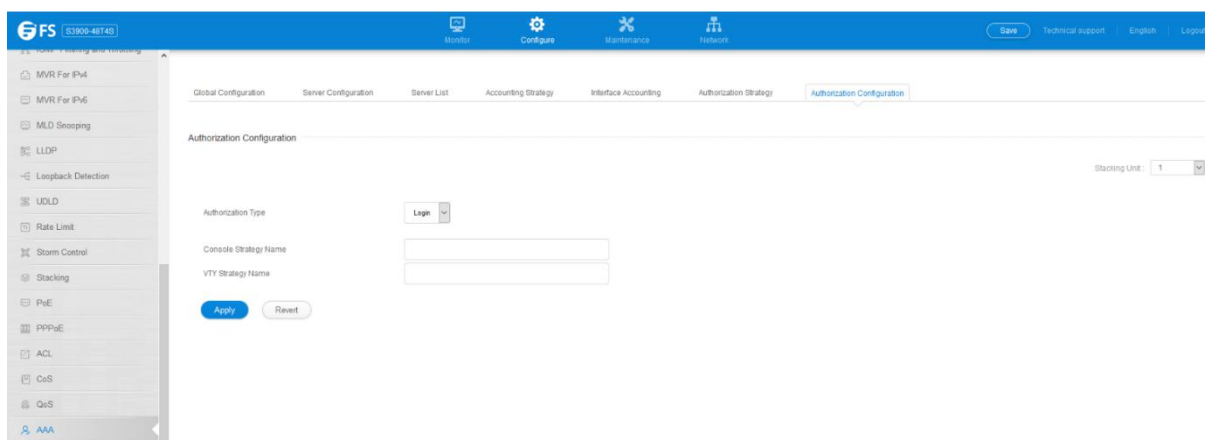
4.27.6 Authorization Strategy

Configure >AAA >Authorization Strategy page is used to configure the strategy for authorization.



4.27.7 Authorization Configuration

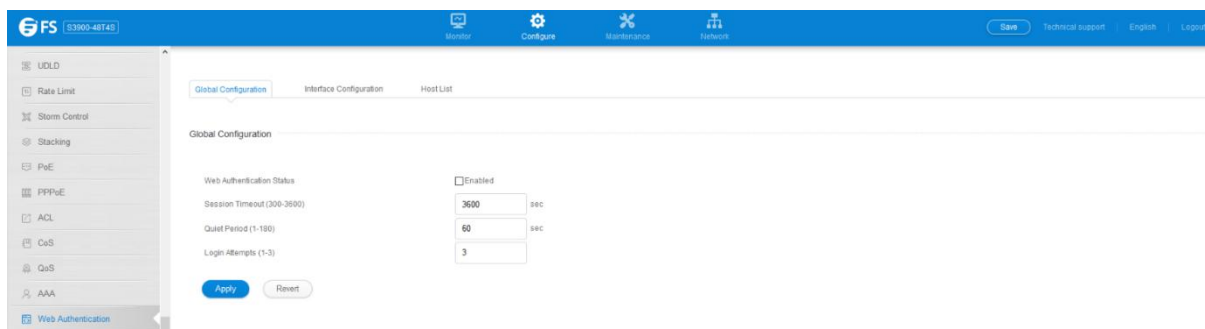
Configure >AAA >Authorization Configuration page is used to configure the authorization strategy for console login and vty(telnet,ssh) login.



4.28 Web Authentication

4.28.1 Global Configuration

Configure > Web Authentication > Global Configuration page is used to edit the global parameters for web authentication.

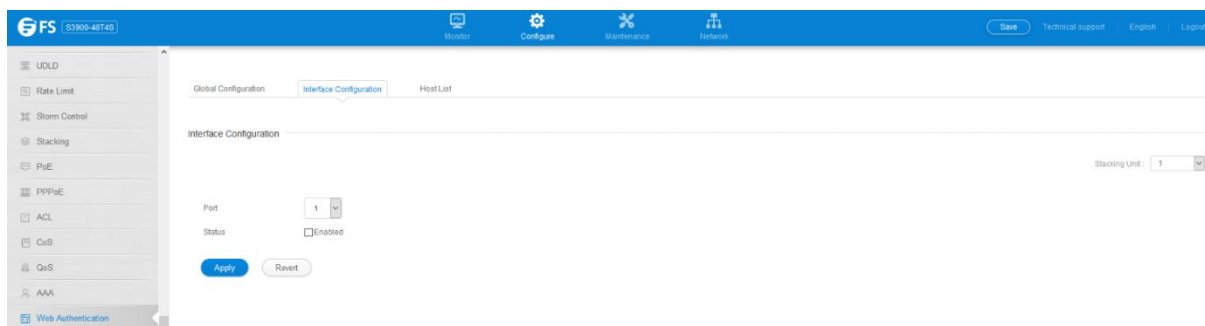


The screenshot shows the 'Global Configuration' page for Web Authentication. The left sidebar contains a tree view with 'Web Authentication' selected. The main content area has three tabs: 'Global Configuration', 'Interface Configuration', and 'Host List'. Under 'Global Configuration', there are four settings: 'Web Authentication Status' (checkbox, checked), 'Session Timeout (300-3600)' (input field with 3600, unit sec), 'Quiet Period (1-180)' (input field with 60, unit sec), and 'Login Attempts (1-3)' (input field with 3). At the bottom are 'Apply' and 'Revert' buttons.

- **Web Authentication Status** – Enables web authentication for the switch. (Default: Disabled) Note that this feature must also be enabled for any port where required under the Configure Interface menu.
- **Session Timeout** – Configures how long an authenticated session stays active before it must re-authenticate itself. (Range: 300-3600 seconds; Default: 3600 seconds)
- **Quiet Period** – Configures how long a host must wait to attempt authentication again after it has exceeded the maximum allowable failed login attempts. (Range: 1-180 seconds; Default: 60 seconds)
- **Login Attempts** – Configures the amount of times a supplicant may attempt and fail authentication before it must wait the configured quiet period. (Range: 1-3 attempts; Default: 3 attempts)

4.28.2 Interface Configuration

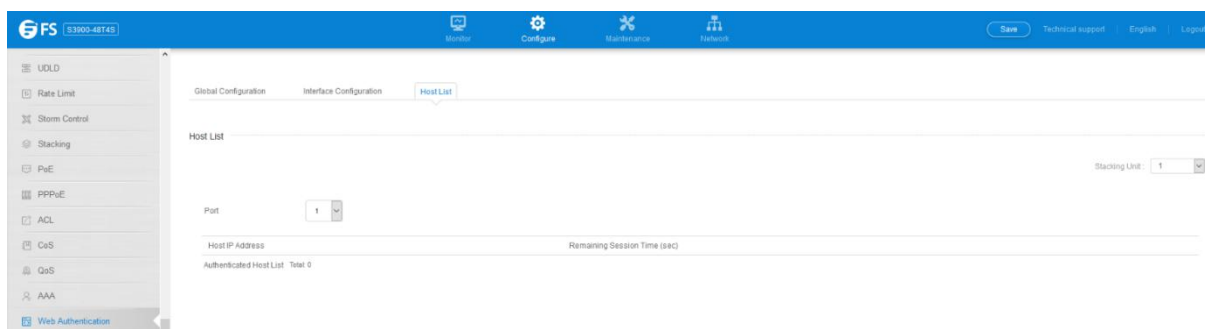
Configure > Web Authentication > Interface Configuration page is used to configure the interface.



The screenshot shows the 'Interface Configuration' page for Web Authentication. The left sidebar is the same as the previous page. The main content area has the same three tabs. Under 'Interface Configuration', there are three settings: 'Port' (dropdown menu with 1 selected), 'Status' (checkbox, checked), and 'Stacking Unit' (input field with 1, unit sec). At the bottom are 'Apply' and 'Revert' buttons.

4.28.3 Host List

Configure > Web Authentication > Host List page is used to show the Host information.

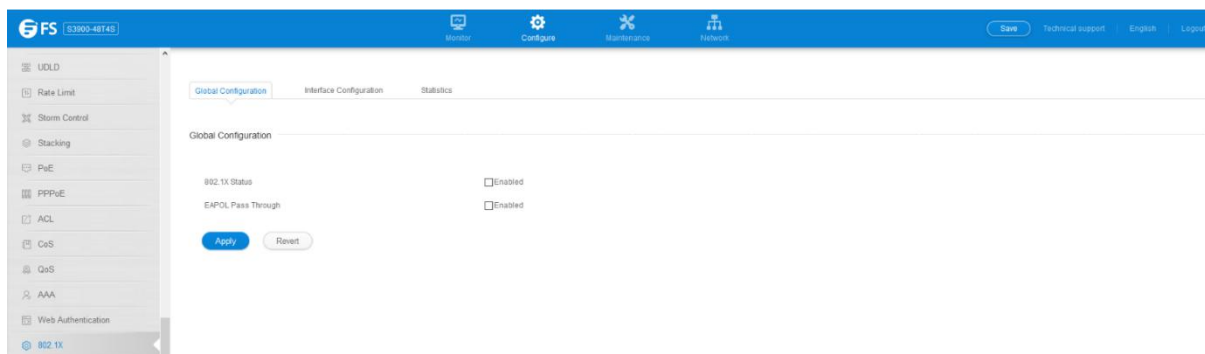


The screenshot shows the 'Host List' page for Web Authentication. The left sidebar is the same. The main content area has the same three tabs. Under 'Host List', there is a table with two columns: 'Host IP Address' and 'Remaining Session Time (sec)'. The table is currently empty. At the bottom, there is a 'Port' dropdown menu with 1 selected and a 'Stacking Unit' input field with 1. There are also 'Apply' and 'Revert' buttons.

4.29 802.1X

4.29.1 Global Configuration

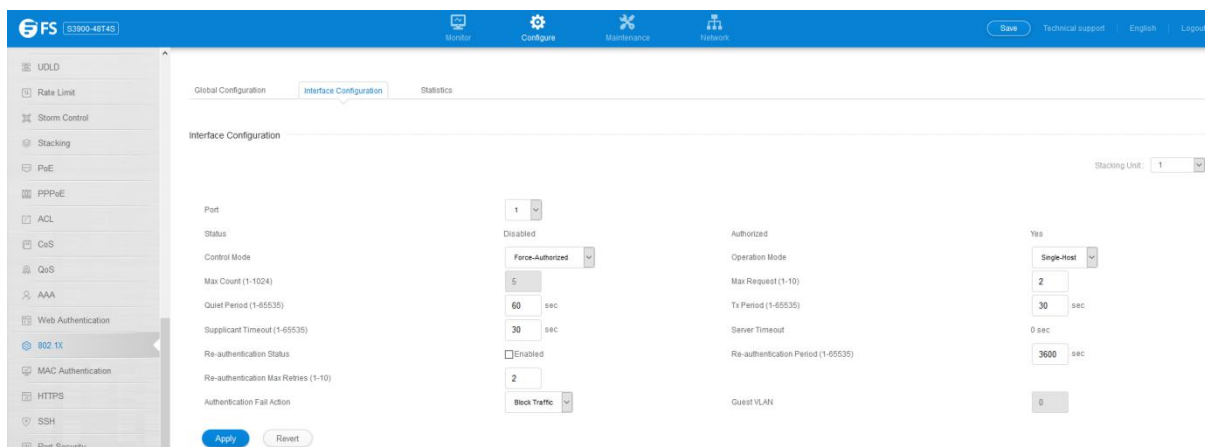
Configure >802.1x >Global Configuration page is used to configure the global parameter of 802.1x.



- 802.1X Status– Sets the global setting for 802.1X. (Default: Disabled)
- EAPOL Pass Through – Passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. (Default: Disabled)

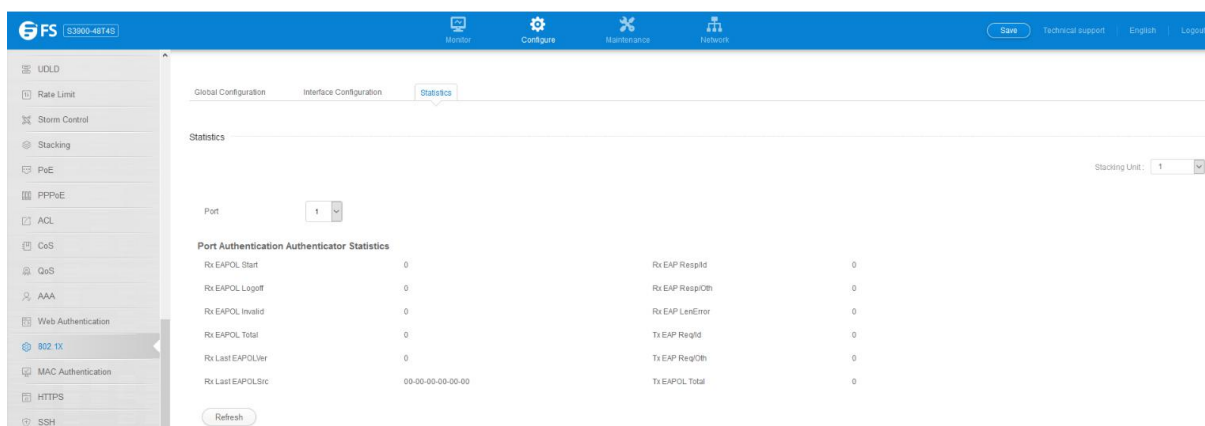
4.29.2 Interface Configuration

Configure >802.1x >Interface Configuration page is used to configure the parameters of a port.



4.29.3 Statistics

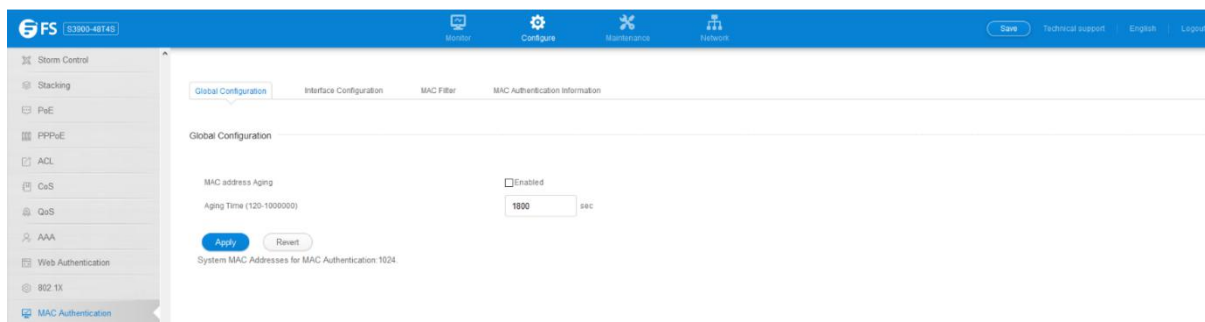
Configure >802.1x >Statistics page is used to display the statistics of 802.1x.



4.30 MAC Authentication

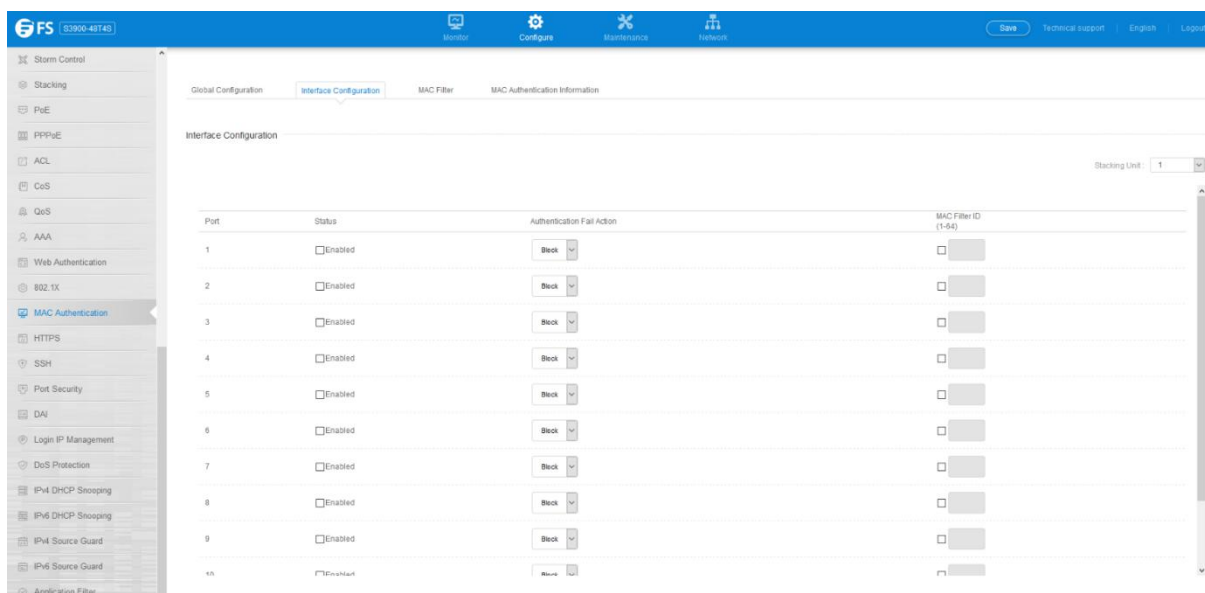
4.30.1 Global Configuration

Configure >MAC Authentication >Global Configuration page is used to configure MAC Authentication global.



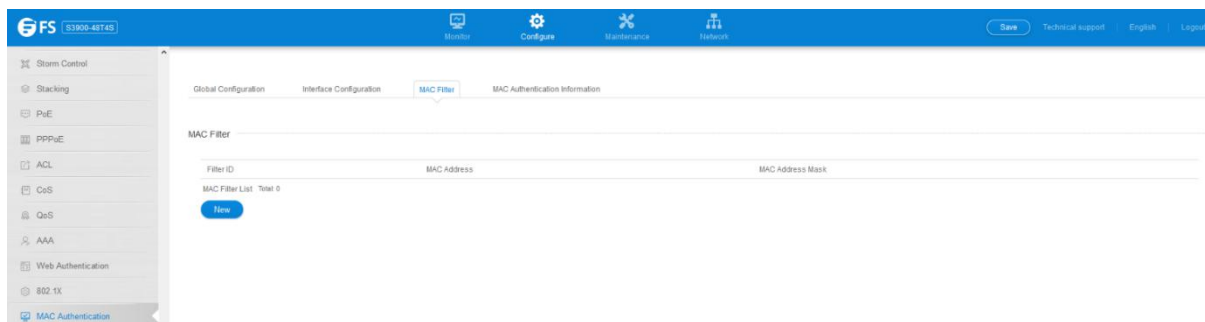
4.30.2 Interface Configuration

Configure >MAC Authentication >Interface Configuration page is used to configure interface.



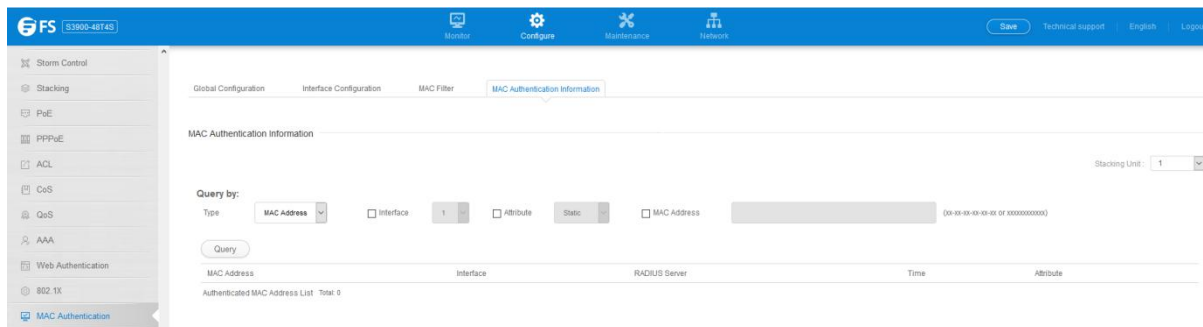
4.30.3 MAC Filter

Configure >MAC Authentication >MAC Filter page is used to configure Mac Filter.



4.30.4 MAC Authentication Information

Configure > MAC Authentication > MAC Authentication Information page is used to show information of MAC Authentication.

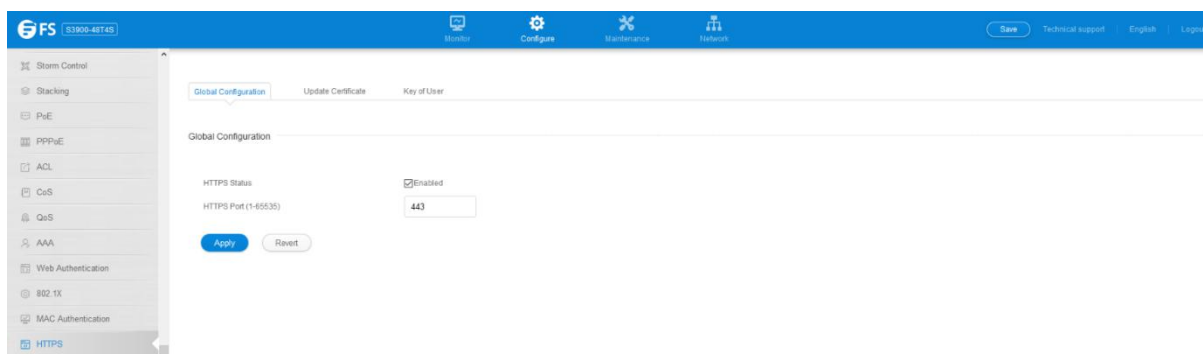


4.31 HTTPS

4.31.1 Global Configuration

Configure > HTTPS > Global Configuration page is used to enable or disable HTTPS and specify the UDP port used for this service.

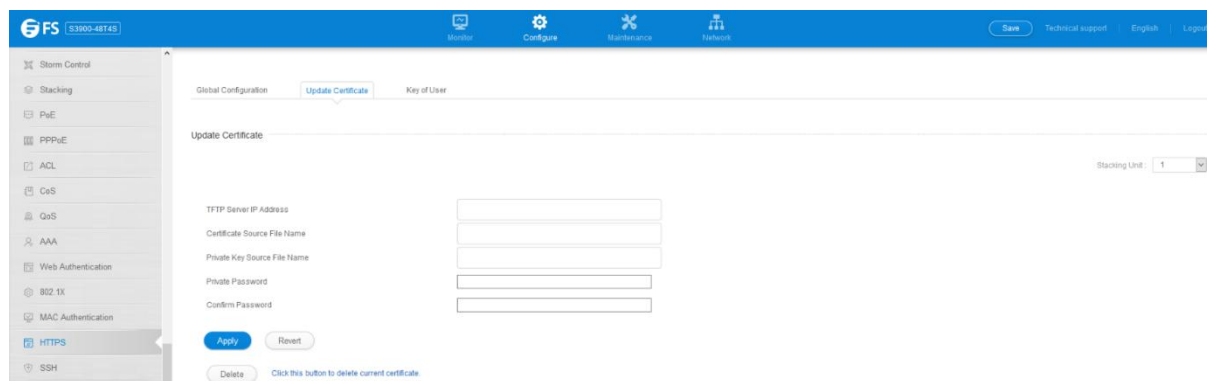
- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- **HTTPS Port** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)



4.31.2 Update Certificate

Configure > HTTPS > Update Certificate page is used to replace the default secure-site certificate.

- **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.
- **Certificate Source File Name** – Name of certificate file stored on the TFTP server.
- **Private Key Source File Name** – Name of private key file stored on the TFTP server.
- **Private Password** – Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.
- **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not download the certificate if these two fields do not match.

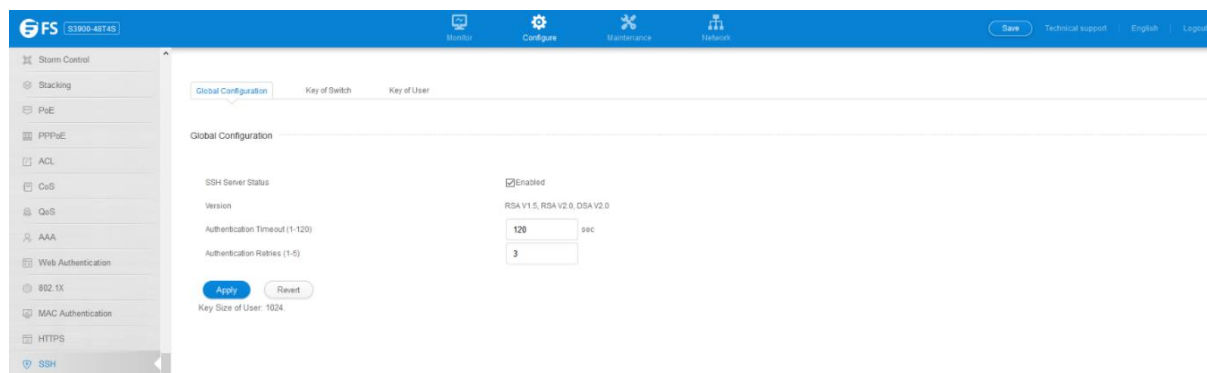


4.32 SSH

4.32.1 Global Configuration

Configure > SSH > Global Configuration page is used to enable the SSH server and configure basic settings for authentication.

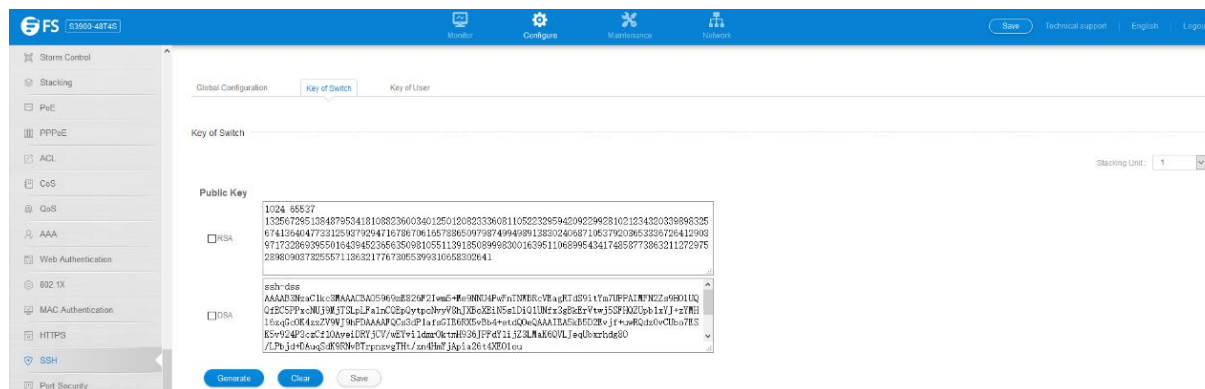
- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)
- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- **Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1-120 seconds; Default: 120 seconds)
- **Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)
- The host key is shared with the SSH client, and is fixed at 1024 bits.



4.32.2 Key of Switch

Configure > SSH > Key of Switch page is used to generate a host public/private key pair used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch.

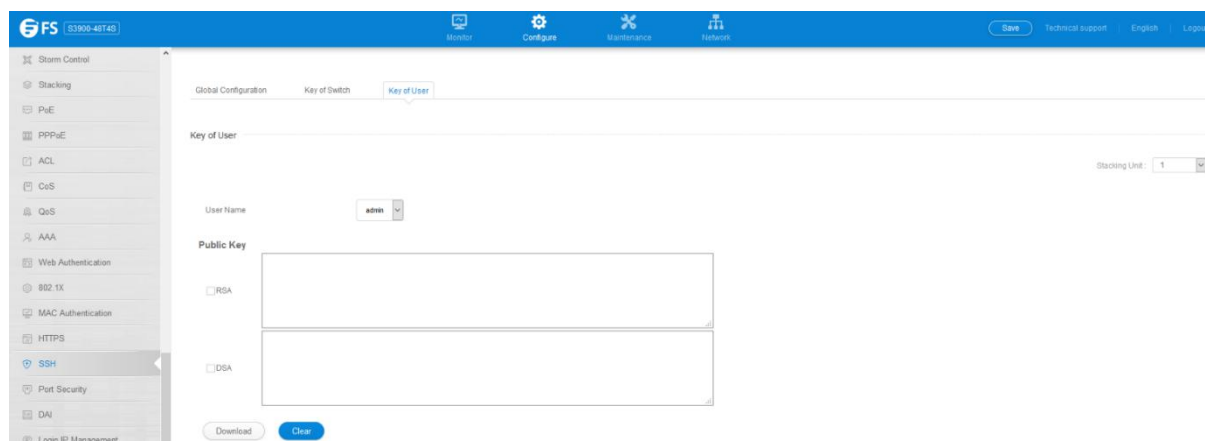
- **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both; Default: Both) The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair. (Default: Disabled)



4.32.3 Key of User

Configure > SSH > Key of User page is used to upload a user's public key to the switch. This public key must be stored on the switch for the user to be able to log in using the public key authentication mechanism. If the user's public key does not exist on the switch, SSH will revert to the interactive password authentication mechanism to complete authentication.

- **User Name** – This drop-down box selects the user who's public key you wish to manage. Note that you must first create users on the User Accounts page.
- **User Key Type** – The type of public key to upload.
 - **RSA**: The switch accepts a RSA version 1 encrypted public key.
 - **DSA**: The switch accepts a DSA version 2 encrypted public key. The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption. The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- **TFTP Server IP Address** – The IP address of the TFTP server that contains the public key file you wish to import.
- **Source File Name** – The public key file to upload.

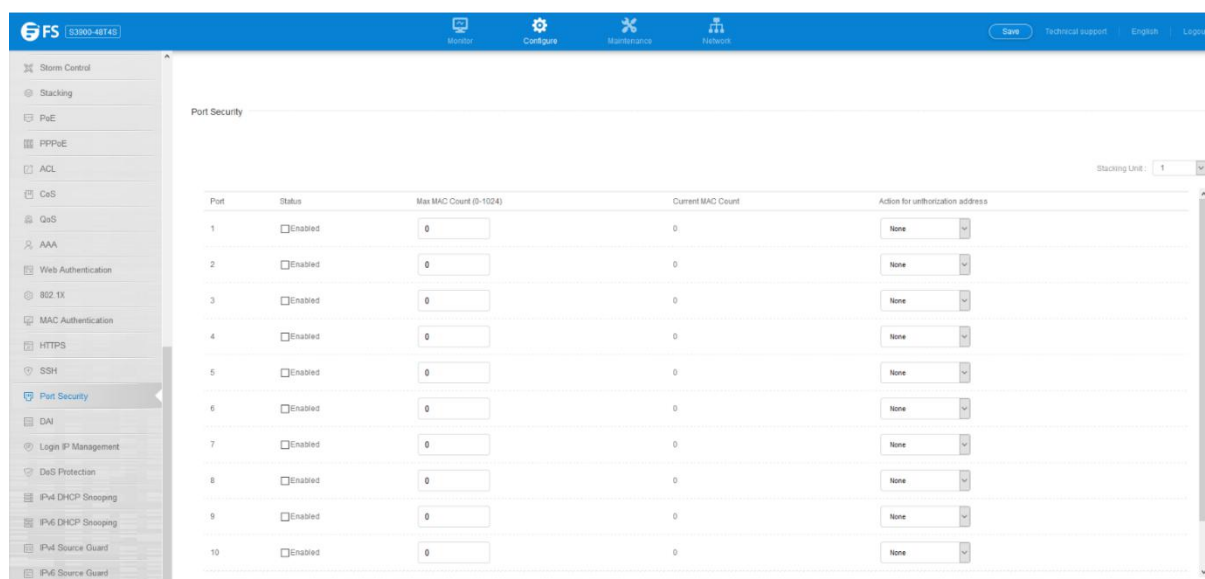


4.33 Port Security

Configure > Port Security page is used to configure the maximum number of device MAC addresses that can be learned by a switch port, stored in the address table, and authorized to access the network.

- **Port** – Port number.
- **Status** – Enables or disables port security on an interface. (Default: Disabled)
- **Port Status** – The operational status:

- **Secure/Down** – Port security is disabled.
- **Secure/Up** – Port security is enabled.
- **Shutdown** – Port is shut down due to a response to a port security violation.
- **Action for unthorization address**– Indicates the action to be taken when a port security violation is detected:
 - **None**: No action should be taken. (This is the default.)
 - **Trap**: Send an SNMP trap message.
 - **Shutdown**: Disable the port.
 - **Trap and Shutdown**: Send an SNMP trap message and disable the port.
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled) The maximum address count is effective when port security is enabled or disabled.
- **Current MAC Count** – The number of MAC addresses currently associated with this interface.



Port Security

Stacking Unit: 1

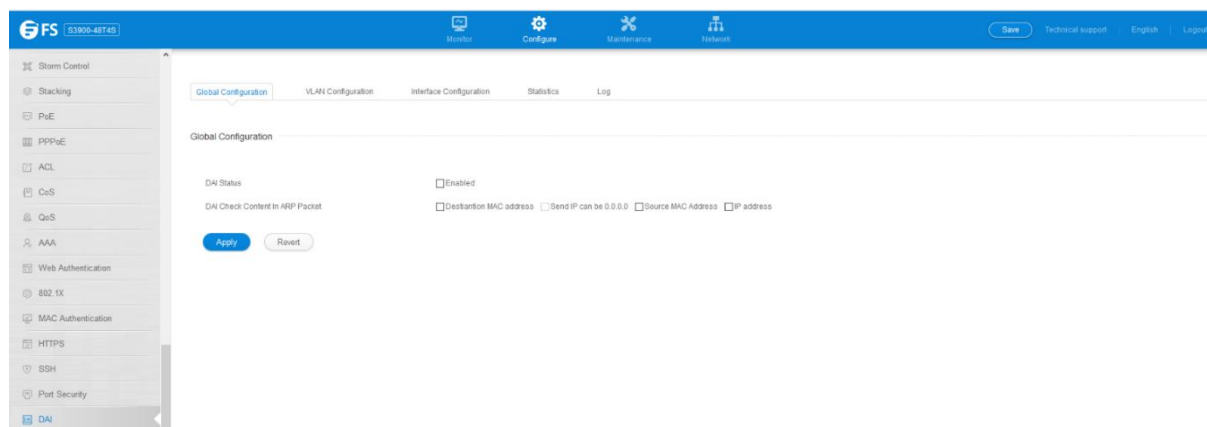
Port	Status	Max MAC Count (0-1024)	Current MAC Count	Action for unthorization address
1	<input type="checkbox"/> Enabled	0	0	None
2	<input type="checkbox"/> Enabled	0	0	None
3	<input type="checkbox"/> Enabled	0	0	None
4	<input type="checkbox"/> Enabled	0	0	None
5	<input type="checkbox"/> Enabled	0	0	None
6	<input type="checkbox"/> Enabled	0	0	None
7	<input type="checkbox"/> Enabled	0	0	None
8	<input type="checkbox"/> Enabled	0	0	None
9	<input type="checkbox"/> Enabled	0	0	None
10	<input type="checkbox"/> Enabled	0	0	None

4.34 DAI

4.34.1 Global Configuration

Configure >DAI >Global Configuration page is used to enable ARP inspection globally for the switch, to validate address information in each packet, and configure logging.

- **DAI Status**– Enables ARP Inspection globally. (Default: Disabled)
- **DAI Check Content In ARP Packet**– Enables extended ARP Inspection Validation if any of the following options are enabled. (Default: Disabled)
 - **Destiantion MAC address**– Validates the destination MAC address in the Ethernet header against the target MAC address in the body of ARP responses.
 - **IP address**– Checks the ARP body for invalid and unexpected IP addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.
 - **Source MAC Address**– Validates the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.

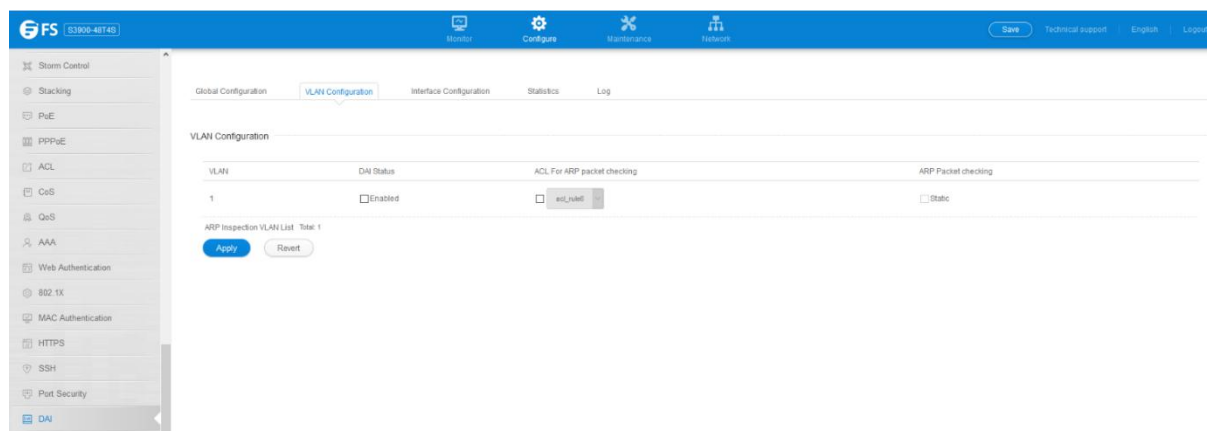


4.34.2 VLAN Configuration

Configure >DAI >VLAN Configuration page is used to enable ARP inspection for any VLAN and to specify the ARP ACL to use.

- **ARP Inspection VLAN ID** – Selects any configured VLAN. (Default: 1)
- **ARP Inspection VLAN Status** – Enables ARP Inspection for the selected VLAN. (Default: Disabled)
- **ARP Inspection ACL Name**
 - **ARP ACL** – Allows selection of any configured ARP ACLs. (Default: None)
 - **Static** – When an ARP ACL is selected, and static mode also selected, the switch only performs ARP Inspection and bypasses validation against the DHCP Snooping Bindings database. When an ARP ACL is selected, but static mode is not selected, the switch first

performs ARP Inspection and then validation against the DHCP Snooping Bindings database. (Default: Disabled)



4.34.3 Interface Configuration

Configure >DAI >Interface Configuration page is used to specify the ports that require ARP inspection, and to adjust the packet inspection rate.

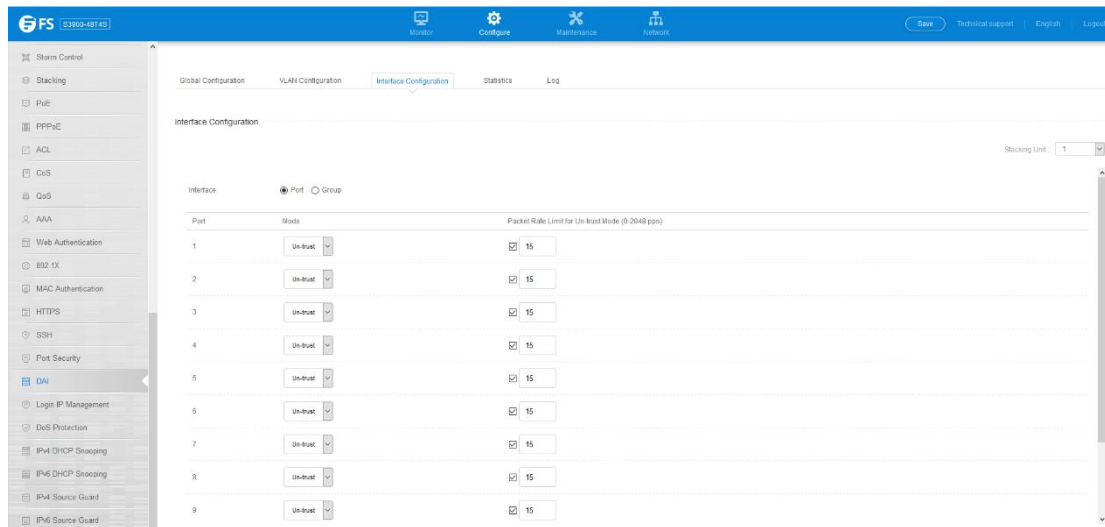
- **Port**– Port or trunk identifier.
- **Mode**– Configures the port as trusted or untrusted.(Default: Untrusted)

By default, all untrusted ports are subject to ARP packet rate limiting, and all trusted ports are exempt from ARP packet rate limiting. Packets arriving on trusted interfaces bypass all ARP Inspection and ARP Inspection Validation checks and will always be forwarded, while

those arriving on untrusted interfaces are subject to all configured ARP inspection tests.

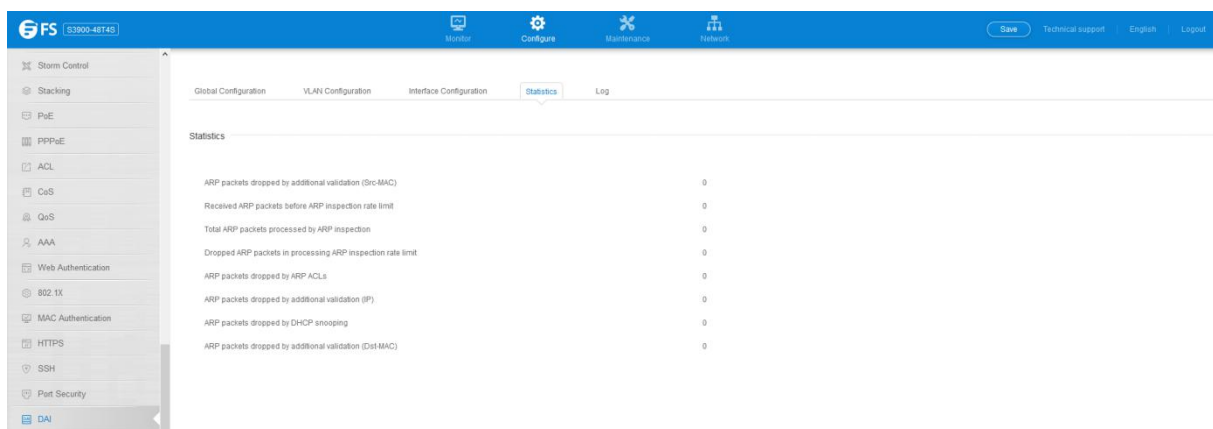
- **Packet Rate Limit for Un-trust Mode (0-2048 pps)**– Sets the maximum number of ARP packets that can be processed by CPU per second on trusted or untrusted ports. (Range: 0-2048; Default: 15) Setting the rate limit to “0” means that there is no restriction on

the number of ARP packets that can be processed by the CPU. The switch will drop all ARP packets received on a port which exceeds the configured ARP-packets-per-second rate limit.



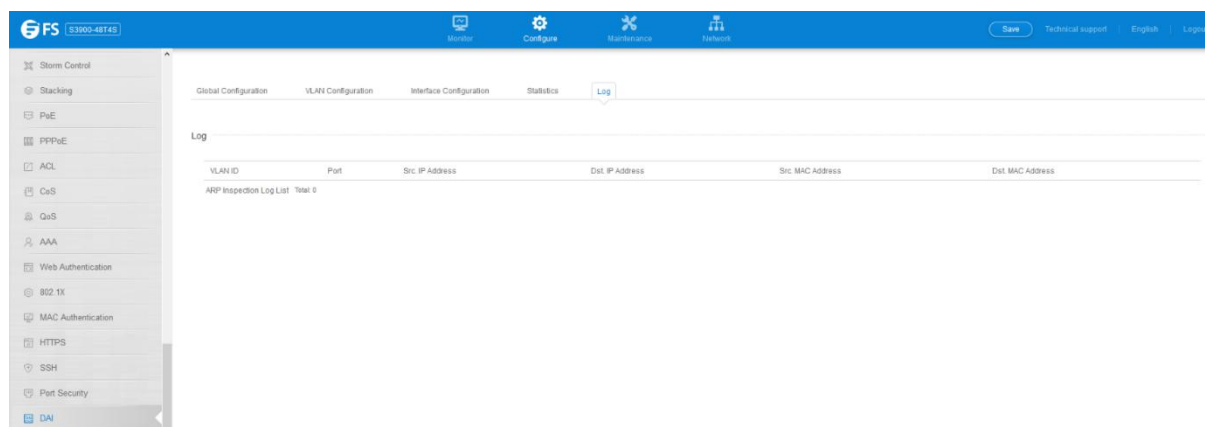
4.34.4 Statistics

Configure >DAI >Statistics page is used to display statistics about the number of ARP packets processed, or dropped for various reasons.



4.34.5 Log

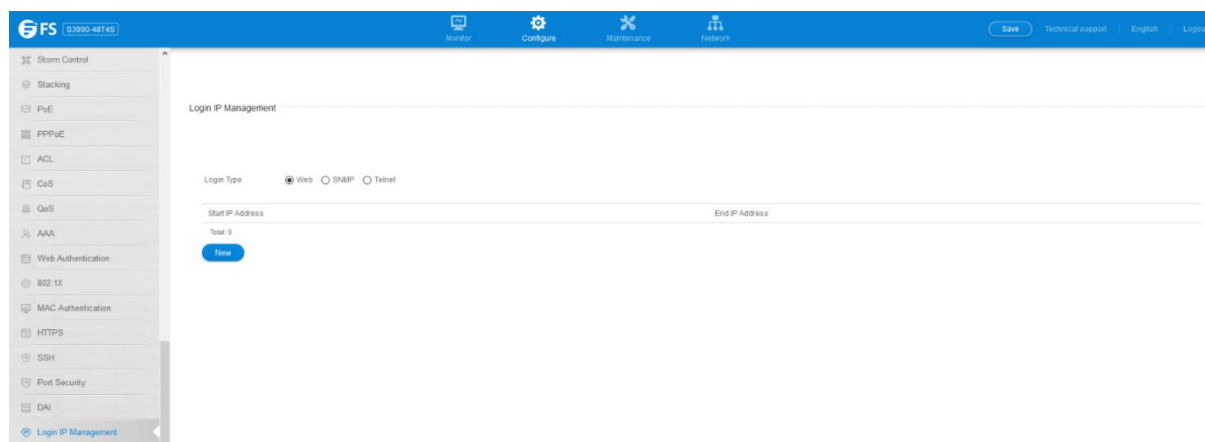
The Configure >DAI >Log page is used to show information about entries stored in the log, including the associated VLAN, port, and address components.



4.35 Login IP Management

The Configure > Login IP Management page is used to create a list of up to 15 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

- **Mode**
 - **Web** – Configures IP address(es) for the web group.
 - **SNMP** – Configures IP address(es) for the SNMP group.
 - **Telnet** – Configures IP address(es) for the Telnet group.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.



4.36 DoS Protection

The Configure > DoS Protection page is used to protect against denial-of-service (DoS) attacks. A DoS attack is an attempt to block the services provided by a computer or network resource.

- **Echo/Chargen Attack** – Attacks in which the echo service repeats anything sent to it, and the chargen (character generator) service generates a continuous stream of data. When used together, they create an infinite loop and result in a denial-of-service. (Default: Disabled)
- **Echo/Chargen Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)
- **Smurf Attack** – Attacks in which a perpetrator generates a large amount of spoofed ICMP Echo Request traffic to the broadcast destination IP address (255.255.255.255), all of which uses a spoofed source address of the intended victim. The victim should

crash due to the many interrupts required to send ICMP Echo response packets. (Default: Enabled)

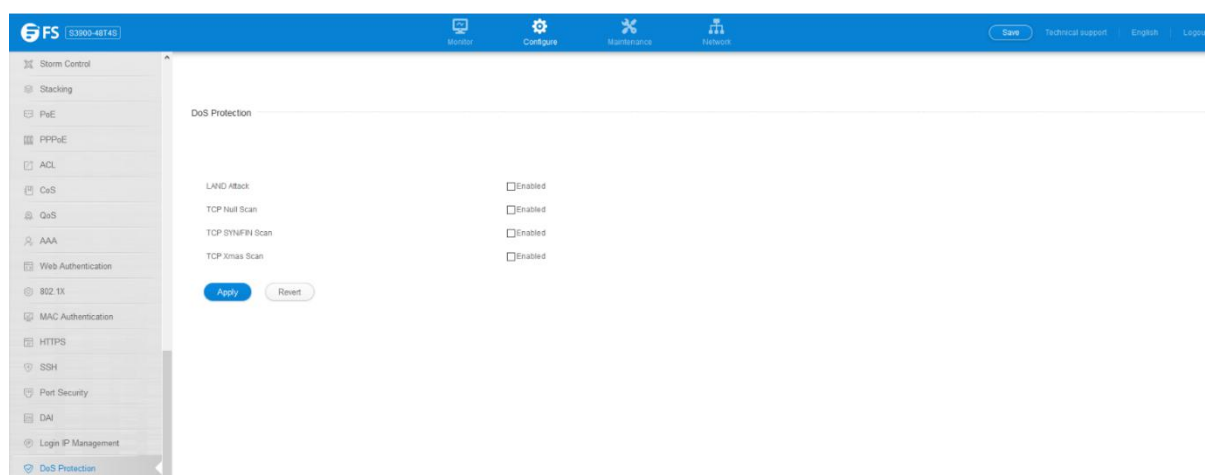
- **TCP Flooding Attack** – Attacks in which a perpetrator sends a succession of TCP SYN requests (with or without a spoofed-Source IP) to a target and never returns ACK packets. These half-open connections will bind resources on the target, and no new connections can be made, resulting in a denial of service. (Default: Disabled)
- **TCP Flooding Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)
- **TCP Null Scan** – A TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. (Default: Enabled)
- **TCP-SYN/FIN Scan** – A TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. (Default: Enabled)
- **TCP Xmas Scan** – A so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target

replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. (Default: Enabled)

- **UDP Flooding Attack** – Attacks in which a perpetrator sends a large number of UDP packets (with or without a spoofed-Source IP) to random ports on a remote host. The target will determine that application is listening at that port, and reply with an ICMP Destination

Unreachable packet. It will be forced to send many ICMP packets, eventually leading it to be unreachable by other clients. (Default: Disabled)

- **UDP Flooding Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)
- **WinNuke Attack** – Attacks in which affected the Microsoft Windows 3.1x/95/NT operating systems. In this type of attack, the perpetrator sends the string of OOB out-of-band (OOB) packets contained a TCP URG flag to the target computer on TCP port 139 (NetBIOS), casing it to lock up and display a “Blue Screen of Death.” This did not cause any damage to, or change data on, the computer's hard disk, but any unsaved data would be lost. Microsoft made patches to prevent the WinNuke attack, but the OOB packets. (Default: Disabled)
- **WinNuke Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)



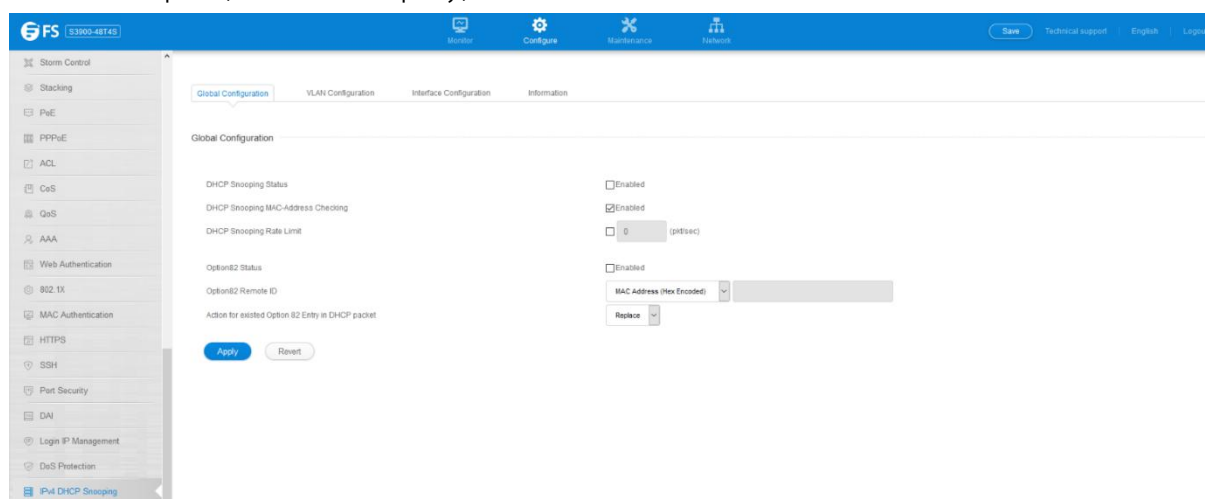
4.37 IPv4 DHCP Snooping

4.37.1 Global Configuration

Configure > IPv4 DHCP Snooping > Global Configuration page is used to enable DHCP Snooping globally on the switch, or to configure

MAC Address Verification.

- **DHCP Snooping Status** – Enables DHCP snooping globally. (Default: Disabled)
- **DHCP Snooping MAC-Address Verification** – Enables or disables MAC address verification. If the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped. (Default: Enabled)
- **DHCP Snooping Rate Limit** – Sets the maximum number of DHCP packets that can be trapped by the switch for DHCP snooping. (Range: 1-2048 packets/ second)
- **DHCP Snooping Information Option Status** – Enables or disables DHCP Option 82 information relay. (Default: Disabled)
- **DHCP Snooping Information Option Sub-option Format** – Enables or disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.
- **DHCP Snooping Information Option Remote ID** – Specifies the MAC address, IP address, or arbitrary identifier of the requesting device (i.e., the switch in this context).
 - **MAC Address** – Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (i.e., the MAC address of the switch's CPU). This attribute can be encoded in Hexadecimal or ASCII.
 - **IP Address** – Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (i.e., the IP address of the management interface). This attribute can be encoded in Hexadecimal or ASCII.
 - **string** – An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)
- **DHCP Snooping Information Option Remote ID TR101 VLAN Field** – Adds ":VLAN" in TR101 field for untagged packets. The format for TR101 option 82 is: "<IP> eth <SID>/<PORT>[:<VLAN>]". Note that the SID (Switch ID) is always 0. By default the PVID is added to the end of the TR101 field for untagged packets. For tagged packets, the VLAN ID is always added.
- **DHCP Snooping Information Option Policy** – Specifies how to handle DHCP client request packets which already contain Option 82 information.
 - **Drop** – Drops the client's request packet instead of relaying it.
 - **Keep** – Retains the Option 82 information in the client request, and forwards the packets to trusted ports.
 - **Replace** – Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports. (This is the default policy.)

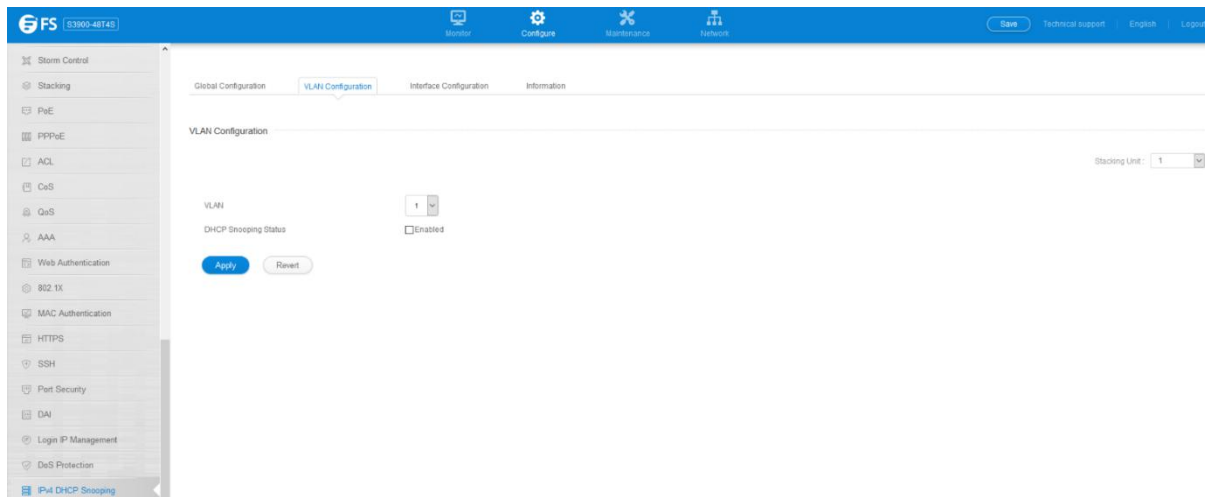


4.37.2 VLAN Configuration

Configure >IPv4 DHCP Snooping >VLAN Configuration page is used to enable or disable DHCP snooping on specific VLANs.

- **VLAN** – ID of a configured VLAN. (Range: 1-4093)
- **DHCP Snooping Status** – Enables or disables DHCP snooping for the selected VLAN. When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.

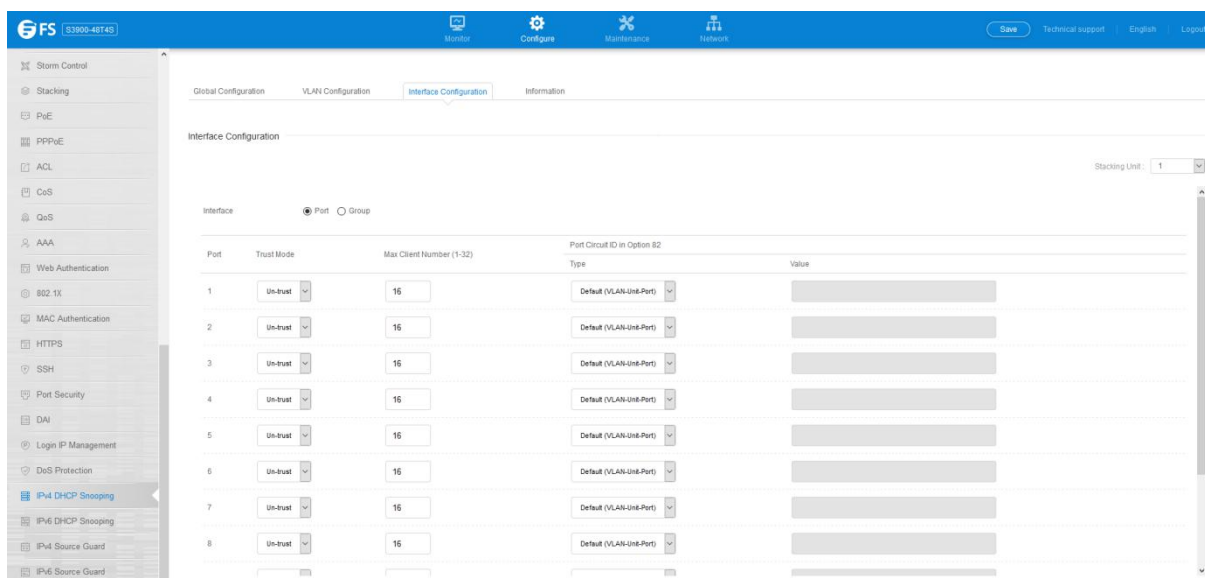
(Default: Disabled)



4.37.3 Interface Configuration

Configure >IPv4 DHCP Snooping >Interface Configuration page is used to configure switch ports as trusted or un-trusted.

- **Trust Status** – Enables or disables a port as trusted. (Default: Disabled)
- **Circuit ID** – Specifies DHCP Option 82 circuit ID sub option information.
 - **Mode** – Specifies the default string “VLAN-Unit-Port” or an arbitrary string. (Default: VLAN-Unit-Port)
 - **Value** – An arbitrary string inserted into the circuit identifier field. (Range: 1-32 characters)



4.37.4 Information

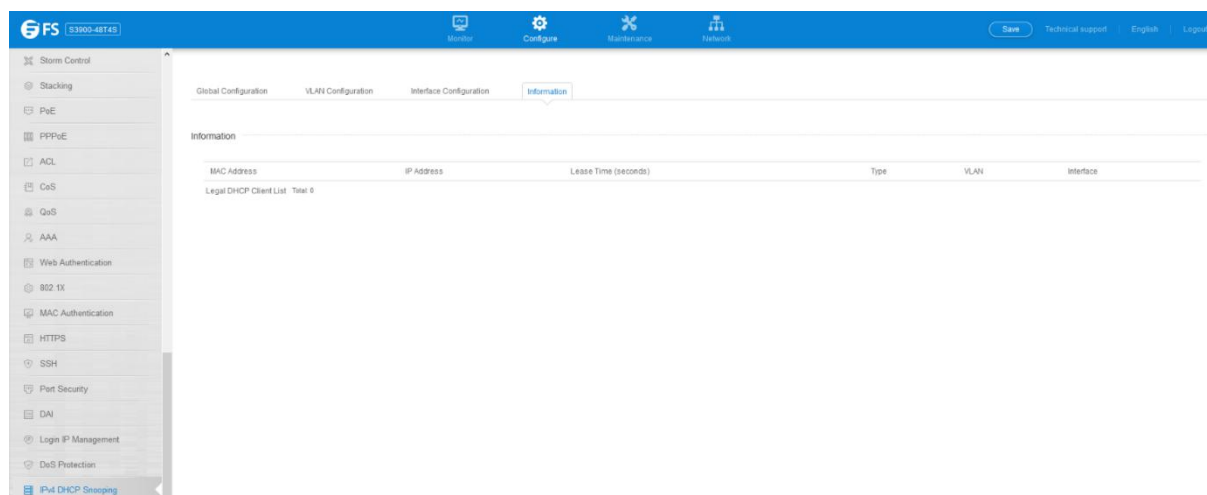
Configure >IPv4 DHCP Snooping >Information page is used to display entries in the binding table.

- **MAC Address** – Physical address associated with the entry.
- **IP Address** – IP address corresponding to the client.
- **Lease Time** – The time for which this IP address is leased to the client.
- **Type** – Entry types include:
 - **DHCP-Snooping** – Dynamically snooped.
 - **Static-DHCPSPNP** – Statically configured.
- **VLAN** – VLAN to which this entry is bound.

- **Interface** – Port or group to which this entry is bound.
- **Store** – Writes all dynamically learned snooping entries to flash memory. This function can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note

that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

- **Clear** – Removes all dynamically learned snooping entries from flash memory.



4.38 IPv6 DHCP Snooping

4.38.1 Global Configuration

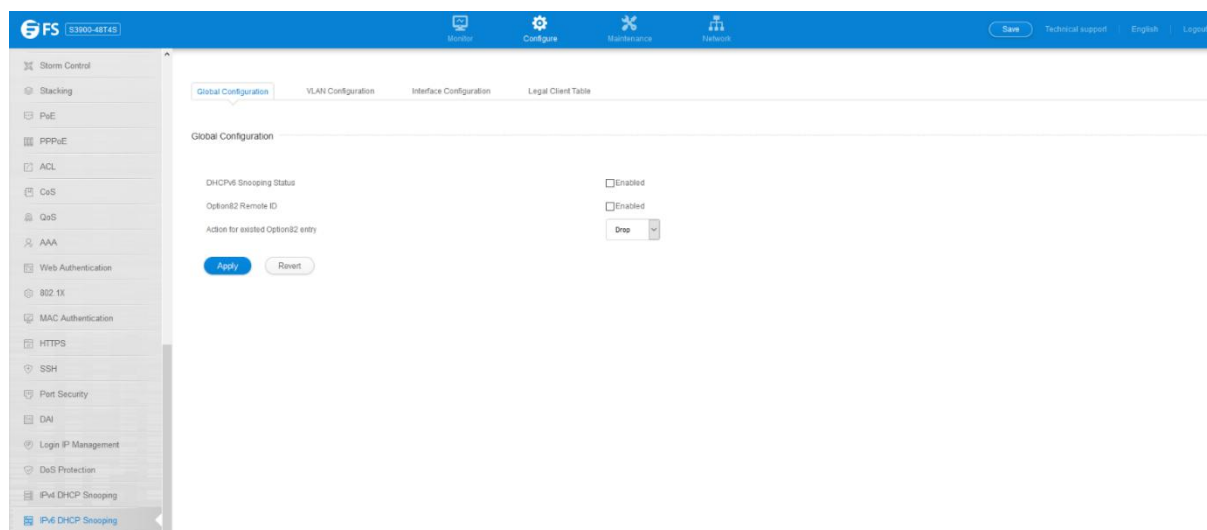
Configure >IPv6 DHCP Snooping >Global Configuration page is used to enable DHCPv6 Snooping globally on the switch, or to configure MAC Address Verification.

- **DHCPv6 Snooping Status**—Enables DHCPv6 snooping globally.(Default: Disabled)
- **DHCPv6 Snooping Option Remote ID**—Enables the insertion of remote-id

option 37 information into DHCPv6 client messages. Remote-id option information such as the port attached to the client, DUID, and VLAN ID is used by the DHCPv6 server to assign pre-assigned configuration data specific to the DHCPv6 client. (Default: Disabled)

- DHCPv6 provides a relay mechanism for sending information about the switch and its DHCPv6 clients to the DHCPv6 server. Known as DHCPv6 Option 37, it allows compatible DHCPv6 servers to use the information when assigning IP addresses, or to set other services or policies for clients.
- When DHCPv6 Snooping Information Option 37 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCPv6 request packets forwarded by the switch and in reply packets sent back from the DHCPv6 server.
- When the DHCPv6 Snooping Option 37 is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCPv6 client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.
- DHCPv6 snooping must be enabled for the DHCPv6 Option 37 information to be inserted into packets. When enabled, the switch will either drop, keep or remove option 37 information in incoming DHCPv6 packets. Packets are processed as follows:
 - If an incoming packet is a DHCPv6 request packet with option 37 information, it will modify the option 37 information according to the settings specified.
 - If an incoming packet is a DHCPv6 request packet without option 37 information, enabling the DHCPv6 snooping information option will add option 37 information to the packet.

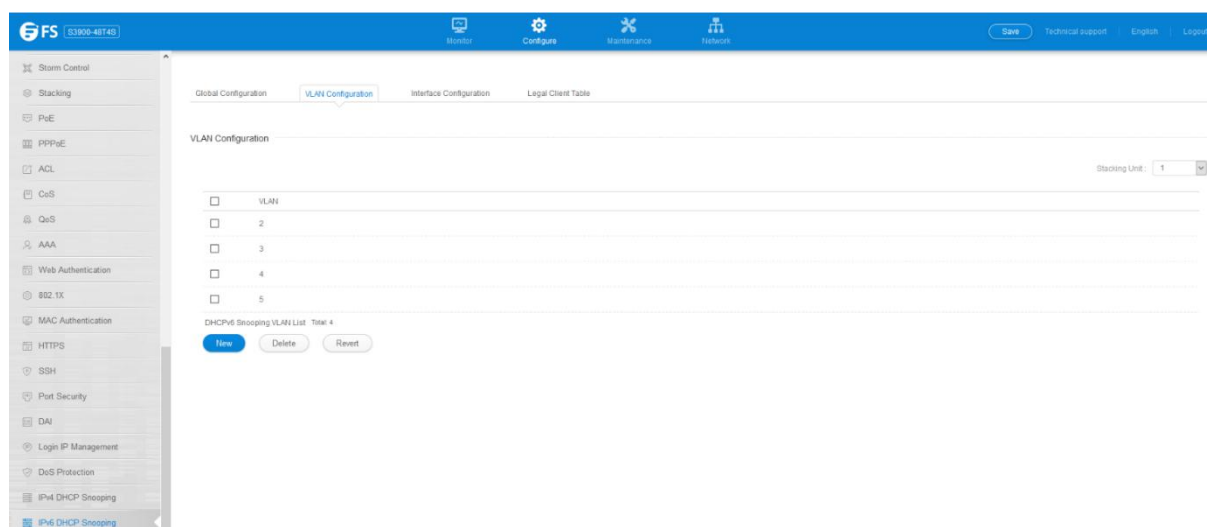
- If an incoming packet is a DHCPv6 reply packet with option 37 information, enabling the DHCPv6 snooping information option will remove option 37 information from the packet.
- When this switch inserts Option 37 information in DHCPv6 client request packets, the switch's MAC address (hexadecimal) is used for the remote ID.
- **DHCPv6 Snooping Option Policy** –Sets the remote-id option policy for DHCPv6 client packets that include Option 37 information. When the switch receives DHCPv6 packets from clients that already include DHCP Option 37 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCPv6 packets, keep the existing information, or replace it with the switch's relay agent information.
 - Drop –Drops the client's request packet instead of relaying it (This is the default policy).
 - Keep –Retains the Option 82 information in the client request, and forwards the packets to trusted ports.
 - Replace –Replaces the Option 37 remote-ID in the client's request with the relay agent's remote-ID (when DHCPv6 snooping is enabled), and forwards the packets to trusted ports.



4.38.2 VLAN Configuration

Configure >IPv6 DHCP Snooping >VLAN Configuration page is used to enable or disable DHCPv6 snooping on specific VLANs.

- **VLAN**—ID of a configured VLAN. (Range: 1-4094)



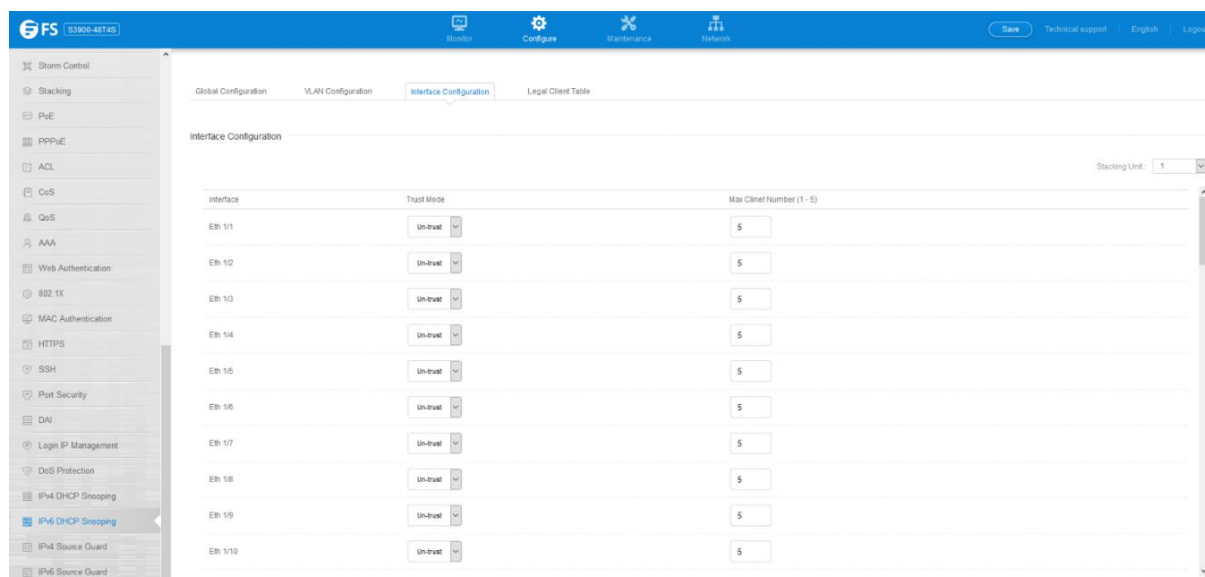


VLAN ID (1-4094) -

4.38.3 Interface Configuration

Configure > IPv6 DHCP Snooping > Interface Configuration page is used to configure switch interfaces as trusted or untrusted, and set the maximum number of entries which can be stored in the binding database for an interface.

- **Interface**—Port or group identifier.
- **Trust Status**—Enables or disables an interface as trusted. (Default: Disabled)
- **Max Binding**—Sets the maximum number of entries which can be stored in the binding database for an interface. (Range: 1-5; Default: 5)
- **Current Binding**—Shows the maximum number of entries which can be stored in the binding database for an interface.

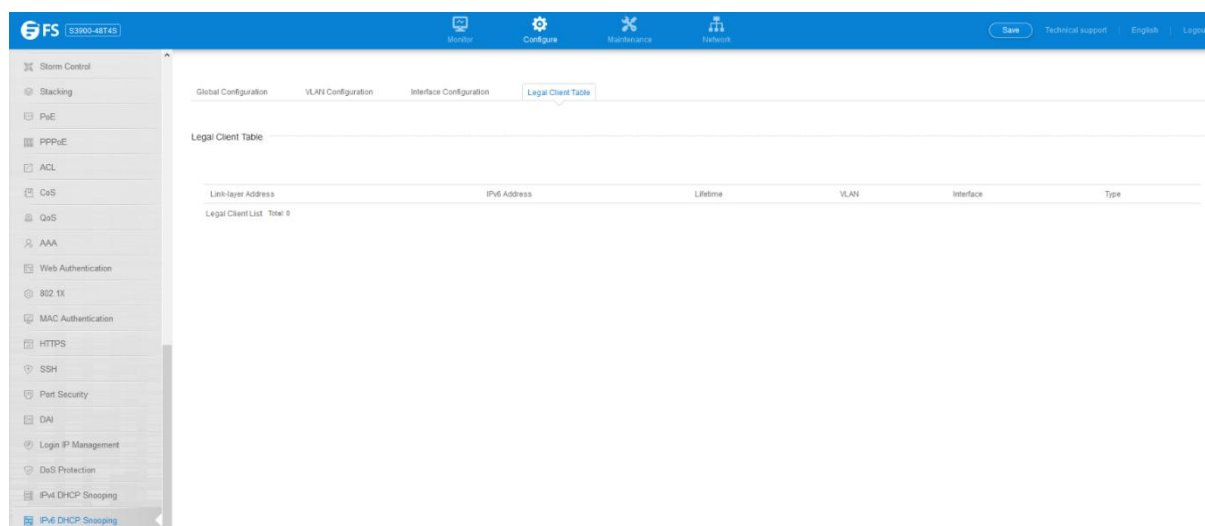


Interface	Trust Mode	Max Client Number (1 - 5)
Eth 1/1	Un-trust	5
Eth 1/2	Un-trust	5
Eth 1/3	Un-trust	5
Eth 1/4	Un-trust	5
Eth 1/5	Un-trust	5
Eth 1/6	Un-trust	5
Eth 1/7	Un-trust	5
Eth 1/8	Un-trust	5
Eth 1/9	Un-trust	5
Eth 1/10	Un-trust	5

4.38.4 Legal Client Table

Configure > IPv6 DHCP Snooping > Legal Client Table page is used to display entries in the binding table.

- **Link-layer Address**—IPv6 link-layer address associated with the entry.
- **IPv6 Address**—IPv6 address corresponding to the client.
- **Lifetime**—The time (number of seconds) for which this IPv6 address is leased to the client.
- **VLAN**—VLAN to which this entry is bound.
- **Interface**—Port or group to which this entry is bound.
- **Type**—Entry types include:
 - **NA**—Non-temporary address.
 - **TA**—Temporary address.
- **Clear**—Removes all dynamically learned snooping entries from RAM.



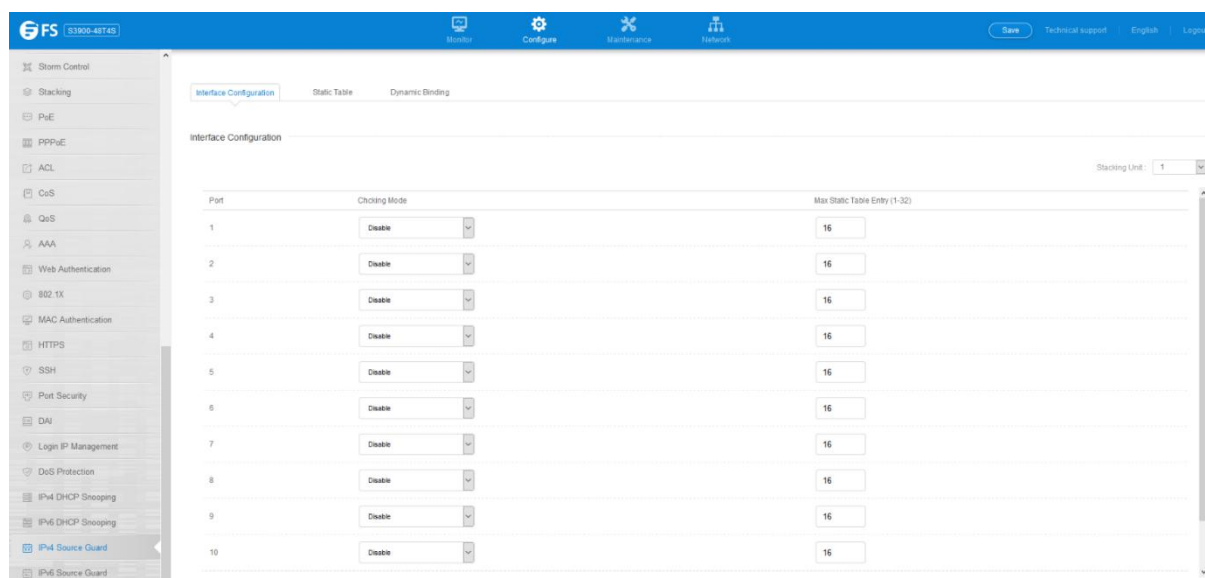
4.39 IPv4 Source Guard

4.39.1 Interface Configuration

Configure > IPv4 Source Guard > Interface Configuration page is used to set the filtering type based on source IP address, or source IP address and MAC address pairs.

- **Checking Mode** – Configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. (Default: None)
 - **None** – Disables IP source guard filtering on the port.
 - **Source IP** – Enables traffic filtering based on IP addresses stored in the binding table.
 - **Source IP and MAC** – Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.
- **Max Static Table Entry** – The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5) This parameter sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic

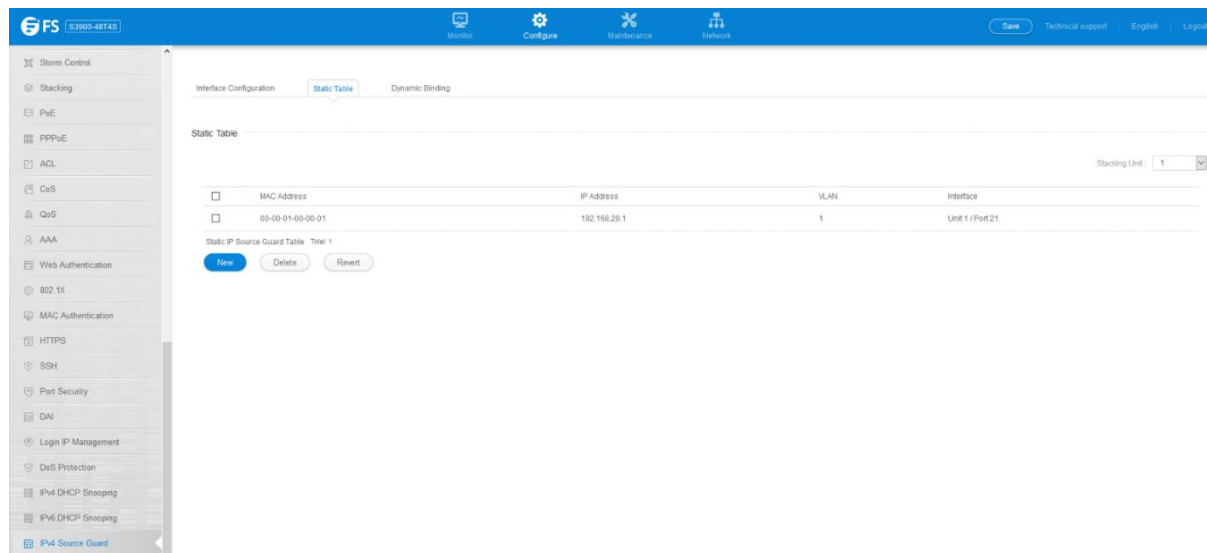
entries discovered by DHCP snooping and static entries set by IP source guard.



4.39.2 Static Table

Configure > IPv4 Source Guard > Static Table page is used to bind a valid static IP source guard entry to a port in ACL mode.

- **Port**—The port to which a static entry is bound.
- **VLAN**—ID of a configured VLAN (Range: 1-4094)
- **MAC Address**—A valid unicast MAC address.
- **IP Address**—A valid unicast IP address, including classful types A, B or C.




4.39.3 Dynamic Binding

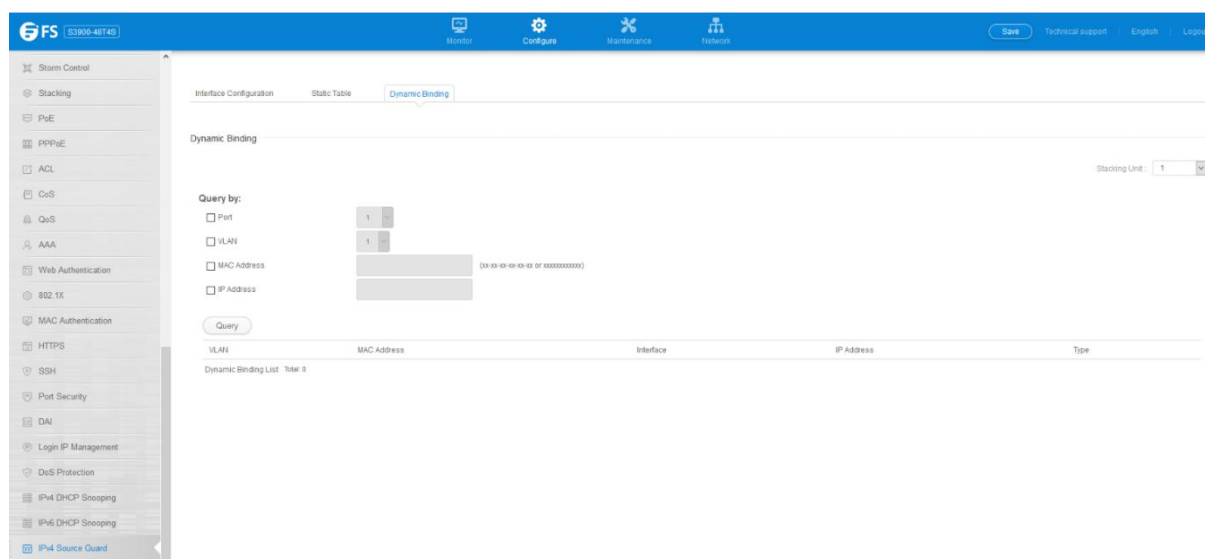
Configure > IPv4 Source Guard > Dynamic Binding page is used to display the source-guard binding table for a selected interface.

Query by

- **Port** – A port on this switch.
- **VLAN** – ID of a configured VLAN (Range: 1-4093)
- **MAC Address** – A valid unicast MAC address.
- **IP Address** – A valid unicast IP address, including classful types A, B or C.

Dynamic Binding List

- **VLAN** – VLAN to which this entry is bound.
- **MAC Address** – Physical address associated with the entry.
- **Interface** – Port to which this entry is bound.
- **IP Address** – IP address corresponding to the client.
- **Lease Time** – The time for which this IP address is leased to the client.

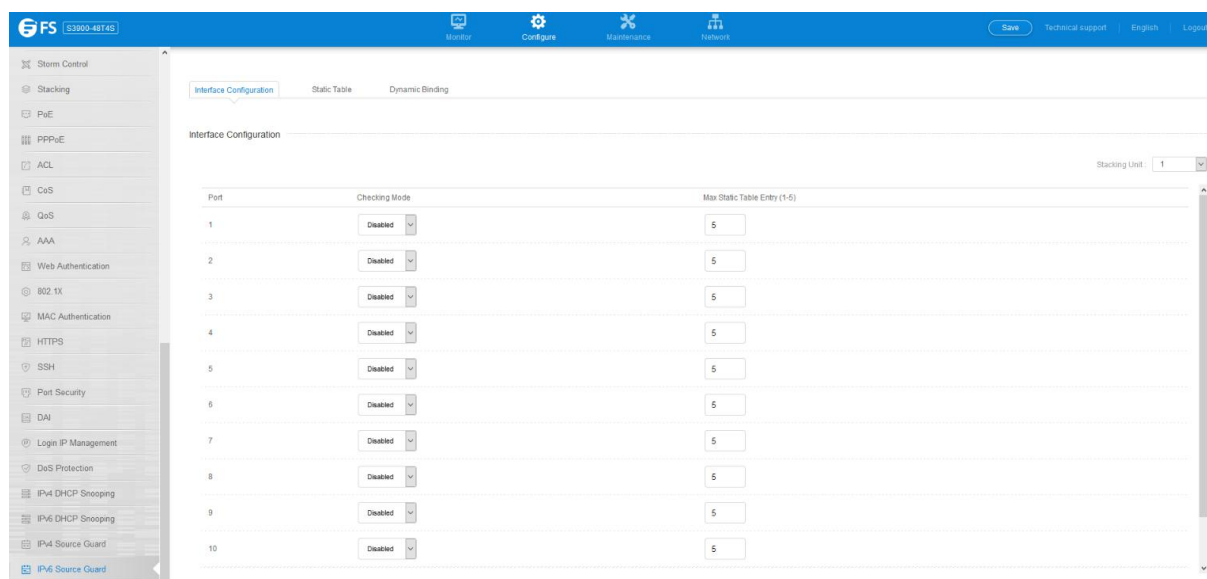


4.40 IPv6 Source Guard

4.40.1 Interface Configuration

Configure > IPv6 Source Guard > Interface Configuration page is used to filter inbound traffic based on the source IPv6 address stored in the binding table.

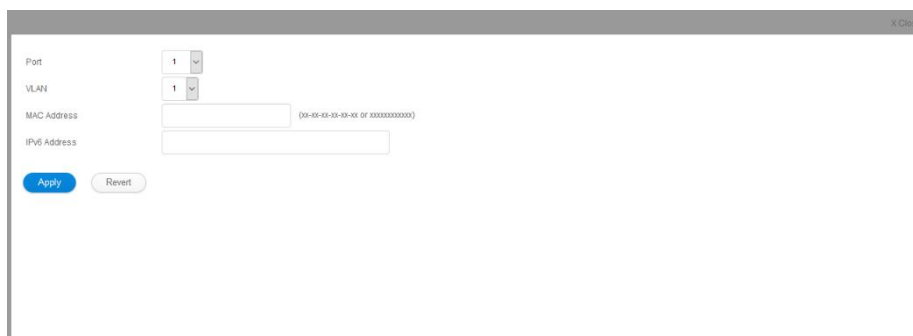
- **Port**—Port identifier.
- **Filter Type**—Configures the switch to filter inbound traffic based on the following options. (Default: Disabled)
 - **Disabled**—Disables IPv6 source guard filtering on the port.
 - **Source IP**—Enables traffic filtering based on IPv6 global unicast source IPv6 addresses stored in the binding table.
- **Max Binding Entry**—The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5)
 - This parameter sets the maximum number of IPv6 global unicast source IPv6 address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by ND snooping, DHCPv6 snooping.
 - IPv6 source guard maximum bindings must be set to a value higher than DHCPv6 snooping maximum bindings and ND snooping maximum bindings.
 - If IPv6 source guard, ND snooping, and DHCPv6 snooping are enabled on a port, the dynamic bindings used by ND snooping, DHCPv6 snooping, and IPv6 source guard static bindings cannot exceed the maximum allowed bindings set by this parameter. In other words, no new entries will be added to the IPv6 source guard binding table.
 - If IPv6 source guard is enabled on a port, and the maximum number of allowed bindings is changed to a lower value, precedence is given to deleting entries learned through DHCPv6 snooping, ND snooping, and then manually configured IPv6 source guard static bindings, until the number of entries in the binding table reaches the newly configured maximum number of allowed bindings.

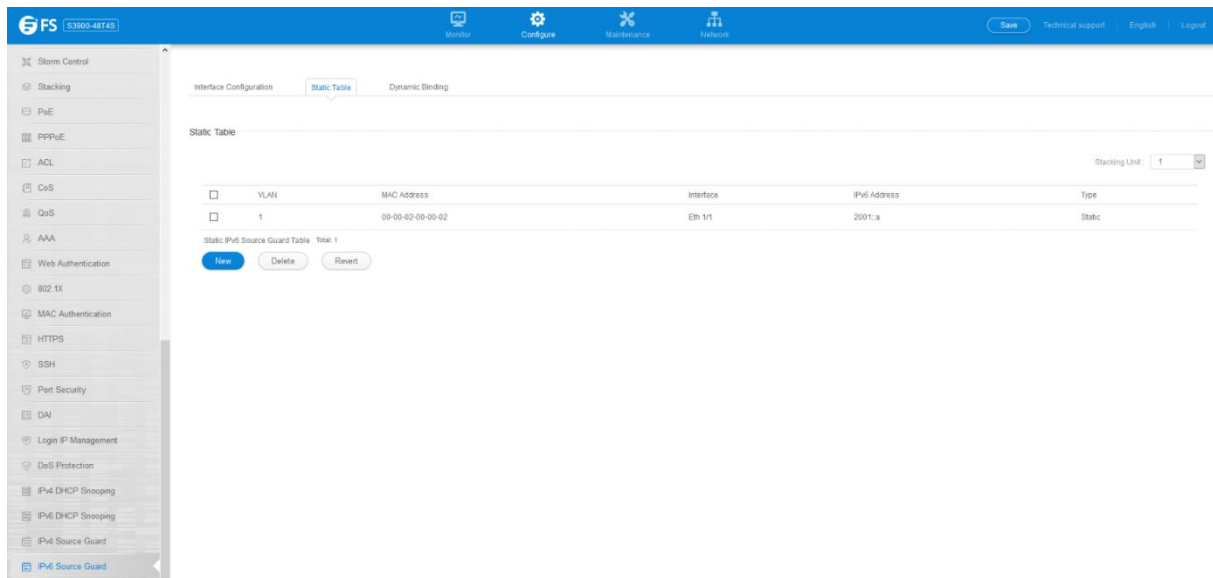


4.40.2 Static Table

Use the Configure > IPv6 Source Guard > Static Table page to bind a static address to a port. Table entries include a MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.

- **Port**—The port to which a static entry is bound.
- **VLAN**—ID of a configured VLAN (Range: 1-4094)
- **MAC Address**—A valid unicast MAC address.
- **IPv6 Address**—A valid global unicast IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.



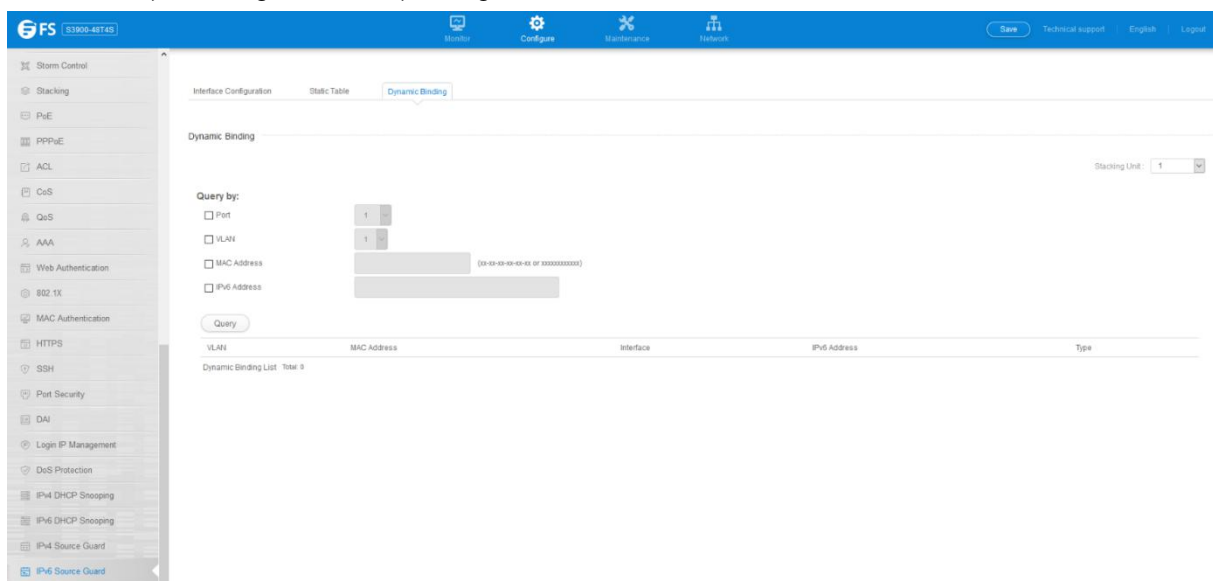


4.40.3 Dynamic Binding

Configure > IPv6 Source Guard > Dynamic Binding page is used to display the source-guard binding table for a selected interface.

Query by

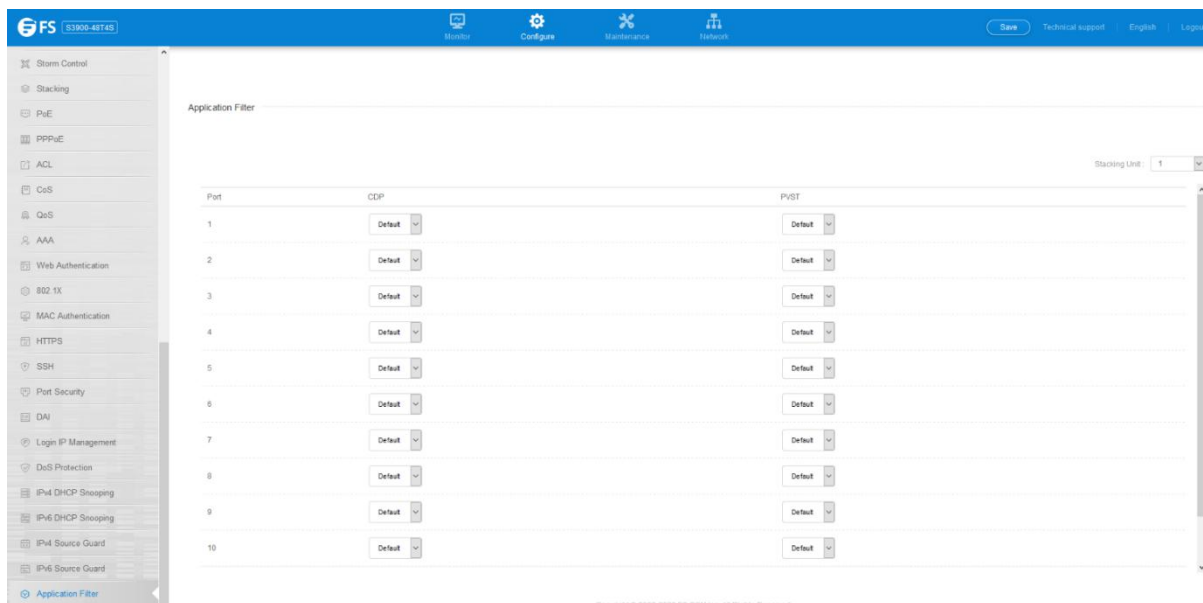
- **Port**—A port on this switch.
- **VLAN**—ID of a configured VLAN (Range: 1-4094)
- **MAC Address**—A valid unicast MAC address.
- **IPv6 Address**—A valid global unicast IPv6 address. Dynamic Binding List
- **VLAN**—VLAN to which this entry is bound.
- **MAC Address**—Physical address associated with the entry.
- **Interface**—Port to which this entry is bound.
- **IPv6 Address**—IPv6 address corresponding to the client.
- **Type**—Shows the entry type:
 - **DHCP**—Dynamic DHCPv6 binding, stateful address.
 - **ND**—Dynamic Neighbor Discovery binding, stateless address.



4.41 Application Filter

Use the Configure > Application Filter page to forward CDP or PVST packets.

- **Port**—Port identifier (Range: 1-26/28/52)
- **CDP**—Cisco Discovery Protocol
- **PVST**—Per-VLAN Spanning Tree



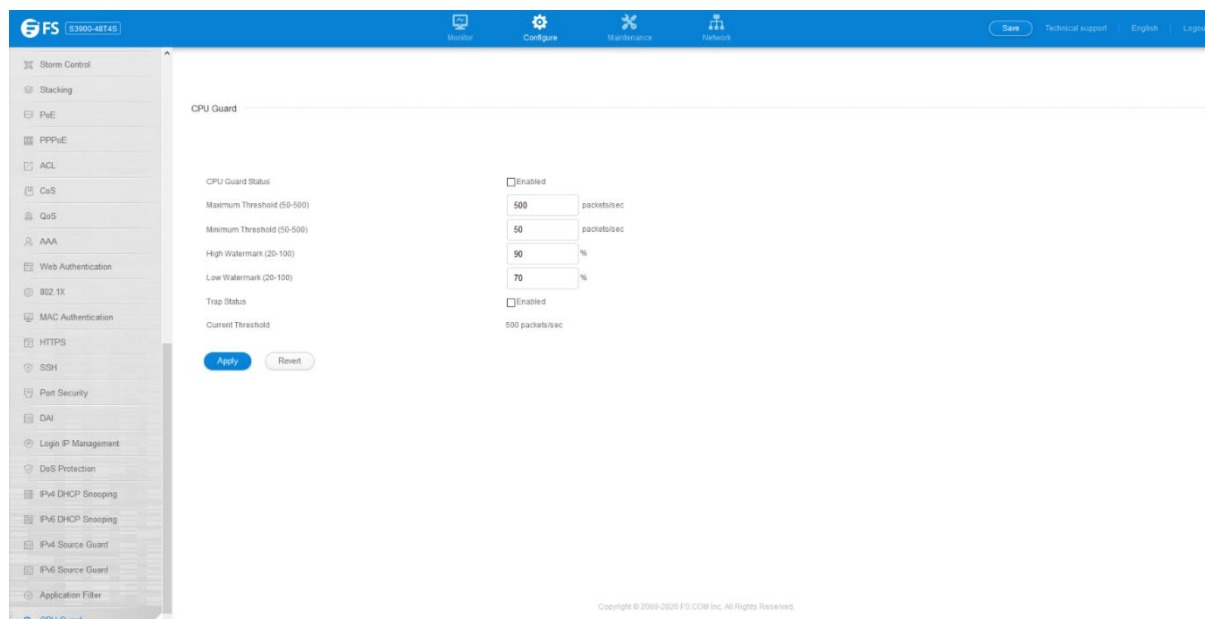
4.42 CPU Guard

Use the Configure > CPU Guard page to set the CPU utilization high and low watermarks in percentage of CPU time utilized and the CPU high and low thresholds in the number of packets being processed per second.

- **CPU Guard Status**—Enables CPU Guard. (Default: Disabled)
- **High Watermark** —If the percentage of CPU usage time is higher than the high-watermark, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until usage time falls below the low watermark. (Range: 40-100 %; Default: 90 %)
- **Low Watermark**—If packet flow has been stopped after exceeding the high watermark, normal flow will be restored after usage falls beneath the low watermark. (Range: 40-100 %; Default: 70 %)
- **Maximum Threshold** —If the number of packets being processed by the CPU is higher than the maximum threshold, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until the number of packets being processed falls below the minimum threshold. (Range: 50-500 pps; Default: 500 pps)
- **Minimum Threshold**—If packet flow has been stopped after exceeding the maximum threshold, normal flow will be restored after usage falls beneath the minimum threshold. (Range: 50-500 pps; Default: 50 pps)
- **Trap Status** —If enabled, an alarm message will be generated when utilization exceeds the high watermark or exceeds the maximum threshold. (Default: Disabled) Once the high watermark is exceeded, utilization must drop beneath the low watermark before the alarm is terminated, and then exceed the high watermark again before another alarm is triggered.

Once the maximum threshold is exceeded, utilization must drop beneath the minimum threshold before the alarm is terminated, and then exceed the maximum threshold again before another alarm is triggered.

- **Current Threshold**—Shows the configured threshold in packets per second.



5. Network

5.1 IP Interface Configuration

This section describes how to configure an IPv4 interface for management access over the network. Network > IP Configuration page is used to configure an IPv4 address for the switch.

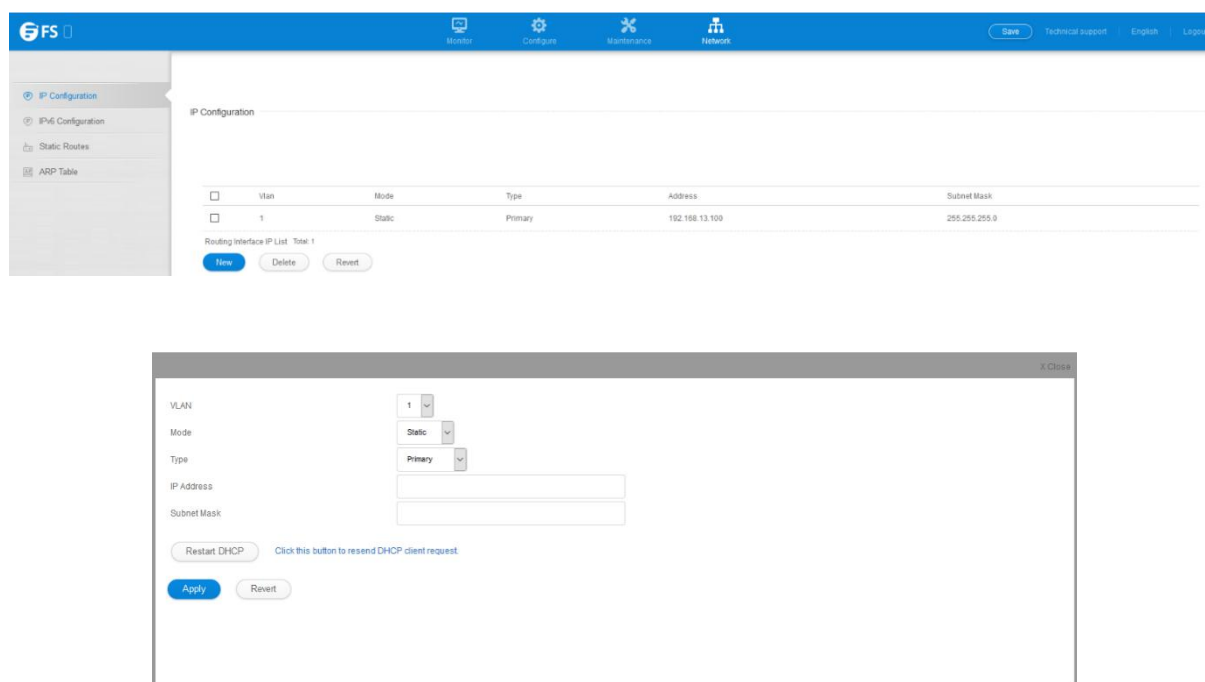
- **VLAN** – ID of the configured VLAN (1-4093). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- **Mode** – Specifies whether IP functionality is enabled via manual configuration (User Specified), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server.

Requests will be broadcast periodically by the switch for an IP address. DHCP/BOOTP responses can include the IP address, subnet mask, and default gateway. (Default: DHCP)

- **Type** – Specifies a primary or secondary IP address. An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this

interface. For initial configuration, set this parameter to Primary. (Options: Primary, Secondary; Default: Primary) Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router or switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.

- **IP Address** – Address of the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: None)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: None)
- **Restart DHCP** – Requests a new IP address from the DHCP server.



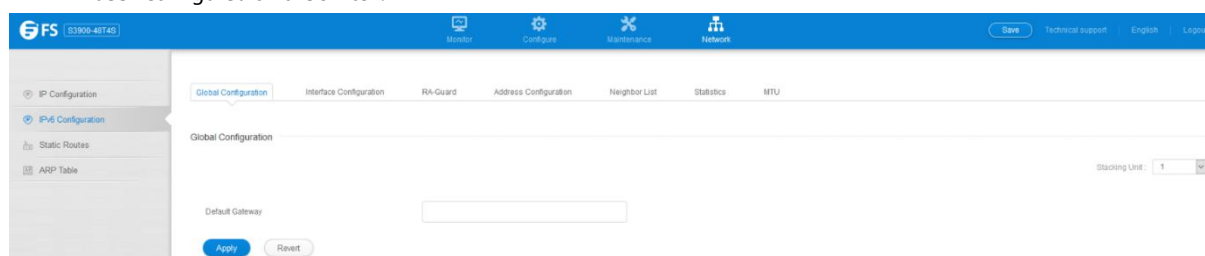
5.2 IPv6 Configuration

This section describes how to configure an IPv6 interface for management access over the network.

5.2.1 Global Configuration

Network > IPv6 Configuration > Global Configuration page is used to configure an IPv6 default gateway for the switch.

- **Default Gateway** – Sets the IPv6 address of the default next hop router.
 - An IPv6 default gateway must be defined if the management station is located in a different IPv6 segment.
 - An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.



5.2.2 Interface Configuration

Network > IPv6 Configuration > Interface Configuration page is used to configure general IPv6 settings for the selected VLAN, including auto-configuration of a global unicast address, explicit configuration of a link local interface address, the MTU size, and neighbor discovery protocol settings for duplicate address detection and the neighbor solicitation interval.

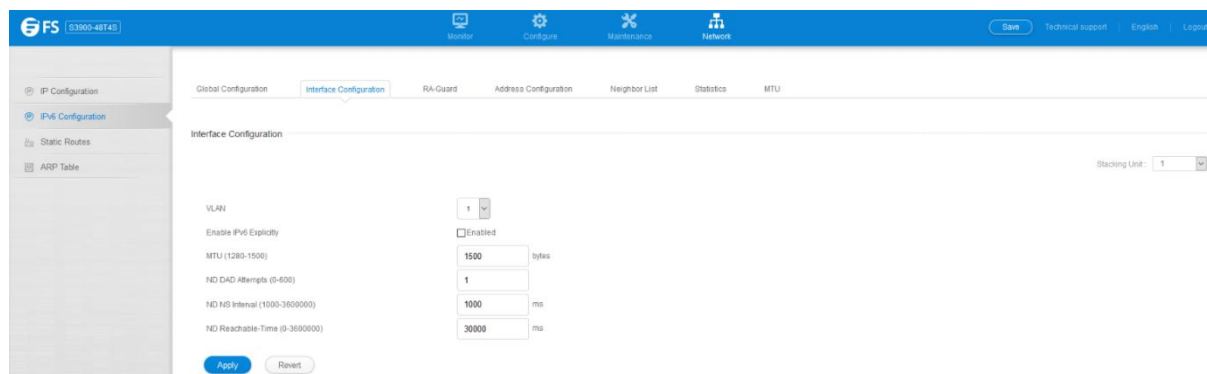
- **VLAN** – ID of a configured VLAN which is to be used for management access. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)
- **Address Autoconfig** – Enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 functionality on that interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier (i.e., the switch's MAC address).
 - If the router advertisements have the "other stateful configuration" flag set, the switch will attempt to acquire other

non-address configuration information (such as a default gateway).

- If auto-configuration is not selected, then an address must be manually configured using the Add Interface page described below.
- **Enable IPv6 Explicitly** – Enables IPv6 on an interface. Note that when an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed. (Default: Disabled) Disabling this parameter does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.
- **MTU** – Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. (Range: 1280-65535 bytes; Default: 1500 bytes)
 - The maximum value set in this field cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.
 - IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
 - All devices on the same physical medium must use the same MTU in order to operate correctly.
 - IPv6 must be enabled on an interface before the MTU can be set. If an IPv6 address has not been assigned to the switch, “N/A” is displayed in the MTU field.
- **ND DAD Attempts** – The number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. (Range: 0-600, Default: 3)
 - Configuring a value of 0 disables duplicate address detection.
 - Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
 - Duplicate address detection is stopped on any interface that has been suspended.

While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.

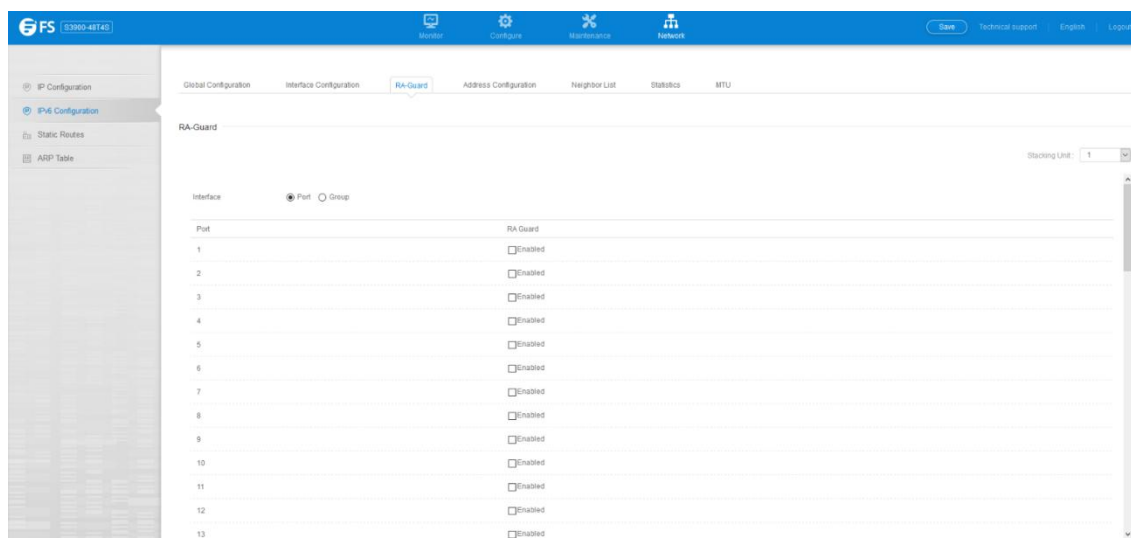
- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other IPv6 addresses remain in a “tentative” state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- If a duplicate address is detected, it is set to “duplicate” state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in “duplicate” state.
- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.
- **ND NS Interval** – The interval between transmitting IPv6 neighbor solicitation messages on an interface. (Range: 1000-3600000 milliseconds; Default: 1000 milliseconds) is used for neighbor discovery operations, 0 milliseconds is advertised in router advertisements. This attribute specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.
- **ND Reachable-Time** – The amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. (Range: 0-3600000 milliseconds; Default: 30000 milliseconds)



5.2.3 RA-Guard

Network >IPv6 Configuration >RA-Guard page is used to configure RA guard status on a port or group.

- **Interface** – Shows port or trunk configuration page.
- **RA Guard** – Blocks incoming Router Advertisement and Router Redirect packets. (Default: Disabled)IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, note that unintended misconfigurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network.RA Guard can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.



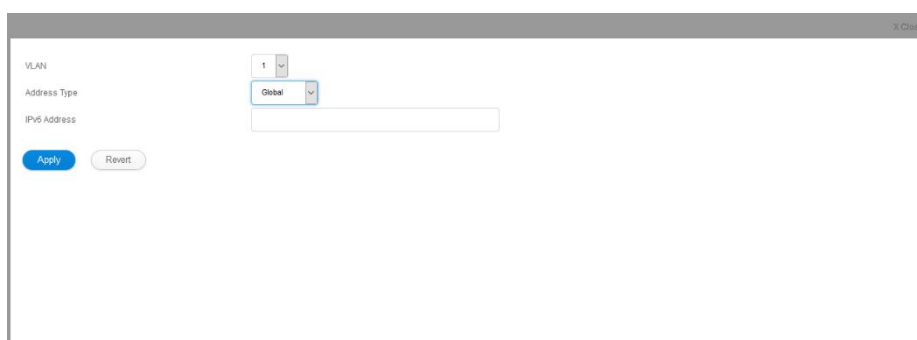
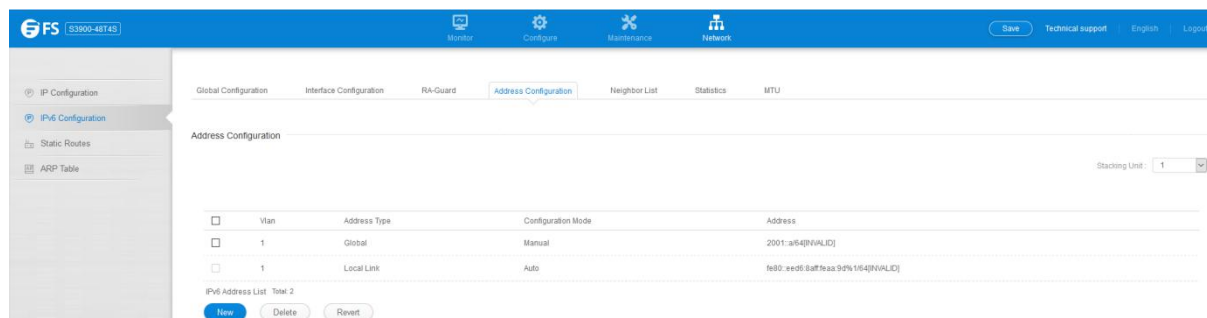
5.2.4 Address Configuration

Network >IPv6 Configuration >Address Configuration page is used to configure anIPv6 interface for management access over the network.

- **VLAN** – ID of a configured VLAN which is to be used for management access. By default, all ports on the switch are members of VLAN 1.However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.(Range: 1-4093)
- **Address Type** – Defines the address type configured for this interface.
 - **Global** – Configures an IPv6 global unicast address with a full IPv6 address including the network prefix and host address bits, followed by a forward slash, and a decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).
 - **EUI-64** (Extended Universal Identifier) – Configures an IPv6 address for an interface using an EUI-64 interface ID in the low

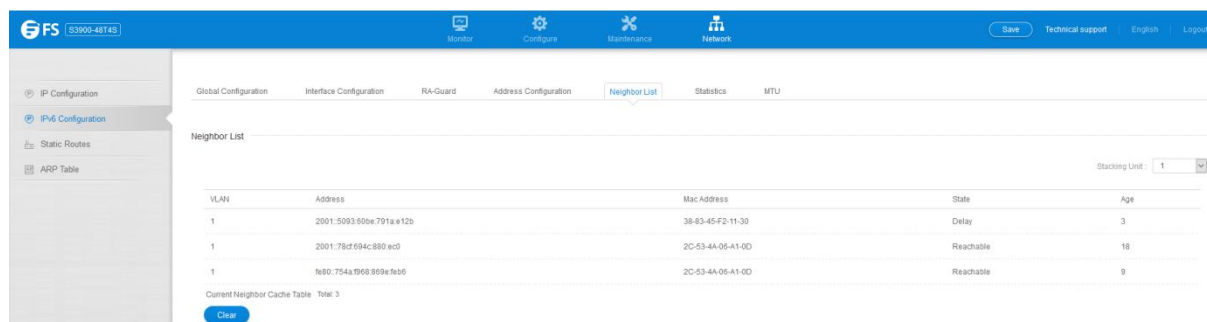
order 64 bits.

- **Link Local** – Configures an IPv6 link-local address.
- **IPv6 Address** – IPv6 address assigned to this interface.



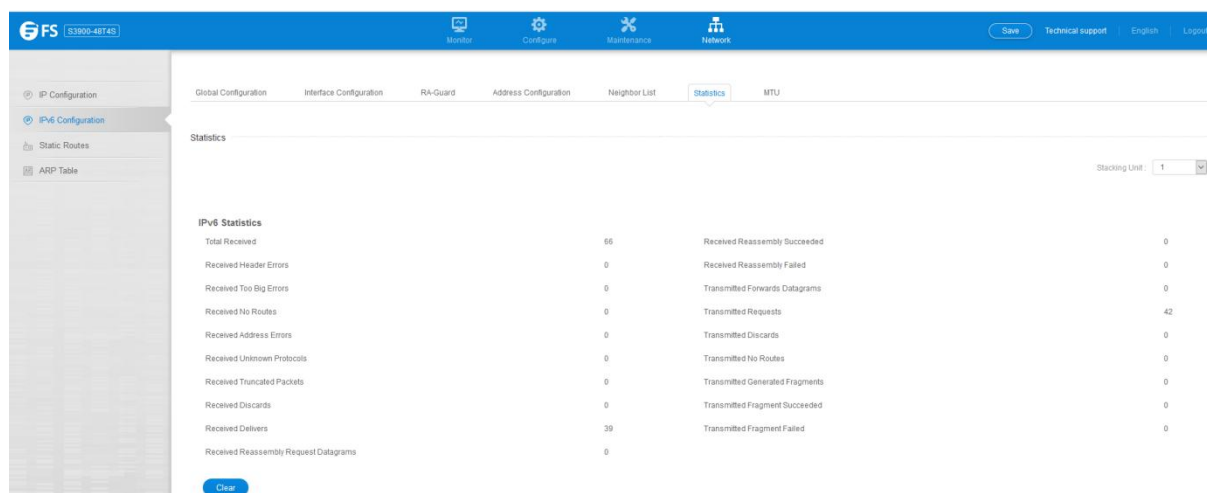
5.2.5 Neighbor List

Network > IPv6 Configuration > Neighbor List page is used to display the IPv6 addresses detected for neighbor devices.



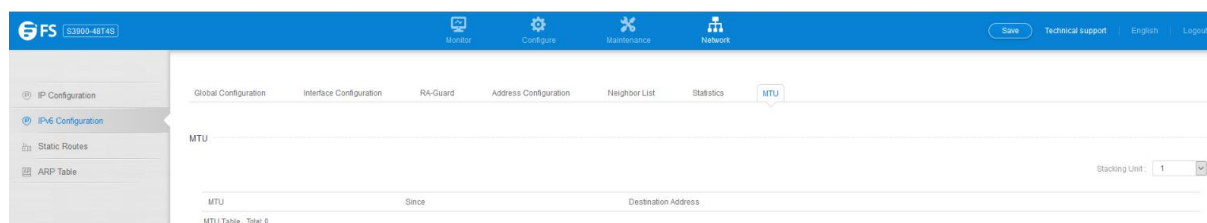
5.2.6 Statistics

Network > IPv6 Configuration > Statistics page is used to display statistics about IPv6 traffic passing through this switch.



5.2.7 MTU

Network > IPv6 Configuration > MTU page is used to display the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

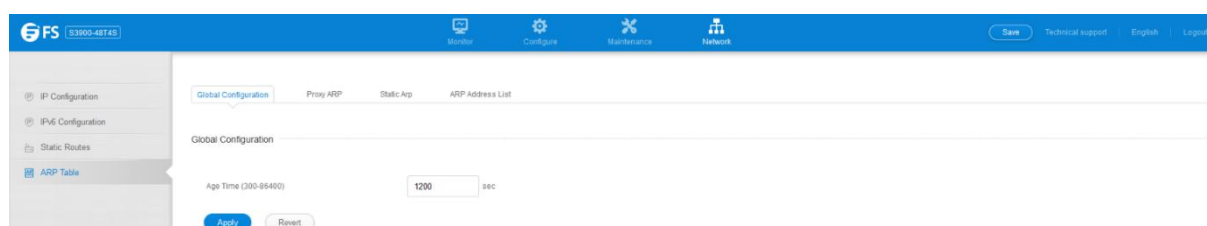


5.3 ARP

5.3.1 Global Configuration

Network > ARP > Global Configuration page is used to set the timeout for ARP entry.

- Age time**—Sets the aging time for dynamic entries in the ARP cache.(Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)The ARP aging timeout can be set for any configured VLAN.The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.



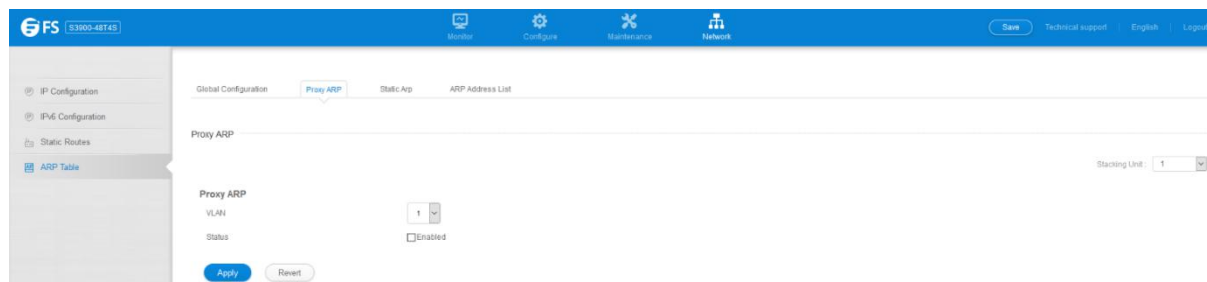
5.3.2 Proxy ARP

Network > ARP > Proxy ARP page is used to enable Proxy ARP for specific VLAN interfaces.

- Proxy ARP**—Enables or disables Proxy ARP for specified VLAN interfaces,allowing a non-routing device to determine the MAC address of a host on another subnet or network. (Default: Disabled)

End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet

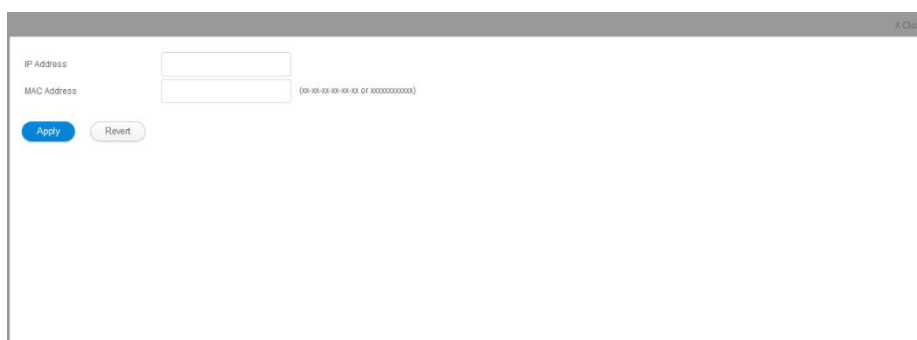
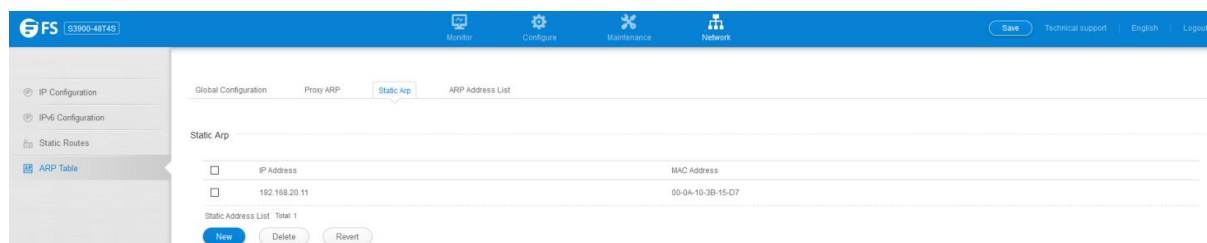
mask than that used by the router or other relevant network devices. Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.



5.3.3 Static ARP

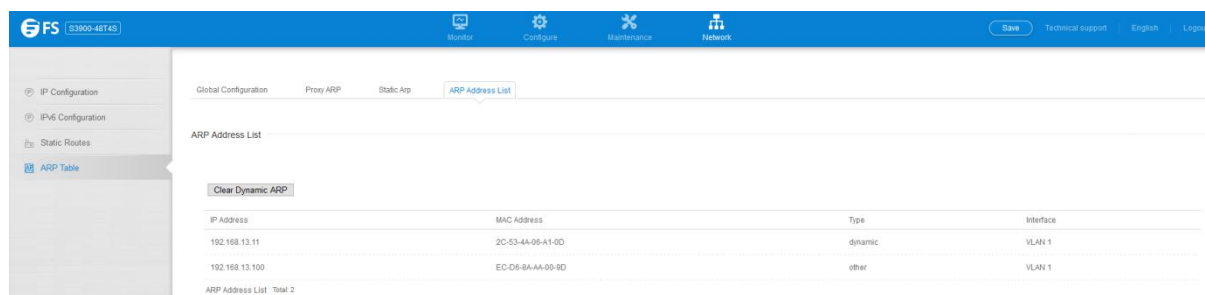
Network > ARP > Static Arp page is used to manually map an IP address to the corresponding physical address in the ARP cache.

- **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)
- **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xx-xx-xx-xx-xx)



5.3.4 ARP Address List

Network > ARP > ARP Address List page is used to display dynamic or local entries in the ARP cache and statistics for ARP messages crossing all interfaces on this router. The ARP cache contains static entries, and entries for local interfaces, including subnet, host, and broadcast addresses. However, most entries will be dynamically learned through replies to broadcast messages.

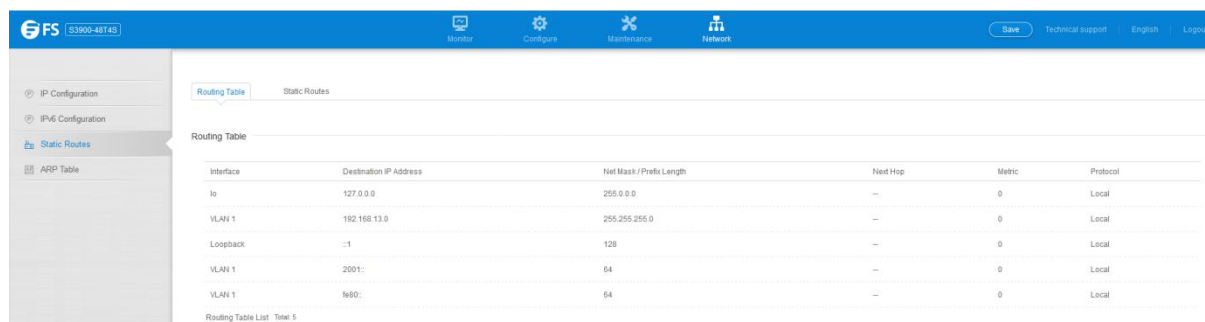


5.4 Static Routes

5.4.1 Routing Table

Network >Static Routes >Routing Table page is used to display all routes that can be accessed via local network interfaces, through static routes, or through a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic (except when the distance parameter of a dynamic route is set to a value that makes its priority exceed that of a static route). Also note that the route for a local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

- **VLAN**—VLAN identifier (i.e., configured as a valid IP subnet).
- **Destination IP Address**— IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
- **Net Mask / Prefix Length**—Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop**—The IP address of the next hop (or gateway) in this route.
- **Metric**—Cost for this interface.
- **Protocol**—The protocol which generated this route information. (Options: Local, Static, RIP, OSPF, Others)



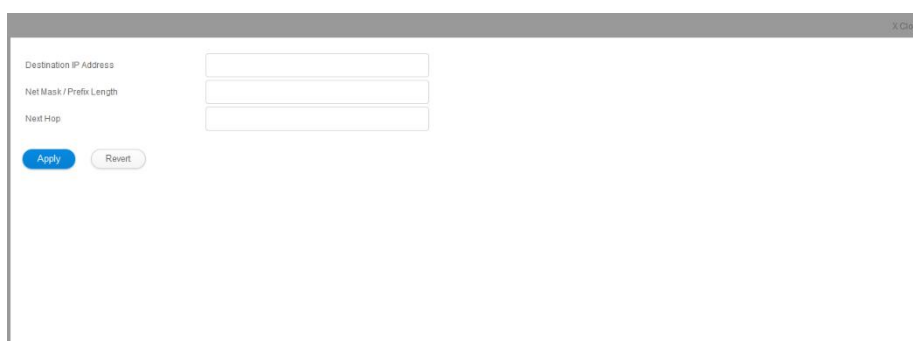
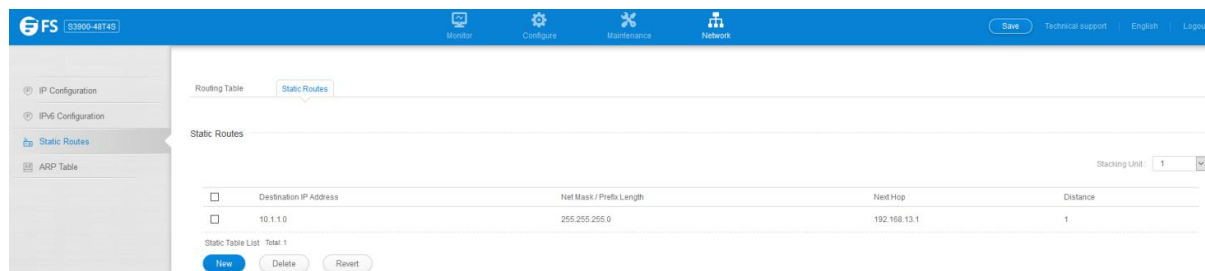
Interface	Destination IP Address	Net Mask / Prefix Length	Next Hop	Metric	Protocol
lo	127.0.0.0	255.0.0.0	—	0	Local
VLAN 1	192.168.13.0	255.255.255.0	—	0	Local
Loopback	::1	128	—	0	Local
VLAN 1	::2001::	64	—	0	Local
VLAN 1	::%8D::	64	—	0	Local

5.4.2 Static Routes

Network >Static Routes >Static Routes page is used to enter static routes in the routing table. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

- **Destination IP Address** — IP address of the destination network, subnetwork, or host.
- **Net Mask / Prefix Length**—Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop**—IP address of the next router hop used for this route.
- **Distance**—An administrative distance indicating that this route can be overridden by dynamic routing information if the distance

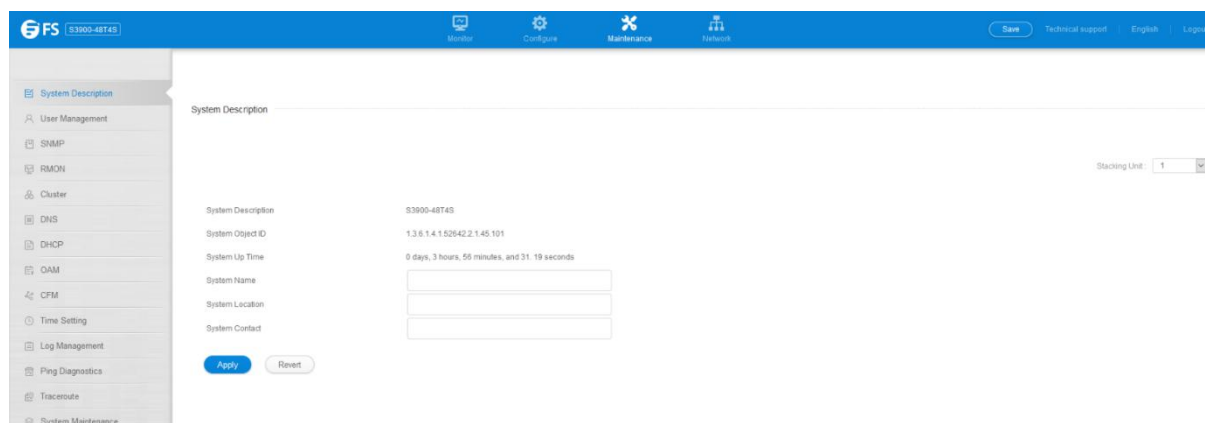
of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF, 120 for RIP, 20 for eBGP, and 200 for iBGP. (Range: 1-255, Default: 1)



6. Maintenance

6.1 System Description

Maintenance > System Description display the information of the firmware and device.



6.2 User Management

Maintenance > User Management page to control management access to the switch based on manually configured user names and passwords.

- **User Name** – The name of the user. (Maximum length: 32 characters; maximum number of users: 16)
- **Access Level** – Specifies the user level. (Options: 0 - Normal, 15 - Privileged) Normal privilege level provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Privileged level provides full access to all commands.

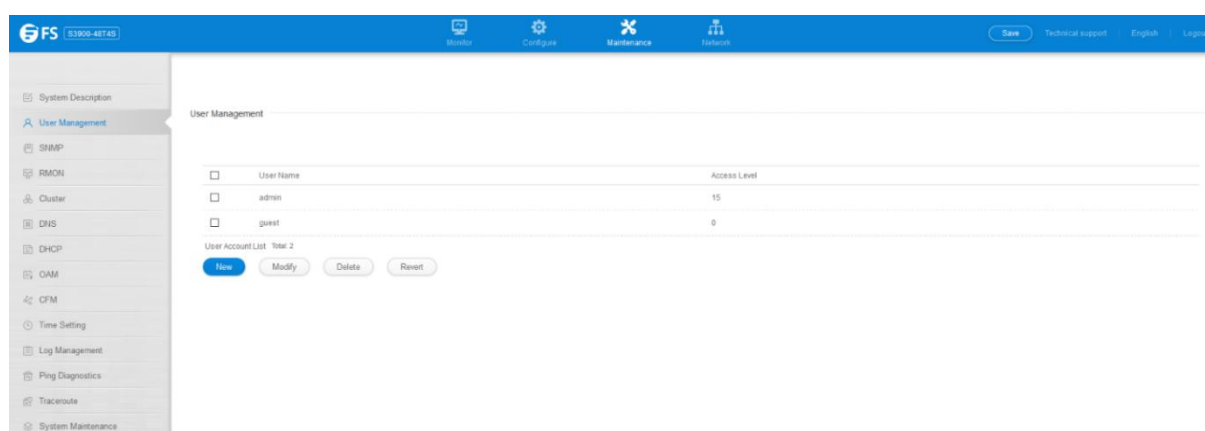
- **Password Type** – Specifies the following options:
 - **No Password** – No password is required for this user to log in.
 - **Plain Password** – Plain text unencrypted password.
 - **Encrypted Password** – Encrypted password.

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP or FTP server. There is no need for you to manually configure encrypted passwords.

- **Password** – Specifies the user password.(Range: 0-32 characters, case sensitive)
- **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

NOTES:

- The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.”

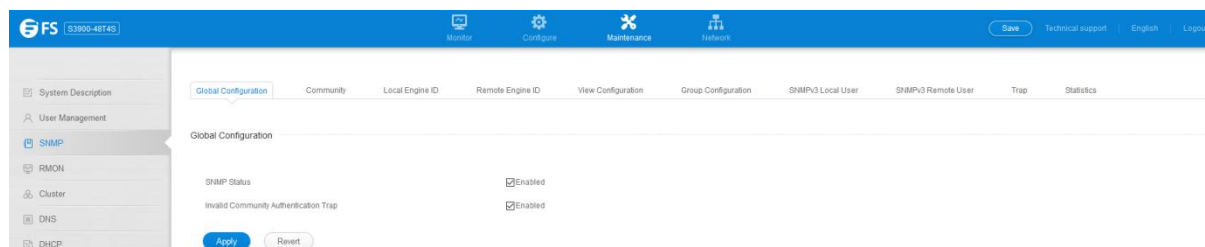


6.3 SNMP

6.3.1 Global Configuration

Maintenance >SNMP >Global Configuration page is used to enable SNMPv3service for all management clients (i.e., versions 1, 2c, 3), and to enable trap messages.

- **Agent Status** – Enables SNMP on the switch. (Default: Enabled)
- **Invalid Community Authentication Trap**– Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)

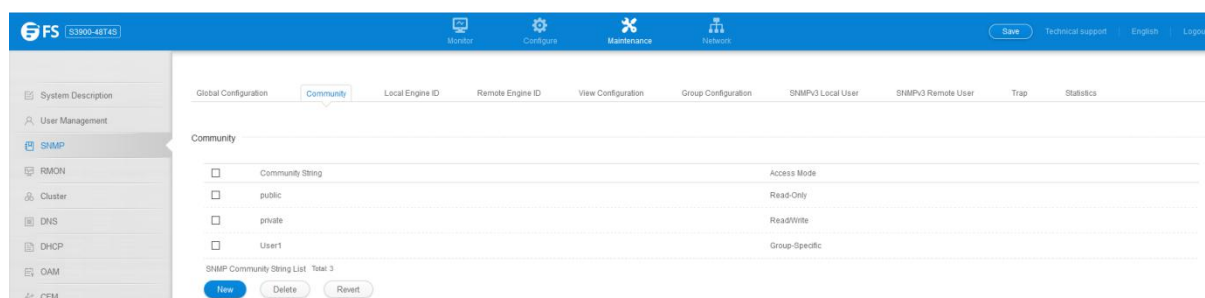


6.3.2 Community

Maintenance >SNMP >Community page is used to configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. For security reasons, you should consider removing the default strings.

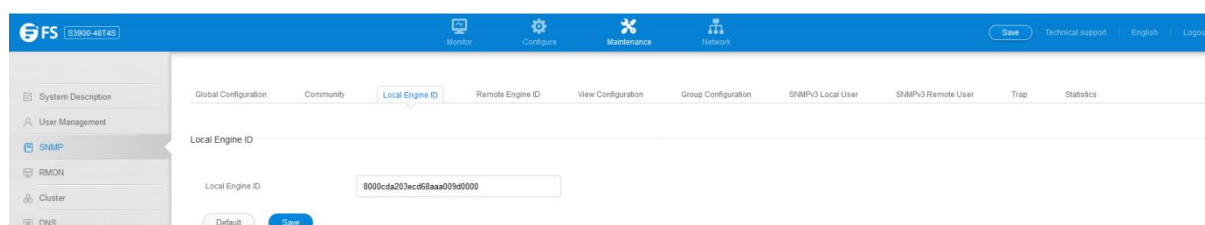
- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.Range: 1-32 characters, case sensitive Default strings: “public” (Read-Only), “private” (Read/Write)

- **Access Mode** – Specifies the access rights for the community string:
 - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
 - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.



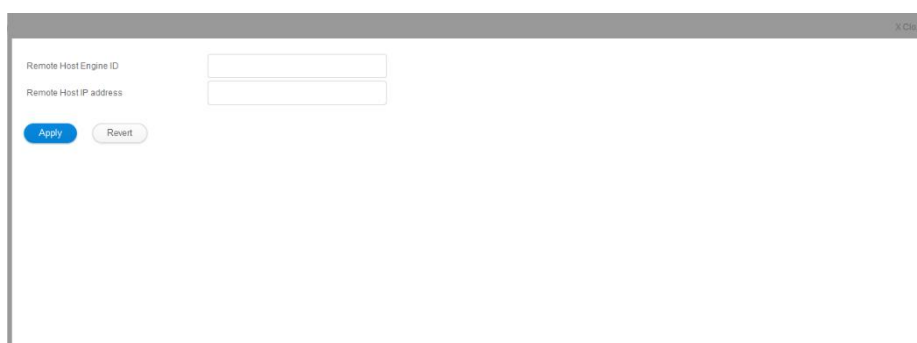
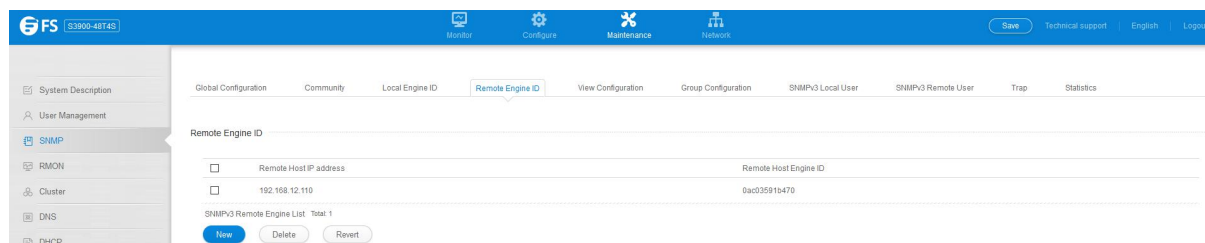
6.3.3 Local Engine ID

The Maintenance >SNMP >Local Engine ID page is used to configure SNMPv3 local engine ID.



6.3.4 Remote Engine ID

The Maintenance >SNMP >Remote Engine ID page is used to configure SNMPv3 remote engine ID.



6.3.5 View Configuration

The Maintenance >SNMP >View Configuration page is used to configure SNMPv3 views which are used to restrict user access to specified portions of the MIB tree. The predefined view “default view” includes access to the entire MIB tree.

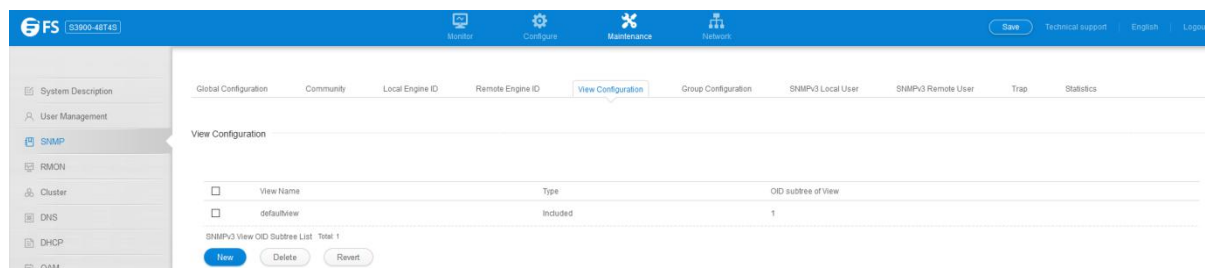
Add View

- **View Name** – The name of the SNMP view. (Range: 1-64 characters)

- **OID Subtree** – Specifies the initial object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. Use the Add OID Subtree page to configure additional object identifiers.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Add OID Subtree

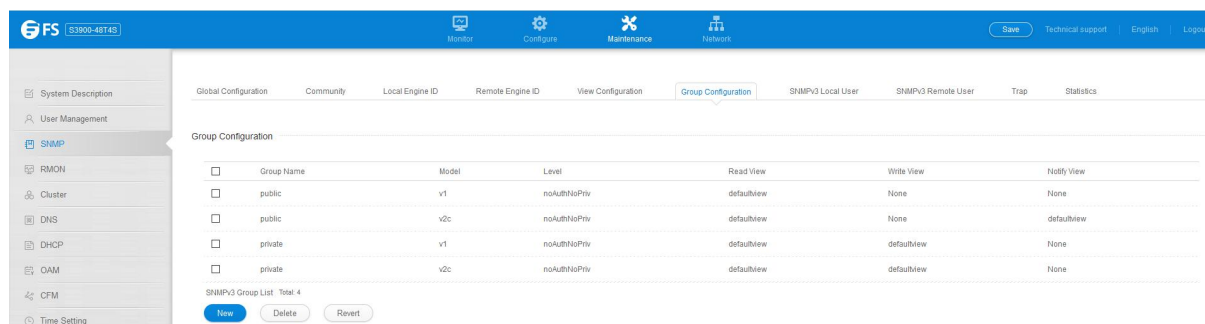
- **View Name** – Lists the SNMP views configured in the Add View page.
- **OID Subtree** – Adds an additional object identifier of a branch within the MIB tree to the selected View. Wild cards can be used to mask a specific portion of the OID string.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.



6.3.6 Group Configuration

Maintenance >SNMP >Group Configuration page is used to add an SNMPv3group which can be used to set the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

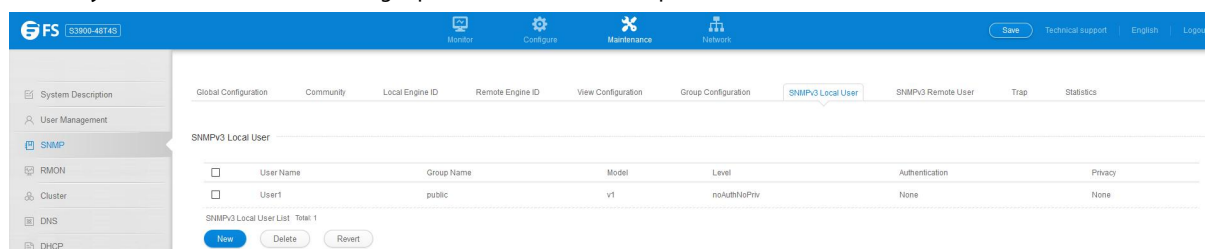
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Read View** – The configured view for read access.(Range: 1-32 characters)
- **Write View** – The configured view for write access.(Range: 1-32 characters)
- **Notify View** – The configured view for notifications.(Range: 1-32 characters)



6.3.7 SNMPv3 Local User

Maintenance >SNMP >SNMPv3 Local User page is used to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch. EachSNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

- **User Name** – The name of user connecting to the SNMP agent.(Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Authentication Protocol** – The method used for user authentication.(Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.



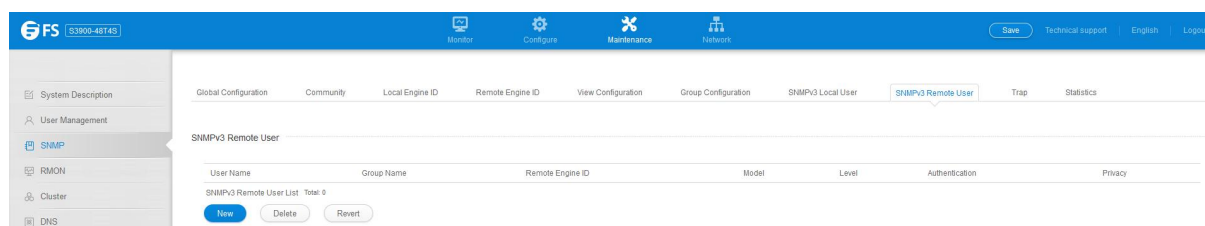


SNMPv3 User configuration dialog box. Fields include: User Name (text input), Group Name (dropdown menu with 'public' selected), Security Model (dropdown menu with 'v1' selected), Security Level (dropdown menu with 'noAuthNoPriv' selected), Authentication Protocol (dropdown menu with 'MD5' selected), Authentication Password (password input), Privacy Protocol (dropdown menu with 'DES56' selected), and Privacy Password (password input). Buttons: Apply, Revert.

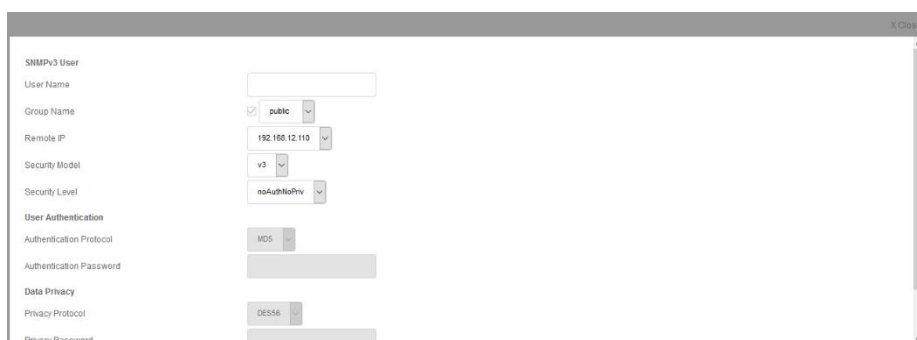
6.3.8 SNMPv3 Remote User

Maintenance >SNMP >SNMPv3 Remote User page is used to identify the source of SNMPv3 inform messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Remote IP** – The Internet address of the remote device where the user resides.
- **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v3)
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.



SNMPv3 Remote User configuration page. The page shows a table with columns: User Name, Group Name, Remote Engine ID, Model, Level, Authentication, and Privacy. Below the table are buttons: New, Delete, and Revert. The page also includes a sidebar with navigation options: System Description, User Management, SNMP, RMON, Cluster, and DNS.



SNMPv3 User configuration dialog box. Fields include: User Name (text input), Group Name (dropdown menu with 'public' selected), Remote IP (dropdown menu with '192.168.12.119' selected), Security Model (dropdown menu with 'v3' selected), Security Level (dropdown menu with 'noAuthNoPriv' selected), User Authentication (dropdown menu with 'MD5' selected), Authentication Password (password input), Data Privacy (dropdown menu with 'DES56' selected), and Privacy Password (password input). Buttons: Apply, Revert.

6.3.9 Trap

Maintenance >SNMP >Trap is used page to specify the host devices to be sent traps and the types of traps to send.

SNMP Version 1

- **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: v1)
- **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.
- **UDP Port** – Specifies the UDP port number used by the trap manager.(Default: 162)

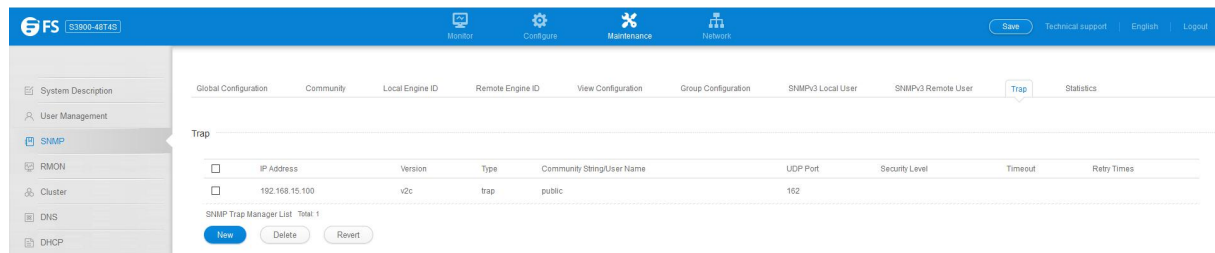
SNMP Version 2c

- **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- Notification Type
 - **Traps** – Notifications are sent as trap messages.
 - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
 - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message.(Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
 - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt.(Range: 0-255; Default: 3)
- **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.
- **UDP Port** – Specifies the UDP port number used by the trap manager.(Default: 162)

SNMP Version 3

- **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- Notification Type
 - **Traps** – Notifications are sent as trap messages.
 - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
 - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message.(Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
 - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt.(Range: 0-255; Default: 3)
- **Local User Name** – The name of a local user which is used to identify the source of SNMPv3 trap messages sent from the local switch.(Range: 1-32 characters)If an account for the specified user has not been created , one will be automatically generated.
- **Remote User Name** – The name of a remote user which is used to identify the source of SNMPv3 inform messages sent from the local switch. (Range: 1-32 characters)If an account for the specified user has not been created , one will be automatically generated.
- **UDP Port** – Specifies the UDP port number used by the trap manager.(Default: 162)
- **Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.

- **AuthPriv** – SNMP communications use both authentication and encryption.

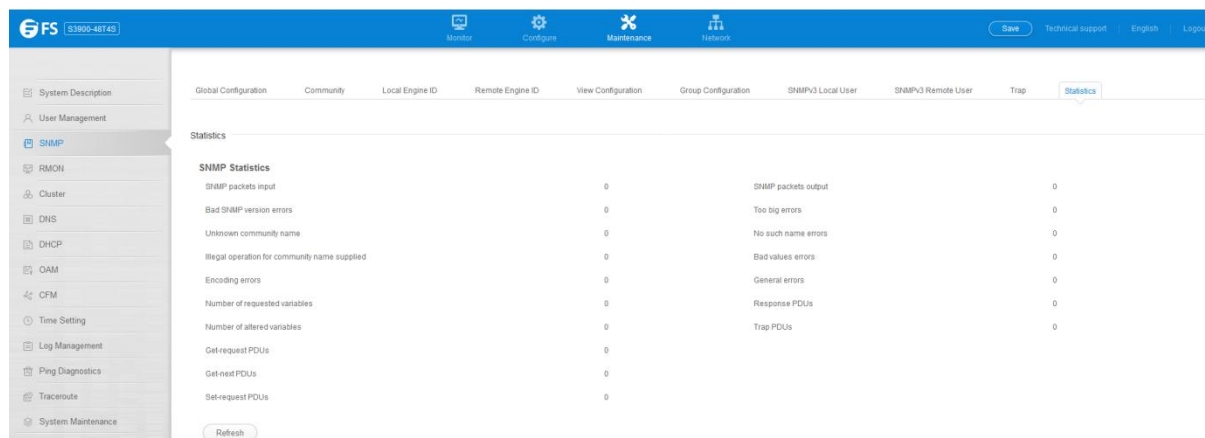



6.3.10 Statistics

Maintenance >SNMP >Statistics page is used to show counters for SNMP input and output protocol data units.

- **SNMP packets input** – The total number of messages delivered to the SNMP entity from the transport service.
- **Bad SNMP version errors** – The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
- **Unknown community name** – The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
- **Illegal operation for community name supplied** – The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
- **Encoding errors** – The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
- **Number of requested variables** – The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
- **Number of altered variables** – The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
- **Get-request PDUs** – The total number of SNMP Get-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- **Get-next PDUs** – The total number of SNMP Get-Next PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- **Set-request PDUs** – The total number of SNMP Set-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- **SNMP packets output** – The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
- **Too big errors** – The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is "tooBig."
- **No such name errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is "noSuchName."

- **Bad values errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is “badValue.”
- **General errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is “genErr.”
- **Response PDUs** – The total number of SNMP Get-Response PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.
- **Trap PDUs** – The total number of SNMP Trap PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.



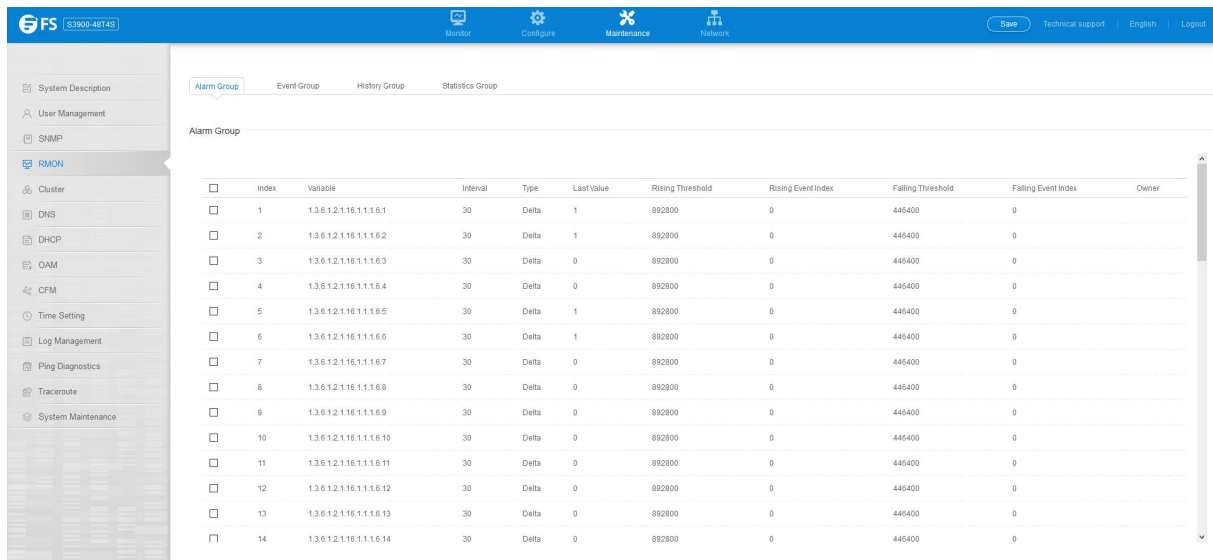
Statistics			
SNMP Statistics			
SNMP packets input	0	SNMP packets output	0
Bad SNMP version errors	0	Too big errors	0
Unknown community name	0	No such name errors	0
Illegal operation for community name supplied	0	Bad values errors	0
Encoding errors	0	General errors	0
Number of requested variables	0	Response PDUs	0
Number of altered variables	0	Trap PDUs	0
Get-request PDUs	0		
Get-next PDUs	0		
Set-request PDUs	0		

6.4 RMON

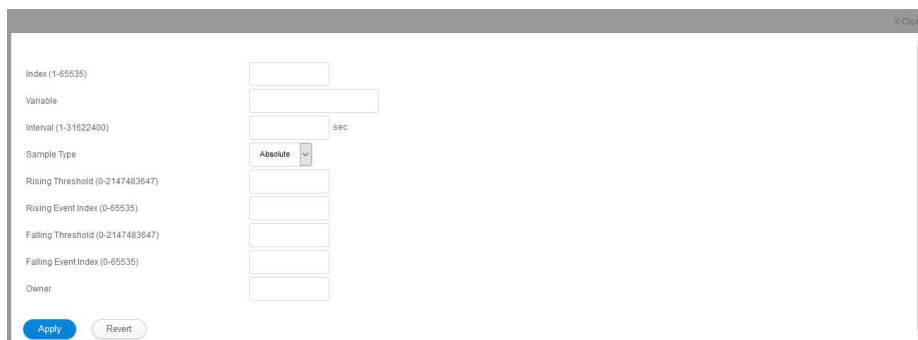
6.4.1 Alarm Group

Maintenance >RMON >Alarm Group page is used to define specific criteria that will generate response events.

- **Index** – Index to this entry. (Range: 1-65535)
- **Variable** – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.
- **Interval** – The polling interval. (Range: 1-31622400 seconds)
- **Sample Type** – Tests for absolute or relative changes in the specified variable.
 - **Absolute** – The variable is compared directly to the thresholds at the end of the sampling period.
 - **Delta** – The last sample is subtracted from the current value and the difference is then compared to the thresholds.
- **Rising Threshold** – If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold.(Range: 0-2147483647)
- **Rising Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing above the rising threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)
- **Falling Threshold** – If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold.(Range: 0-2147483647)
- **Falling Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing below the falling threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)
- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)



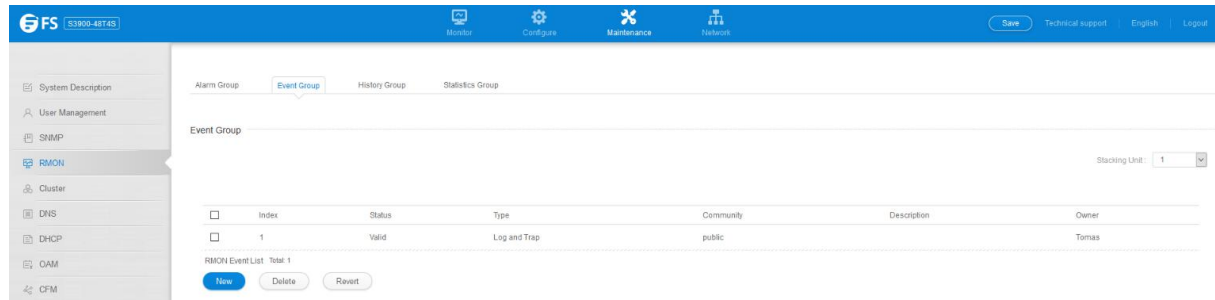
<input type="checkbox"/>	Index	Variable	Interval	Type	Last Value	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner
<input type="checkbox"/>	1	1.3.6.1.2.1.16.1.1.1.6.1	30	Delta	1	892800	0	445400	0	
<input type="checkbox"/>	2	1.3.6.1.2.1.16.1.1.1.6.2	30	Delta	1	892800	0	445400	0	
<input type="checkbox"/>	3	1.3.6.1.2.1.16.1.1.1.6.3	30	Delta	0	892800	0	445400	0	
<input type="checkbox"/>	4	1.3.6.1.2.1.16.1.1.1.6.4	30	Delta	0	892800	0	445400	0	
<input type="checkbox"/>	5	1.3.6.1.2.1.16.1.1.1.6.5	30	Delta	1	892800	0	445400	0	
<input type="checkbox"/>	6	1.3.6.1.2.1.16.1.1.1.6.6	30	Delta	1	892800	0	445400	0	
<input type="checkbox"/>	7	1.3.6.1.2.1.16.1.1.1.6.7	30	Delta	0	892800	0	445400	0	
<input type="checkbox"/>	8	1.3.6.1.2.1.16.1.1.1.6.8	30	Delta	0	892800	0	445400	0	
<input type="checkbox"/>	9	1.3.6.1.2.1.16.1.1.1.6.9	30	Delta	0	892800	0	445400	0	
<input type="checkbox"/>	10	1.3.6.1.2.1.16.1.1.1.6.10	30	Delta	0	892800	0	445400	0	
<input type="checkbox"/>	11	1.3.6.1.2.1.16.1.1.1.6.11	30	Delta	0	892800	0	445400	0	
<input type="checkbox"/>	12	1.3.6.1.2.1.16.1.1.1.6.12	30	Delta	0	892800	0	445400	0	
<input type="checkbox"/>	13	1.3.6.1.2.1.16.1.1.1.6.13	30	Delta	0	892800	0	445400	0	
<input type="checkbox"/>	14	1.3.6.1.2.1.16.1.1.1.6.14	30	Delta	0	892800	0	445400	0	



6.4.2 Event Group

Maintenance >RMON >Event Group page is used to set the action to take when an alarm is triggered. The response can include logging the alarm or sending a message to a trap manager. Alarms and corresponding events provide a way of immediately responding to critical network problems.

- **Index** – Index to this entry. (Range: 1-65535)
- **Type** – Specifies the type of event to initiate:
 - **None** – No event is generated.
 - **Log** – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging.
 - **Trap** – Sends a trap message to all configured trap managers.
 - **Log and Trap** – Logs the event and sends a trap message.
- **Community** – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page prior to configuring it here. (Range: 1-127 characters)
- **Description** – A comment that describes this event. (Range: 1-127 characters)
- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)



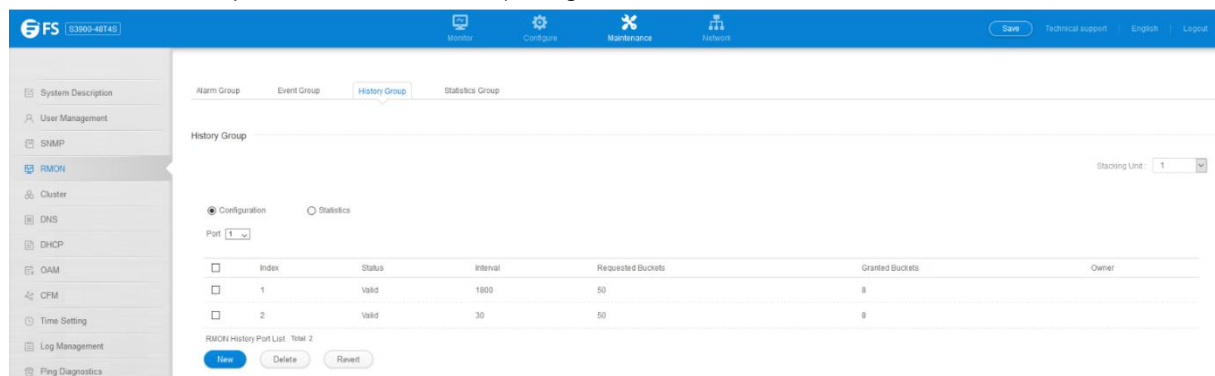
6.4.3 History Group

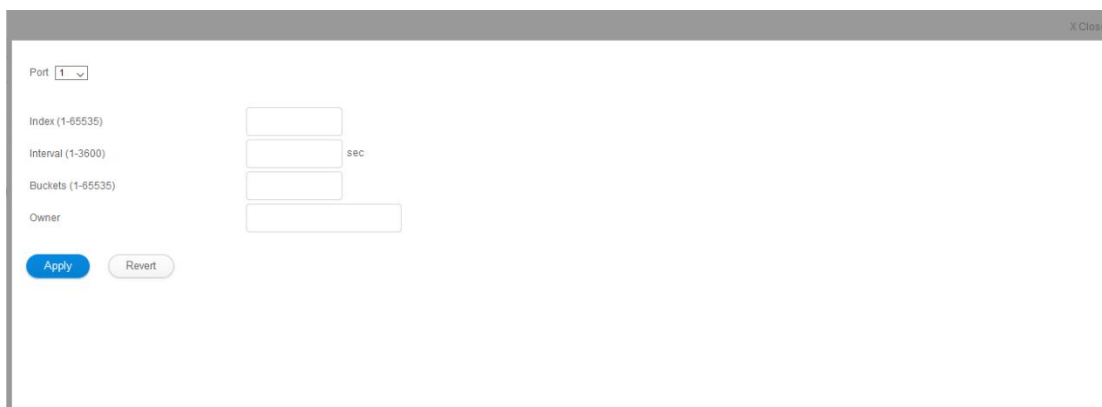
Maintenance >RMON >History Group page is used to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A historical record of activity can be used to track down intermittent problems.

- **Port** – The port number on the switch.
- **Index** - Index to this entry. (Range: 1-65535)
- **Interval** - The polling interval. (Range: 1-3600 seconds; Default: 1800seconds)
- **Buckets** - The number of buckets requested for this entry.(Range: 1-65536; Default: 50)

The number of buckets granted are displayed on the Show page.

- **Owner** - Name of the person who created this entry. (Range: 1-127characters)





Port

Index (1-65535)

Interval (1-3600) sec

Buckets (1-65535)

Owner

6.4.4 Statistics Group

Maintenance > RMON > Statistics Group page is used to collect statistics on a port, which can subsequently be used to monitor the network for common errors and overall traffic rates.

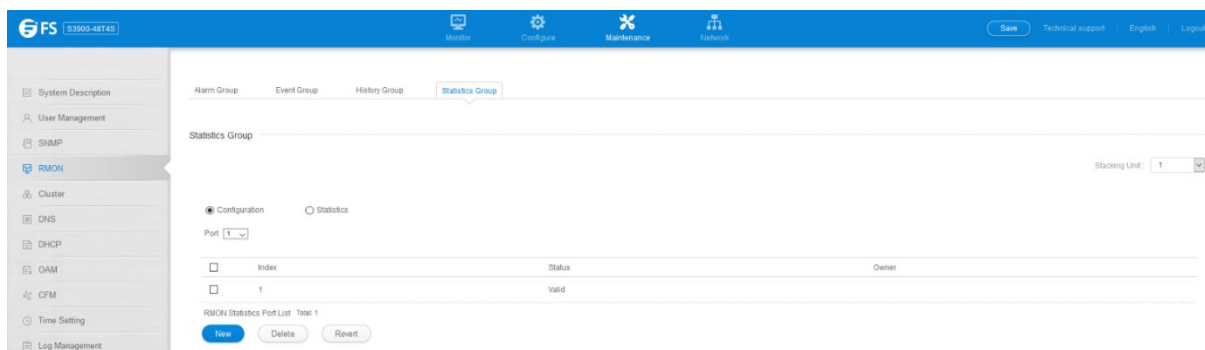
COMMAND USAGE

- If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made.
- The information collected for each entry includes: input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, CRC alignment errors, jabbers, fragments, collisions, drop events, and frames of various sizes.

PARAMETERS

These parameters are displayed:

- **Port** – The port number on the switch.
- **Index** - Index to this entry. (Range: 1-65535)
- **Owner** - Name of the person who created this entry. (Range: 1-127characters)



FS S3900-48T4S

Menu Configure Maintenance Network

Save Technical support English Logout

Alarm Group Event Group History Group **Statistics Group**

Statistics Group

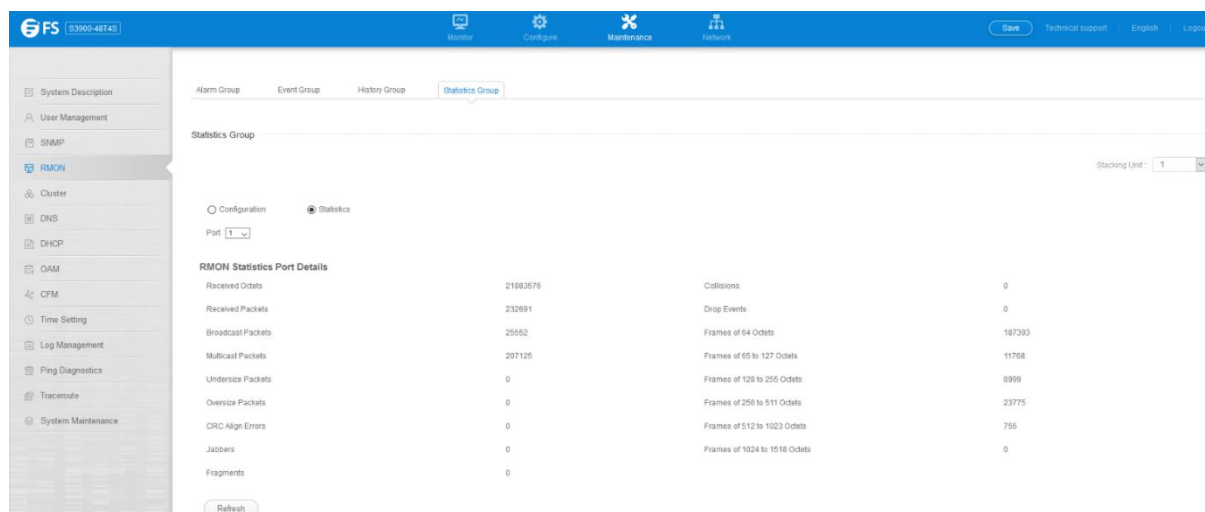
Stacking Unit:

☒ Configuration ☐ Statistics

Port

<input type="checkbox"/>	Index	Status	Owner
<input type="checkbox"/>	1	Valid	

RMON Statistics Port List Total: 1



6.5 Cluster

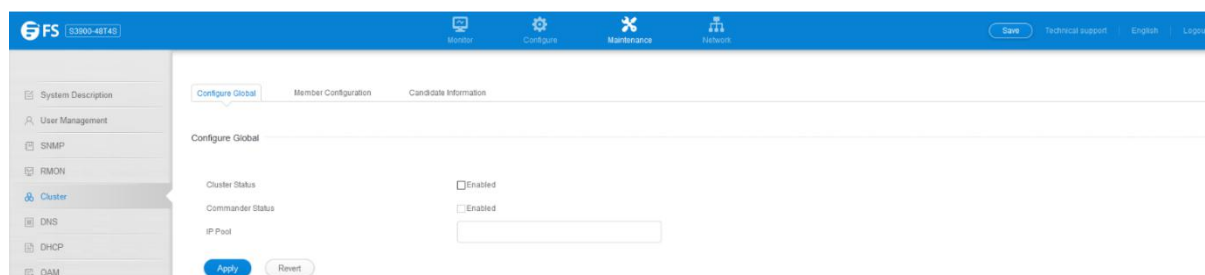
Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

6.5.1 Global Configuration

Maintenance > Cluster > Global Configuration page is used to create a switch cluster.

- **Cluster Status** – Enables or disables clustering on the switch. (Default: Disabled)
- **Commander Status** – Enables or disables the switch as a cluster Commander. (Default: Disabled)
- **IP Pool** – An “internal” IP address pool that is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1

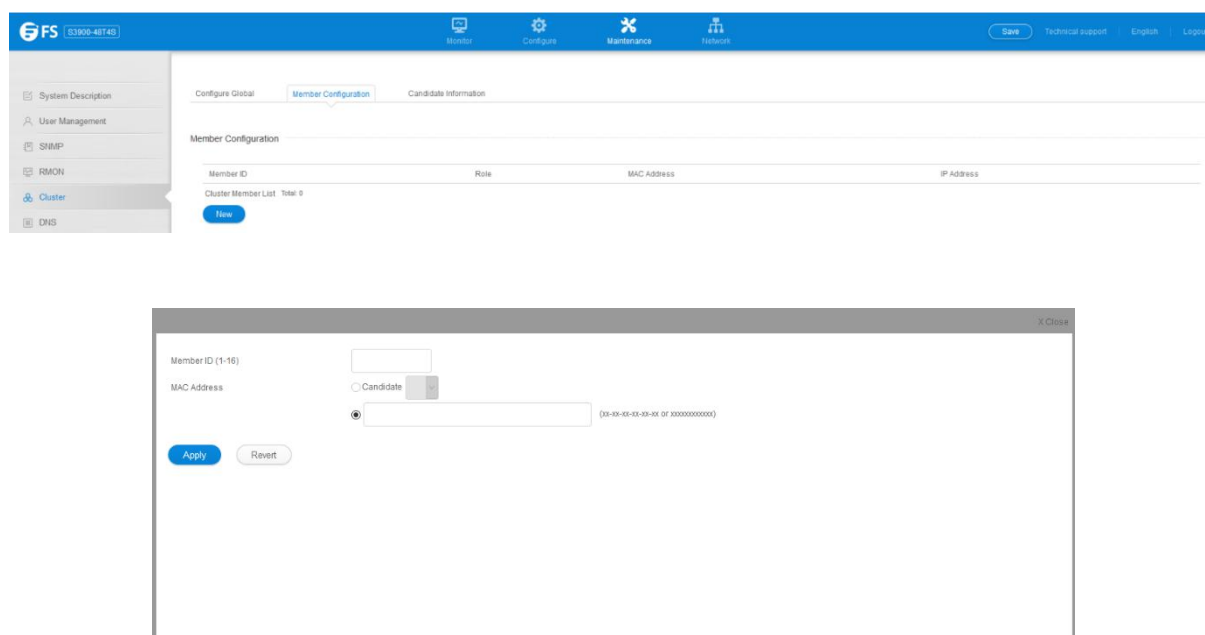
and 36. Note that you cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled. (Default: 10.254.254.1)



6.5.2 Member Configuration

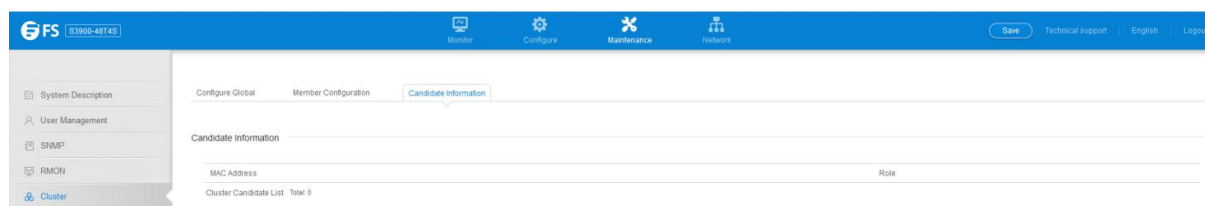
Maintenance > Cluster > Member Configuration page is used to add Candidate switches to the cluster as Members.

- **Member ID** – Specify a Member ID number for the selected Candidate switch. (Range: 1-36)
- **MAC Address** – Select a discovered switch MAC address from the Candidate Table, or enter a specific MAC address of a known switch.



6.5.3 Candidate Information

Maintenance >Cluster >Candidate Information page is used to show Candidate.



6.6 DNS

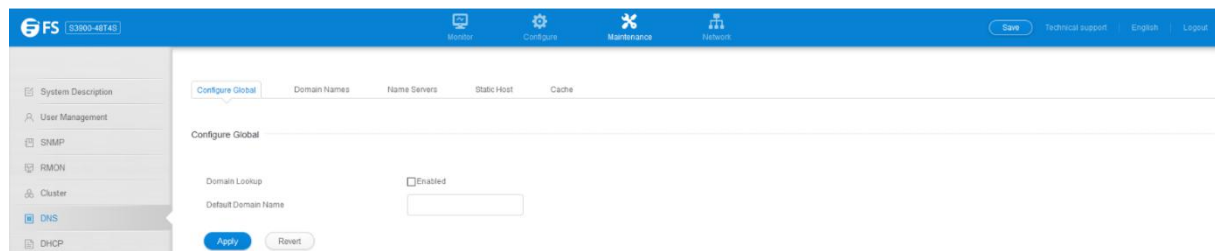
DNS service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response. You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

6.6.1 Global Configuration

Maintenance >DNS >Global Configuration page is used to enable domain lookup and set the default domain name.

- **Domain Lookup** – Enables DNS host name-to-address translation.(Default: Disabled)
- **Default Domain Name** – Defines the default domain name appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name.

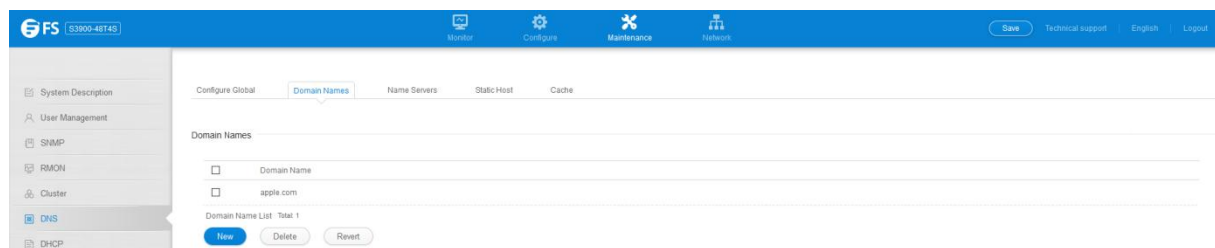
(Range: 1-127 alphanumeric characters)



6.6.2 Domain Names

Maintenance > DNS > Domain Names page is used to configure domain names that can be appended to incomplete host names.

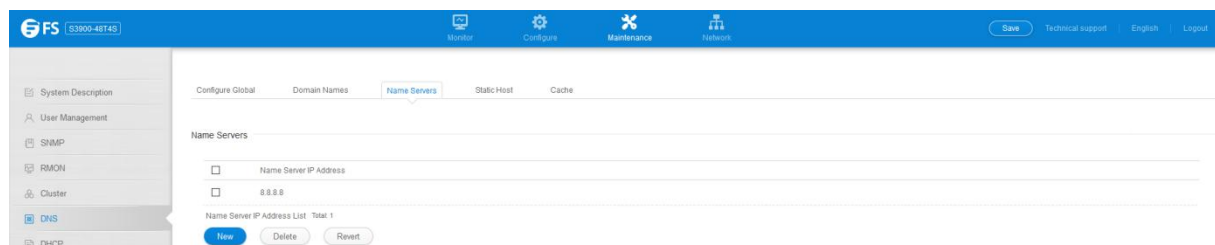
Domain Name – Specifies name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)



6.6.3 Name Servers

Maintenance > DNS > Name Servers is used page to configure a list of name servers to be tried in sequential order.

Name Server IP Address – Specifies the IPv4 or IPv6 address of a domain name server to use for name-to-address resolution. Up to six IP addresses can be added to the name server list.

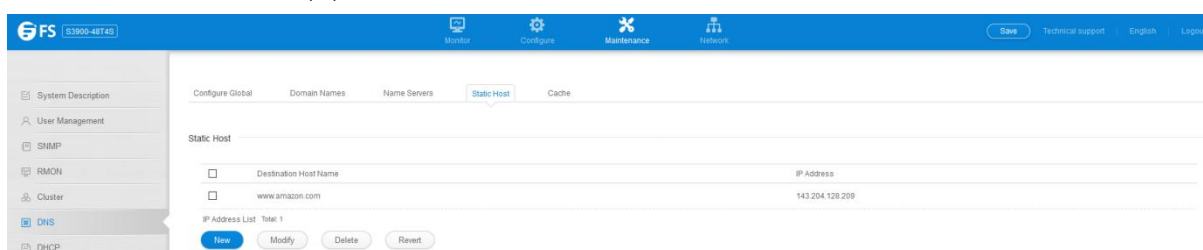




6.6.4 Static Table

Maintenance > DNS > Static Table page is used to manually configure static entries in the DNS table that are used to map domain names to IP addresses.

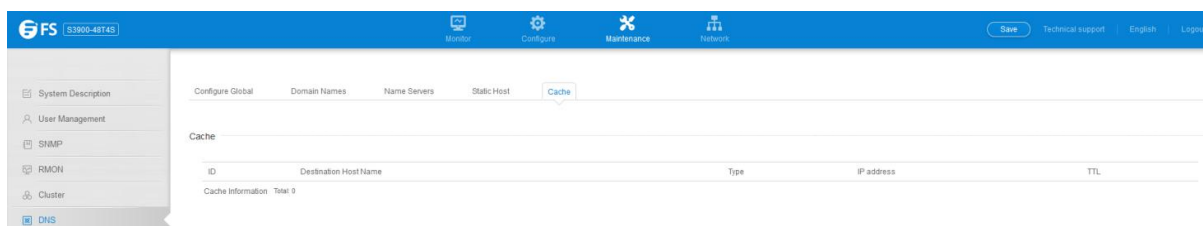
- **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-127 characters)
- **IP Address** – Internet address(es) associated with a host name.




6.6.5 Cache

Maintenance > DNS > Cache page is used to display entries in the DNS cache that have been learned via the designated name servers.

- **ID.** – The entry number for each resource record.
- **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- **IP address** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Host** – The host name associated with this record.

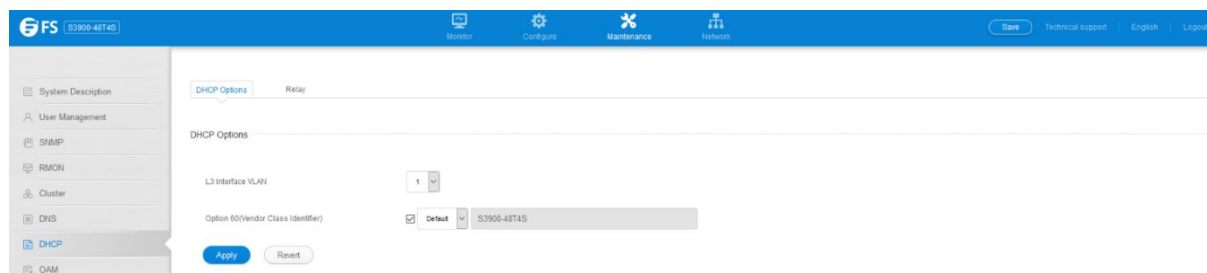


6.7 DHCP

6.7.1 DHCP Options

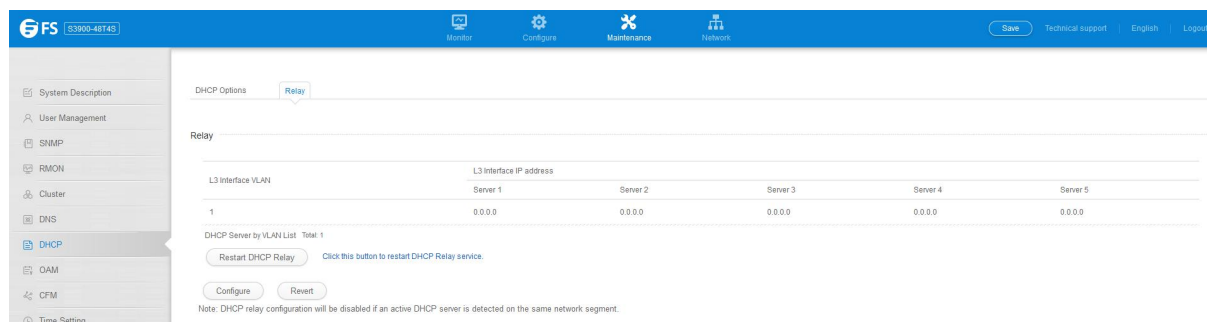
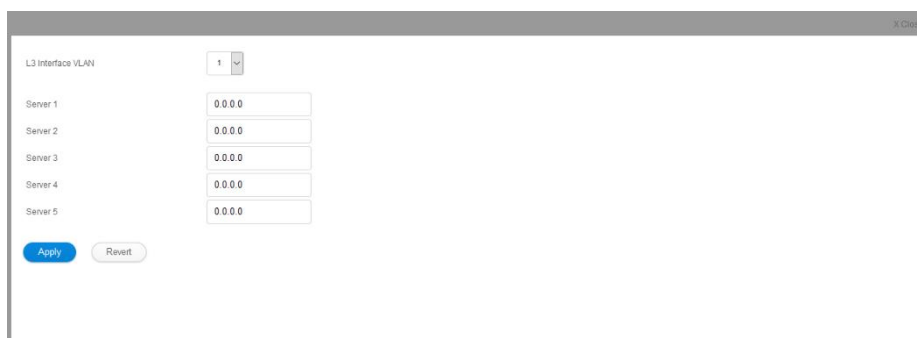
Maintenance > DHCP > DHCP Options page is used to specify the DHCP client identifier for a VLAN interface.

- **L3 Interface VLAN** – ID of configured VLAN.
- **Vendor Class ID** – The following options are supported when the check box is marked to enable this feature:
 - **Default** – The default string is S3900-48T4S.
 - **Text** – A text string. (Range: 1-32 characters)
 - **Hex** – A hexadecimal value. (Range: 1-64 characters)



6.7.2 Relay

- **L3 Interface VLAN ID**—ID of configured VLAN.
- **Server IP Address**—Addresses of DHCP servers or relay servers to be used by the switch's DHCP relay agent in order of preference.
- **Restart DHCP Relay**—Use this button to re-initialize DHCP relay service.

6.8 OAM

6.8.1 Interface

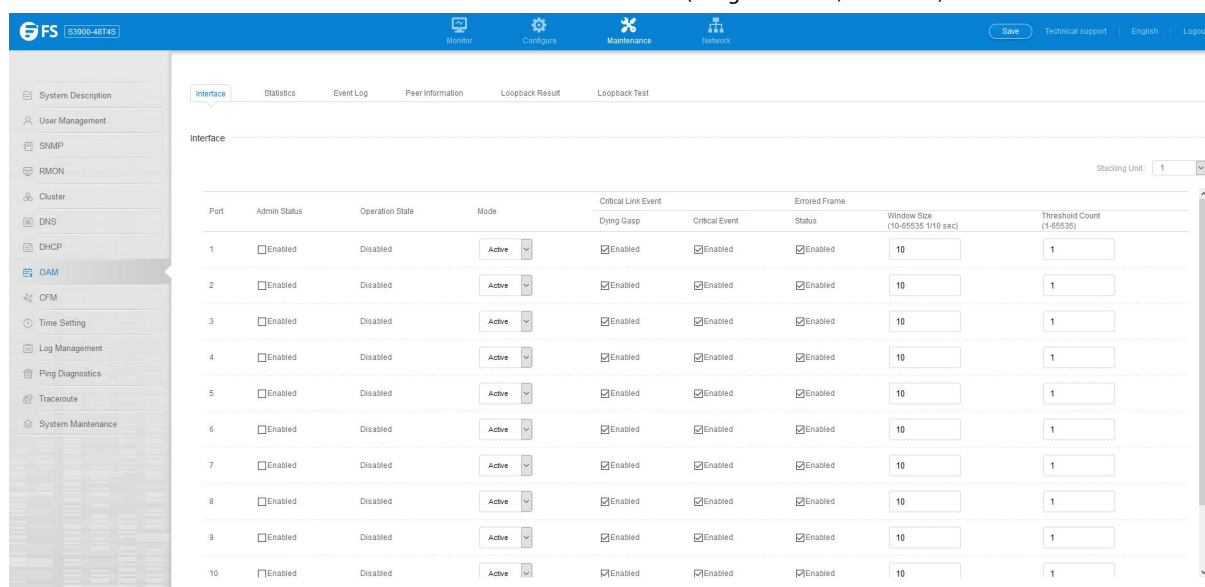
The Maintenance > OAM > Interface page is used to enable OAM functionality on the selected port. Not all CPEs support operation and maintenance functions, so OAM is therefore disabled by default. If a CPE supports OAM, this functionality must first be enabled on the

connected port to gain access to the configuration functions provided under the OAM menu.

- **Port** – Port identifier. (Range: 1-28)
- **Admin Status** – Enables or disables OAM functions.(Default: Disabled)
- **Operation State** – Shows the operational state between the local and remote OAM devices. This value is always “disabled” if OAM is disabled on the local interface.

OAM Operation State

- **Mode** – Sets the OAM operation mode. (Default: Active)
 - **Active** – All OAM functions are enabled.
 - **Passive** – All OAM functions are enabled, except for OAM discovery, sending variable request OAMPDUs, and sending loopback control OAMPDUs.
- **Critical Link Event** – Controls reporting of critical link events to its OAM peer.
 - **Dying Gasp** – If an unrecoverable condition occurs, the local OAM entity (i.e., this switch) indicates this by immediately sending a trap message. (Default: Enabled)Dying gasp events are caused by an unrecoverable failure, such as a power failure or device reset.
 - **Critical Event** – If a critical event occurs, the local OAM entity indicates this to its peer by setting the appropriate flag in the next OAMPDU to be sent and stores this information in its OAM event log.(Default: Enabled)Critical events include various failures, such as abnormal voltage fluctuations, out-of-range temperature detected, fan failure, CRC error in flash memory, insufficient memory, or other hardware faults.
- **Errored Frame** – Controls reporting of errored frame link events.An errored frame is a frame in which one or more bits are errored.An errored frame link event occurs if the threshold is reached or exceeded within the specified period.If reporting is enabled and an errored frame link event occurs, the local OAM entity (this switch) sends an Event Notification OAMPDU to the remote OAM entity. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.
 - **Status** – Enables reporting of errored frame link events.(Default: Enabled)
 - **Window Size** – The period of time in which to check the reporting threshold for errored frame link events. (Range: 10-65535 in units of 10 milliseconds; Default: 10 units of 10 milliseconds, or the equivalent of 1 second)
 - **Threshold Count** – The threshold for errored frame link events.(Range: 1-65535; Default: 1)



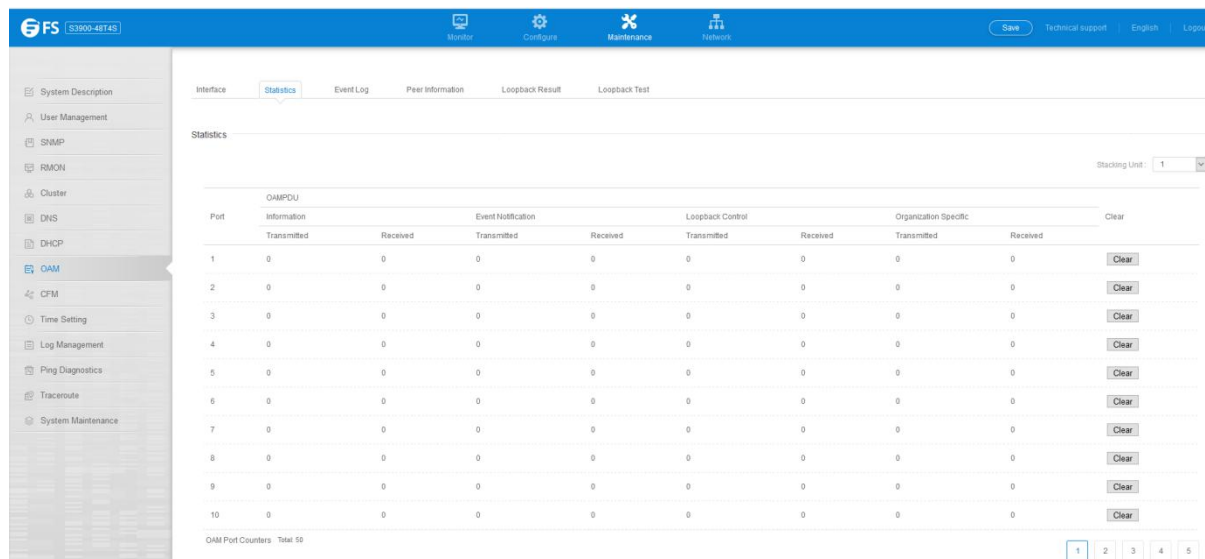
Port	Admin Status	Operation State	Mode	Critical Link Event		Errored Frame	Window Size (10-65535 1/10 sec)	Threshold Count (1-65535)
				Dying Gasp	Critical Event	Status		
1	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
2	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
3	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
4	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
5	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
6	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
7	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
8	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
9	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
10	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1

6.8.2 Statistics

The Maintenance >OAM >Statistics page is used to display statistics for the various types of OAM messages passed across each port.

- **Port** – Port identifier. (Range: 1-28)

- **Clear** – Clears statistical counters for the selected ports.
- **OAMPDU** – Message types transmitted and received by the OAM protocol, including Information OAMPDUs, unique Event OAMPDUs, Loopback Control OAMPDUs, and Organization Specific OAMPDUs.



Port	OAMPDU Information		Event Notification		Loopback Control		Organization Specific		Clear
	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	
1	0	0	0	0	0	0	0	0	Clear
2	0	0	0	0	0	0	0	0	Clear
3	0	0	0	0	0	0	0	0	Clear
4	0	0	0	0	0	0	0	0	Clear
5	0	0	0	0	0	0	0	0	Clear
6	0	0	0	0	0	0	0	0	Clear
7	0	0	0	0	0	0	0	0	Clear
8	0	0	0	0	0	0	0	0	Clear
9	0	0	0	0	0	0	0	0	Clear
10	0	0	0	0	0	0	0	0	Clear

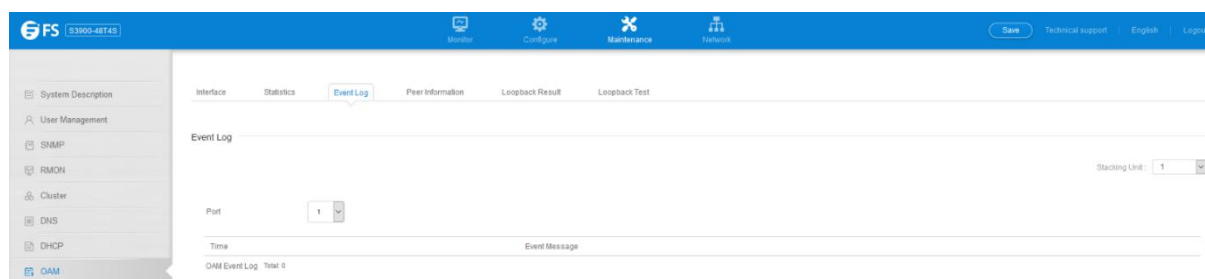
OAM Port Counters: Total 50

6.8.3 Event Log

The Maintenance >OAM >Event Log page is used to display link events for the selected port.

To display link events for the selected port:

1. Click Maintenance, OAM, Event Log.
2. Select a port from the drop-down list.



Port: 1

Time: Event Message

OAM Event Log: Total 0

6.8.4 Peer Information

The Maintenance >OAM >Peer Information page is used to display information about attached OAM-enabled devices.

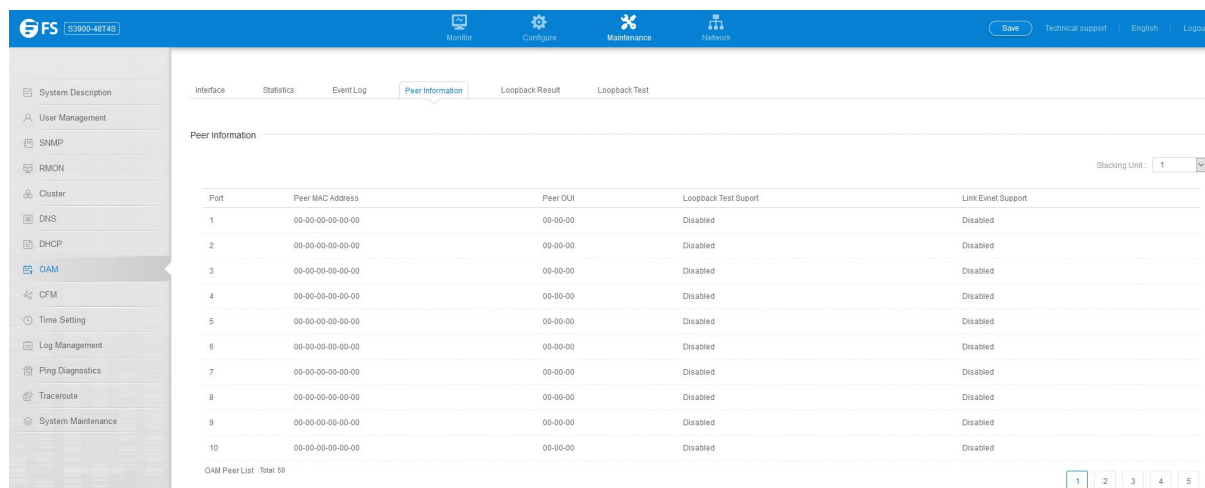
- **Port** – Port identifier. (Range: 1-28)
- **MAC Address** – MAC address of the OAM peer.
- **OUI** – Organizational Unit Identifier of the OAM peer.
- **Remote Loopback** – Shows if remote loopback is supported by the OAM peer.
- **Unidirectional Function** – Shows if this function is supported by the OAM peer.

If supported, this indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (where traffic flows in one direction only). Some newer physical layer devices support the optional ability to encode and transmit data

while one direction of the link is non-operational. This function allows OAM remote fault indication during fault conditions. This switch does not support the unidirectional function, but can parse error messages sent from a peer with unidirectional capability.

- **Link Monitor** – Shows if the OAM entity can send and receive Event Notification OAMPDUs.

- **MIB Variable Retrieval** – Shows if the OAM entity can send and receive Variable Request and Response OAMPDUs.



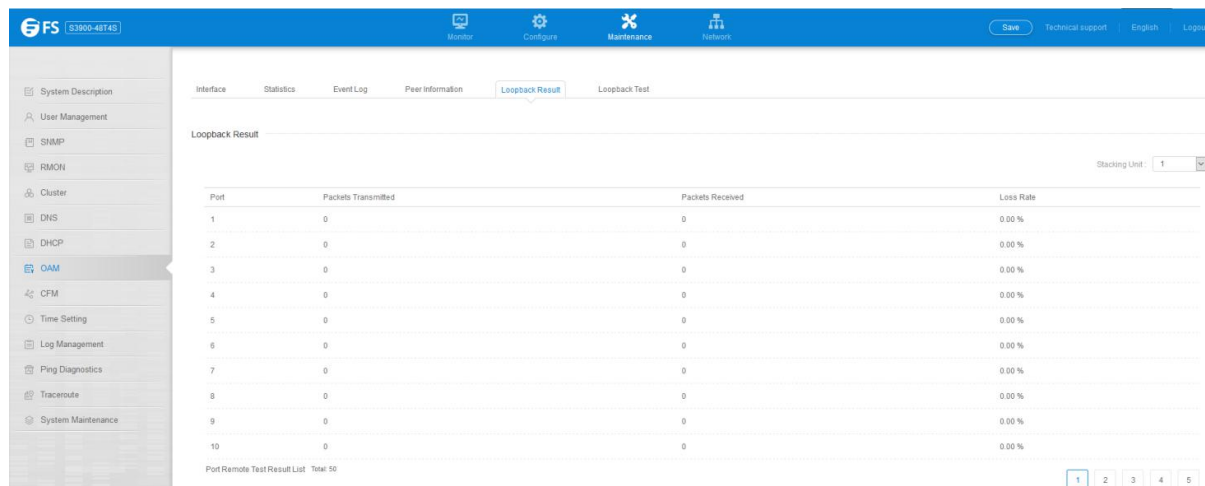
The screenshot shows the 'Peer Information' page in the FS S3900-48T4S web management interface. The left sidebar contains a navigation menu with options like System Description, User Management, SNMP, RMON, Cluster, DNS, DHCP, OAM (selected), CFM, Time Setting, Log Management, Ping Diagnostics, Traceroute, and System Maintenance. The main content area has tabs for Interface, Statistics, Event Log, Peer Information (selected), Loopback Result, and Loopback Test. Below the tabs, there is a 'Peer Information' section with a 'Stacking Unit' dropdown set to 1. A table displays peer information for 10 ports, with columns for Port, Peer MAC Address, Peer OUI, Loopback Test Support, and Link Evmt Support. All 'Loopback Test Support' values are 'Disabled'. At the bottom, it says 'OAM Peer List Total: 50' and there are pagination buttons 1 through 5.

Port	Peer MAC Address	Peer OUI	Loopback Test Support	Link Evmt Support
1	00-00-00-00-00-00	00-00-00	Disabled	Disabled
2	00-00-00-00-00-00	00-00-00	Disabled	Disabled
3	00-00-00-00-00-00	00-00-00	Disabled	Disabled
4	00-00-00-00-00-00	00-00-00	Disabled	Disabled
5	00-00-00-00-00-00	00-00-00	Disabled	Disabled
6	00-00-00-00-00-00	00-00-00	Disabled	Disabled
7	00-00-00-00-00-00	00-00-00	Disabled	Disabled
8	00-00-00-00-00-00	00-00-00	Disabled	Disabled
9	00-00-00-00-00-00	00-00-00	Disabled	Disabled
10	00-00-00-00-00-00	00-00-00	Disabled	Disabled

6.8.5 Loopback Result

Use the Maintenance > OAM > Loopback Result page is used to display the results of remote loop back testing for each port for which this information is available.

- **Port** – Port identifier. (Range: 1-12/26)
- **Packets Transmitted** – The number of loop back frames transmitted during the last loop back test on this interface.
- **Packets Received** – The number of loop back frames received during the last loop back test on this interface.
- **Loss Rate** – The percentage of packets transmitted for which there was no response.



The screenshot shows the 'Loopback Result' page in the FS S3900-48T4S web management interface. The left sidebar is the same as the previous screenshot. The main content area has tabs for Interface, Statistics, Event Log, Peer Information, Loopback Result (selected), and Loopback Test. Below the tabs, there is a 'Loopback Result' section with a 'Stacking Unit' dropdown set to 1. A table displays loopback test results for 10 ports, with columns for Port, Packets Transmitted, Packets Received, and Loss Rate. All 'Packets Transmitted' and 'Packets Received' values are 0, and all 'Loss Rate' values are 0.00 %. At the bottom, it says 'Port Remote Test Result List Total: 50' and there are pagination buttons 1 through 5.

Port	Packets Transmitted	Packets Received	Loss Rate
1	0	0	0.00 %
2	0	0	0.00 %
3	0	0	0.00 %
4	0	0	0.00 %
5	0	0	0.00 %
6	0	0	0.00 %
7	0	0	0.00 %
8	0	0	0.00 %
9	0	0	0.00 %
10	0	0	0.00 %

6.8.6 Loopback Test

The Maintenance > OAM > Loopback Test page is used to initiate a loop back test to the peer device attached to the selected port.

Loopback Mode of Remote Device

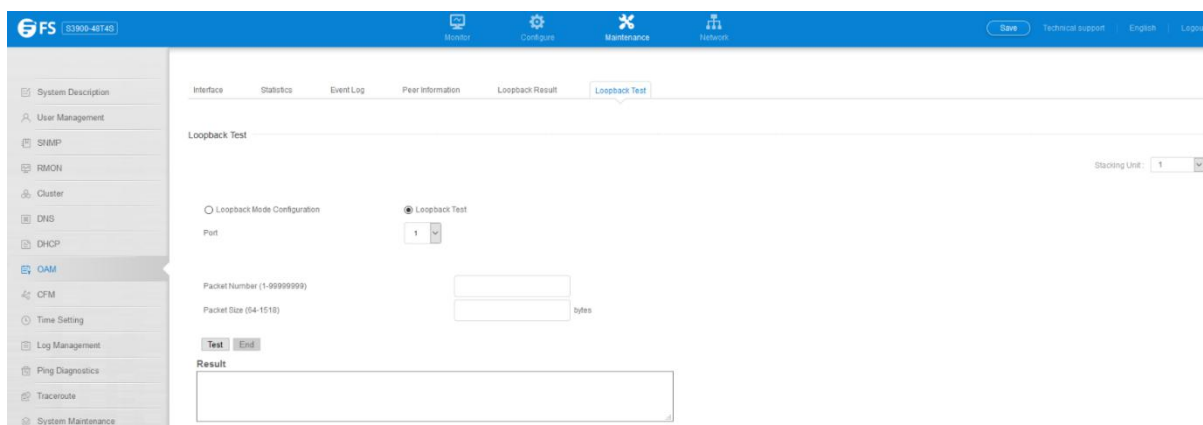
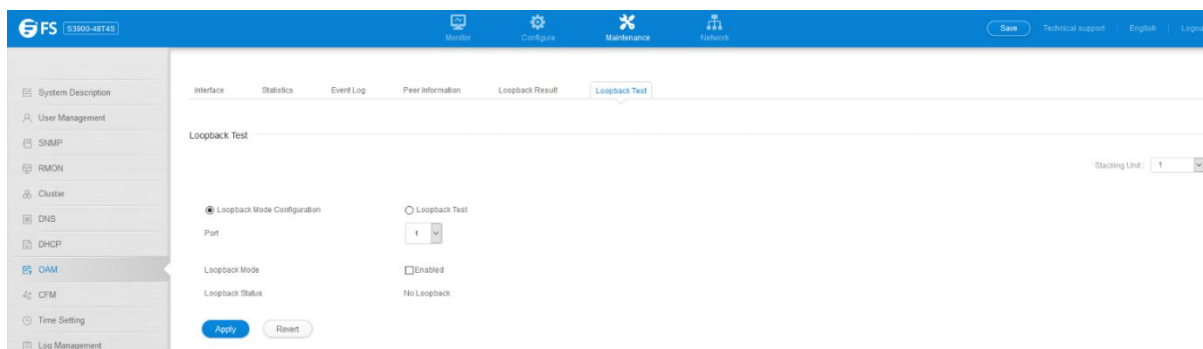
- **Port** – Port identifier. (Range: 1-28)
- **Loopback Mode** – Shows if loop back mode is enabled on the peer. This attribute must be enabled before starting the loopback test.
- **Loopback Status** – Shows if loopback testing is currently running. Loopback Test parameters
- **Packets Number** – Number of packets to send. (Range: 1-99999999; Default: 10000)
- **Packet Size** – Size of packets to send. (Range: 64-1518 bytes; Default: 64 bytes)
- **Test** – Starts the loop back test.
- **End** – Stops the loop back test.

Loop Back Status of Remote Device

- **Result** – Shows the loop back status on the peer. The loop back states shown in this field are described below.

OAM Operation State

- **Packets Transmitted** – The number of loop back frames transmitted during the last loopback test on this interface.
- **Packets Received** – The number of loop back frames received during the last loopback test on this interface.
- **Loss Rate** – The percentage of packets for which there was no response.



6.9 CFM

6.9.1 Global Configuration

The Maintenance >CFM >Global Configuration page is used to configure global settings for CFM, such as enabling the CFM process on the switch, setting the start-up delay for cross-check operations, configuring parameters for the link trace cache, and enabling traps for events discovered by continuity check messages or cross-check messages.

Global Configuration

- **CFM Status** – Enables CFM processing globally on the switch.(Default: Enabled)

To avoid generating an excessive number of traps, the complete CFM maintenance structure and process parameters should be configured prior to enabling CFM processing globally on the switch. Specifically, the maintenance domains, maintenance associations, and maintenance end-points (MEPs) should be configured on each participating bridge using the Configure MD page, Configure MA page, and the Configure MEP page. When CFM is enabled, hardware resources are allocated for CFM processing.

- **MEP Cross Check Start Delay** – Sets the maximum delay that a device waits for remote MEPs to come up before starting the crosscheck operation. (Range: 1-65535 seconds; Default: 10 seconds)

This parameter sets the time to wait for a remote MEP to come up, and the switch starts cross-checking the list of statically configured remote MEPs in the local maintenance domain against the MEPs learned through continuity check messages (CCMs). The cross-check start delay should be configured to a value greater than or equal to the continuity check message interval to avoid generating

unnecessary traps.

Link Trace Cache Settings

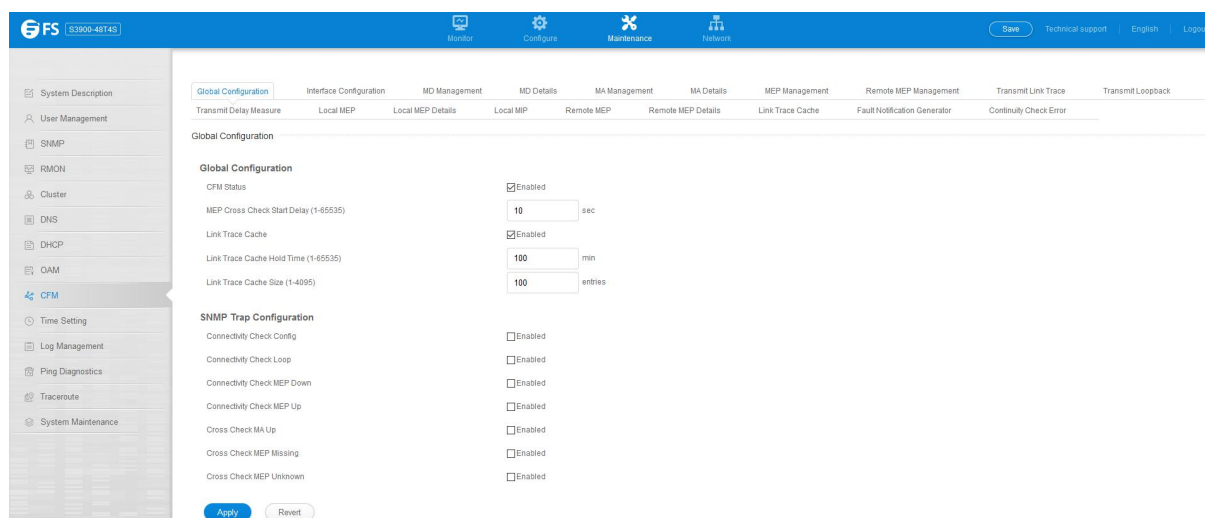
- **Link Trace Cache** – Enables caching of CFM data learned through link trace messages. (Default: Enabled) A linktrace message is a multicast CFM frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a linktrace reply, up to the point at which the linktrace message reaches its destination or can no longer be forwarded. Use this command attribute to enable the link trace cache to store the results of link trace operations initiated on this device. Use the CFM Transmit Link Trace page to transmit a linktrace message. Linktrace responses are returned from each MIP along the path and from the target MEP. Information stored in the cache includes the maintenance domain name, MA name, MEPID, sequence number, and TTL value.
- **Link Trace Cache Hold Time** – The hold time for CFM link trace cache entries. (Range: 1-65535 minutes; Default: 100 minutes) Before setting the aging time for cache entries, the cache must first be enabled in the Linktrace Cache attribute.
- **Link Trace Cache Size** – The maximum size for the link trace cache. (Range: 1-4095 entries; Default: 100 entries) If the cache reaches the maximum number of specified entries, or the size is set to a value less than the current number of stored entries, no new entries are added. To add additional entries, the cache size must first be increased, or purged.

Continuity Check Errors

- **Connectivity Check Config** – Sends a trap if this device receives a continuity check message (CCM) with the same maintenance end point identifier (MPID) as its own but with a different source MAC address, indicating that a CFM configuration error exists.
- **Connectivity Check Loop** – Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.
- **Connectivity Check MEP Down** – Sends a trap if this device loses connectivity with a remote maintenance end point (MEP), or connectivity has been restored to a remote MEP which has recovered from an error condition.
- **Connectivity Check MEP Up** – Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which as an expired entry in the archived database. MEP Up traps are suppressed when cross-checking of MEPs is enabled¹¹ because cross-check traps include more detailed status information.

Cross-check Errors

- **Cross Check MA Up** – Sends a trap when all remote MEPs in an MA come up. An MA Up trap is sent if cross-checking is enabled, and a CCM is received from all remote MEPs configured in the static list for this maintenance association.
- **Cross Check MEP Missing** – Sends a trap if the cross-check timer expires and no CCMs have been received from a remote MEP configured in the static list. A MEP Missing trap is sent if cross-checking is enabled¹¹, and no CCM is received for a remote MEP configured in the static list¹².
- **Cross Check MEP Unknown** – Sends a trap if an unconfigured MEP comes up. A MEP Unknown trap is sent if cross-checking is enabled¹¹, and a CCM is received from a remote MEP that is not configured in the static list¹².



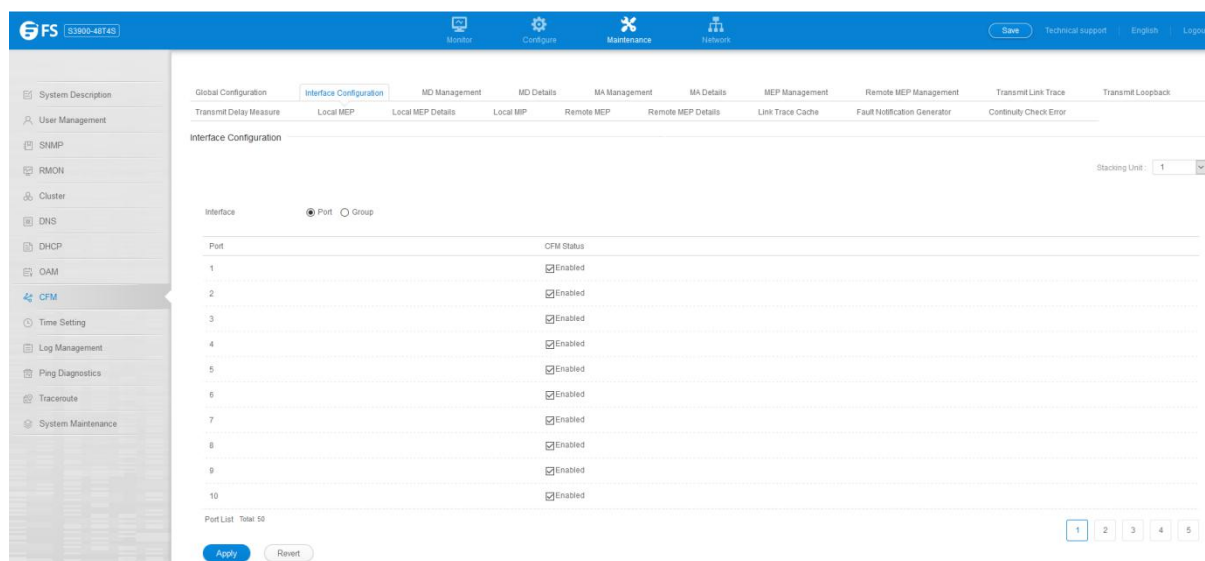
The screenshot shows the web management interface for an FS S3900-48T4S switch. The top navigation bar includes tabs for Monitor, Configure, Maintenance, and Network. The left sidebar lists various system settings, with CFM (Control Plane Forwarding) selected. The main content area is titled 'Global Configuration' and contains two sections:

- Global Configuration:**
 - CFM Status: ☒ Enabled
 - MEP Cross Check Start Delay (1-65535): 10 sec
 - Link Trace Cache: ☒ Enabled
 - Link Trace Cache Hold Time (1-65535): 100 min
 - Link Trace Cache Size (1-4095): 100 entries
- SNMP Trap Configuration:**
 - Connectivity Check Config: ☐ Enabled
 - Connectivity Check Loop: ☐ Enabled
 - Connectivity Check MEP Down: ☐ Enabled
 - Connectivity Check MEP Up: ☐ Enabled
 - Cross Check MA Up: ☐ Enabled
 - Cross Check MEP Missing: ☐ Enabled
 - Cross Check MEP Unknown: ☐ Enabled

At the bottom of the configuration area, there are 'Apply' and 'Revert' buttons.

6.9.2 Interface Configuration

CFM processes are enabled by default for all physical interfaces, both ports and trunks. You can use the Maintenance >CFM >Interface Configuration page to change these settings.

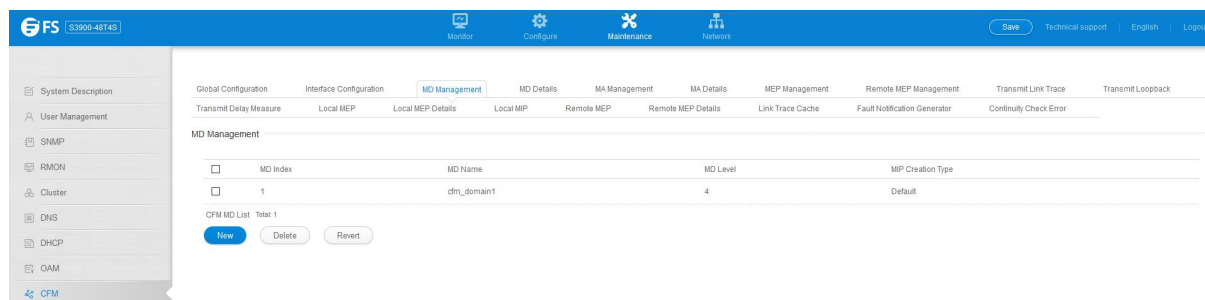


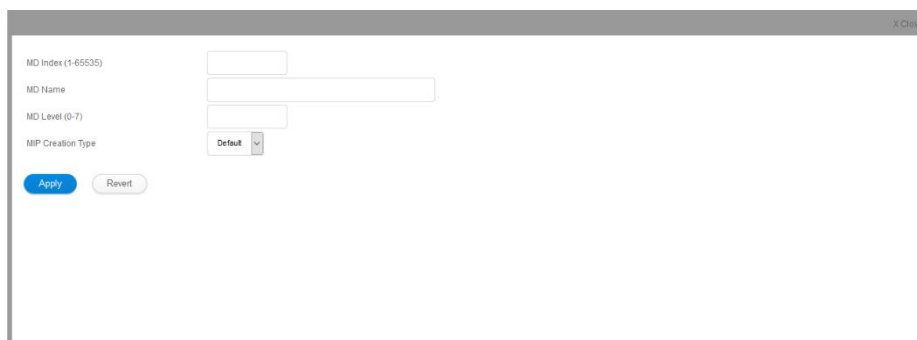
6.9.3 MD Management

Maintenance >CFM >MD Management pages is used to create and configure a Maintenance Domain (MD) which defines a portion of the network for which connectivity faults can be managed. Domain access points are set up on the boundary of a domain to provide end-to-end connectivity fault detection, analysis, and recovery. Domains can be configured in a hierarchy to provide management access to the same basic network resources for different user levels.

Creating a Maintenance Domain

- **MD Index** – Domain index. (Range: 1-65535)
- **MD Name** – Maintenance domain name. (Range: 1-43 alphanumeric characters)
- **MD Level** – Authorized maintenance level for this domain.(Range: 0-7)
- **MIP Creation Type** – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this domain:
 - Default – MIPs can be created for any maintenance association (MA) configured in this domain on any bridge port through which the MA's VID can pass.
 - Explicit – MIPs can be created for any MA configured in this domain only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.
 - None – No MIP can be created for any MA configured in this domain.





MD Index (1-65535):

MD Name:

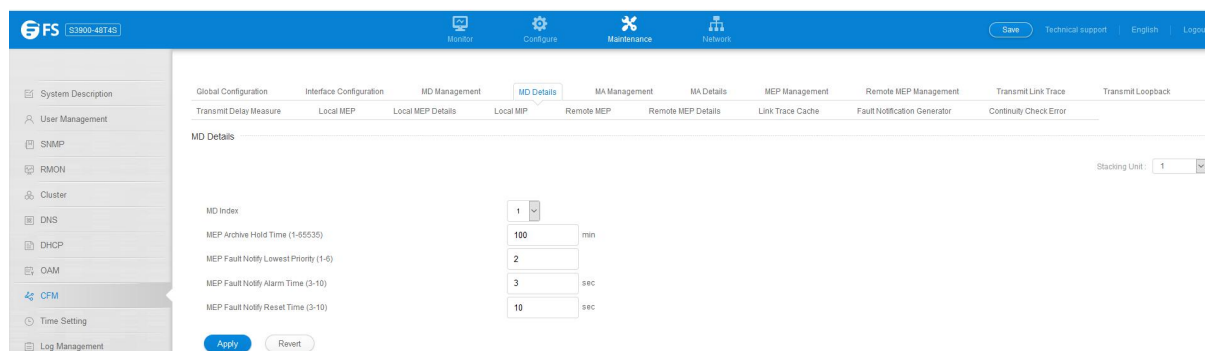
MD Level (0-7):

MIP Creation Type:

6.9.4 MD Details

Maintenance >CFM >MD Details page is used to configure details of specify MD.

- **MD Index** – Domain index. (Range: 1-65535)
- **MEP Archive Hold Time** – The time that data from a missing MEP is retained in the continuity check message (CCM) database before being purged. (Range: 1-65535 minutes; Default: 100 minutes)A change to the hold time only applies to entries stored in the database after this attribute is changed.
- **MEP Fault Notify Lowest Priority** – The lowest priority defect that is allowed to generate a fault alarm. (Range: 1-6, Default: 2)
- **MEP Fault Notify Alarm Time** – The time that one or more defects must be present before a fault alarm is issued. (Range: 3-10 seconds;Default: 3 seconds)
- **MEP Fault Notify Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued.(Range: 3-10 seconds; Default: 10 seconds)



Global Configuration | Interface Configuration | MD Management | **MD Details** | MA Management | MA Details | MEP Management | Remote MEP Management | Transmit Link Trace | Transmit Loopback

Transmit Delay Measure | Local MEP | Local MEP Details | Local MIP | Remote MEP | Remote MEP Details | Link Trace Cache | Fault Notification Generator | Continuity Check Error

MD Details

MD Index:

MEP Archive Hold Time (1-65535): min

MEP Fault Notify Lowest Priority (1-6):

MEP Fault Notify Alarm Time (3-10): sec

MEP Fault Notify Reset Time (3-10): sec

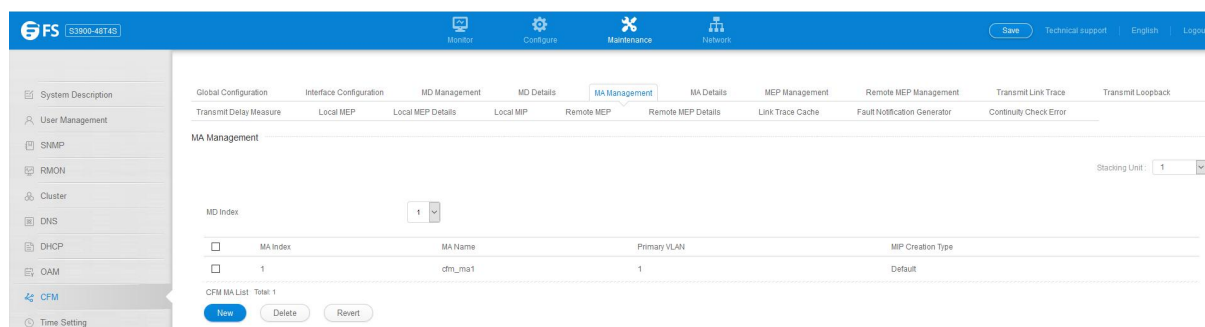
Stacking Unit:

6.9.5 MA Management

Maintenance >CFM >MA Management pages is used to create and configure the Maintenance Associations (MA) which define a unique CFM service instance. Each MA can be identified by its parent MD, the MD's maintenance level, the VLAN assigned to the MA, and the set of maintenance end points (MEPs) assigned to it.

Creating a Maintenance Association

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MA Name** – MA name. (Range: 1-43 alphanumeric characters)Each MA name must be unique within the CFM domain.
- **Primary VLAN** – Service VLAN ID. (Range: 1-4093)This is the VLAN through which all CFM functions are executed for this MA.
- **MIP Creation Type** – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this MA:
 - **Default** – MIPs can be created for this MA on any bridge port through which the MA's VID can pass.
 - **Explicit** – MIPs can be created for this MA only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.
 - **None** – No MIP can be created for this MA.




6.9.6 MA Details

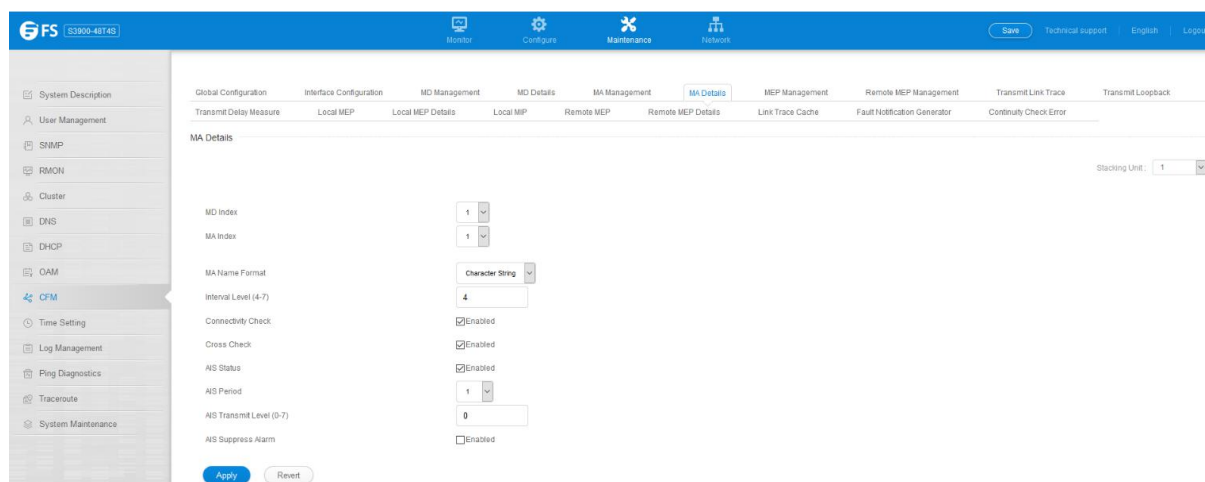
Maintenance > CFM > MA Details page is used to configure details of specify MA.

Configuring Detailed Settings for a Maintenance Association

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MA Name Format** – Specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format.
 - **Character String** – IEEE 802.1ag defined character string format. This is an IETF RFC 2579 DisplayString.
 - **ICC Based** – ITU-T SG13/SG15 Y.1731 defined ICC based format.
- **Interval Level** – The delay between sending CCMs. The setting for this parameter is expressed as levels 4 through 7, which in turn map to specific intervals of time. (Options: 4 - 100 ms, 5 - 1 sec, 6 - 10 sec, 7 - 60 sec)
- **Connectivity Check** – Enables transmission of CCMs. (Default: Disabled)
- **Cross Check** – Enables cross-checking between a static list of MEPs assigned to other devices within the same maintenance association and the MEPs learned through CCMs.

Before starting the cross-check process, first configure the remote MEPs that exist on other devices inside the maintenance association using the Remote MEP List. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational. The cross-check start delay, which sets the maximum delay this device waits for a remote MEP to come up before starting the cross-check operation, is a domain-level parameter. To set this parameter, use the CFM MD Configuration screen.

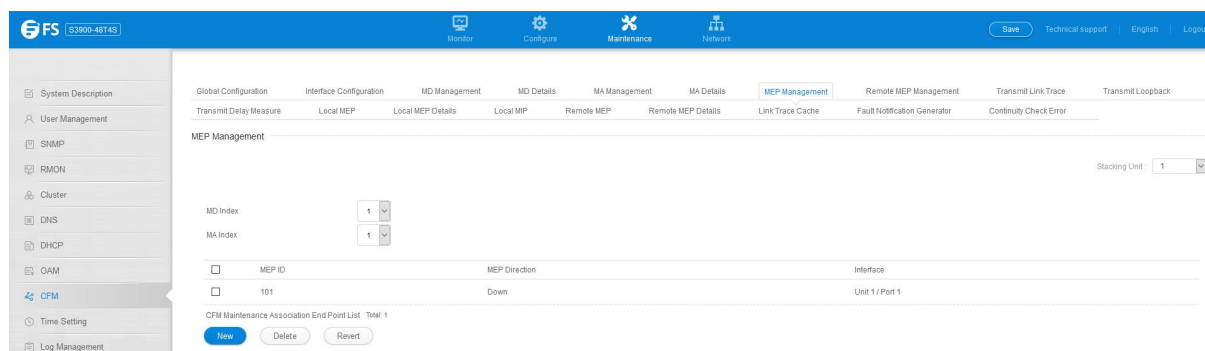
- **AIS Status** – Enables/disables suppression of the Alarm Indication Signal (AIS). (Default: Disabled)
- **AIS Period** – Configures the period at which AIS is sent in an MA. (Range: 1 or 60 seconds; Default: 1 second)
- **AIS Transmit Level** – Configure the AIS maintenance level in an MA. (Range: 0-7; Default is 0) AIS Level must follow this rule: AIS Level >= Domain Level
- **AIS Suppress Alarm** – Enables/disables suppression of the AIS. (Default: Disabled)



6.9.7 MEP Management

Maintenance >CFM >MEP Management page is used to configure Maintenance End Points (MEPs). MEPs, also called Domain Service Access Points (DSAPs), must be configured at the domain boundary to provide management access for each maintenance association.

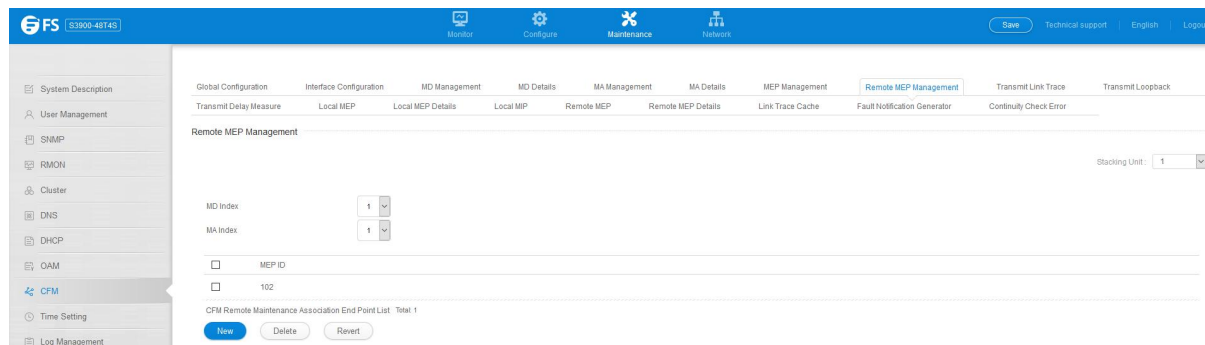
- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- **MEP Direction** – Up indicates that the MEP faces inward toward the switch cross-connect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism. If the **Up** option is not selected, then the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.
- **Interface** – Indicates a port or trunk.




6.9.8 Remote MEP Management

Maintenance >CFM >Remote MEP Management page is used to specify remote maintenance end points (MEPs) set on other CFM-enabled devices within a common MA.

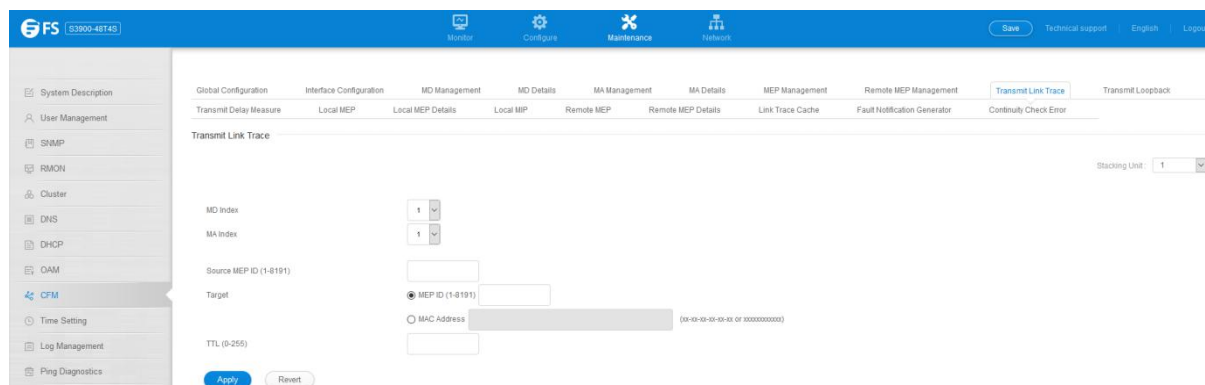
- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MEP ID** – Identifier for a maintenance end point which exists on another CFM-enabled device within the same MA. (Range: 1-8191)




6.9.9 Transmit Link Trace

Maintenance >CFM >Transmit Link Trace page is used to transmit link trace messages (LTMs). These messages can isolate connectivity faults by tracing the path through a network to the designated target node (i.e., a remote maintenance end point).

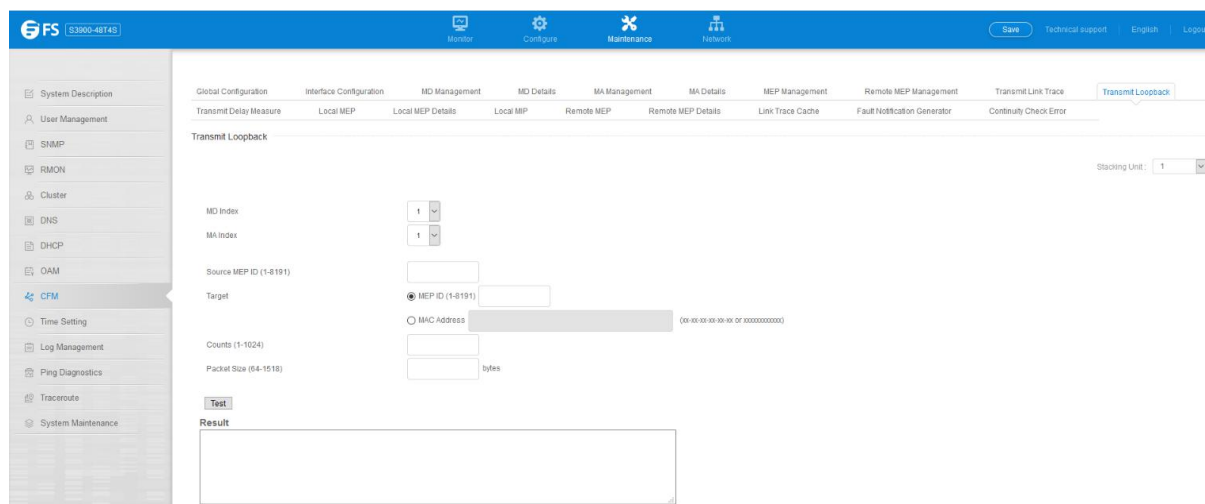
- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **Source MEP ID** – The identifier of a source MEP that will send the link trace message. (Range: 1-8191)
- **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a link trace message. (Range: 1-8191)
 - **MAC Address** – MAC address of a remote MEP that is the target of a link trace message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- **TTL** – The time to live of the link trace message. (Range: 0-255 hops)



6.9.10 Transmit Loopback

Maintenance >CFM >Transmit Loopback page is used to transmit Loopback Messages (LBMs). These messages can be used to isolate or verify connectivity faults by submitting a request to a target node (i.e., a remote MEP or MIP) to echo the message back to the source.

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **Source MEP ID** – The identifier of a source MEP that will send the loopback message. (Range: 1-8191)
- **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a loopback message. (Range: 1-8191)
 - **MAC Address** – MAC address of a remote MEP that is the target of a loopback message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- **Count** – The number of times the loopback message is sent. (Range: 1-1024)
- **Packet Size** – The size of the loopback message. (Range: 64-1518 bytes; Default: 64 bytes)

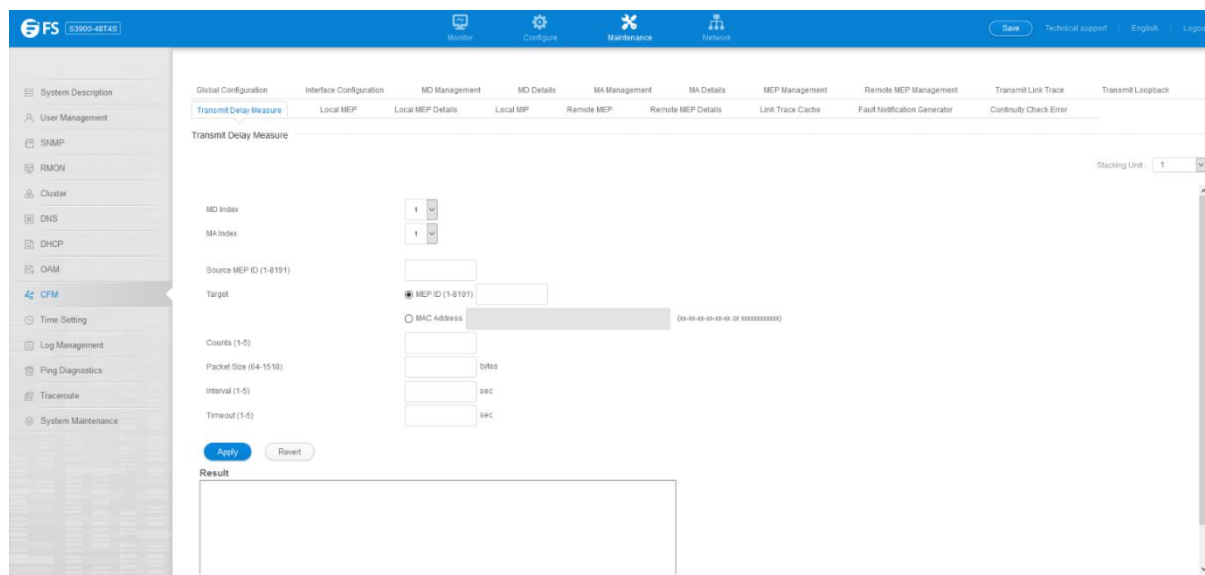


6.9.11 Transmit Delay Measure

Maintenance >CFM >Transmit Delay Measure page is used to send periodic delay-measure requests to a specified MEP within a maintenance association.

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **Source MEP ID** – The identifier of a source MEP that will send the delay-measure message. (Range: 1-8191)
- **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a delay-measure message. (Range: 1-8191)

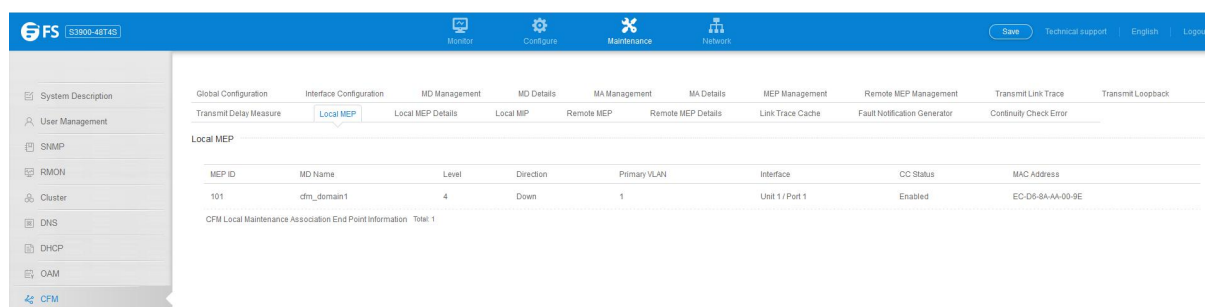
- **MAC Address** – MAC address of a remote MEP that is the target of a delay-measure message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxxxx
- **Count** – The number of times to retry sending the message if no response is received before the specified timeout. (Range: 1-5; Default: 5)
- **Packet Size** – The size of the delay-measure message. (Range: 64-1518 bytes; Default: 64 bytes)
- **Interval** – The transmission delay between delay-measure messages. (Range: 1-5 seconds; Default: 1 second)
- **Timeout** – The timeout to wait for a response. (Range: 1-5 seconds; Default: 5 seconds)



6.9.12 Local MEP

Maintenance > CFM > Local MEP page is used to show information for the MEPs configured on this device.

- **MEP ID** – Maintenance end point identifier.
- **MD Name** – Maintenance domain name.
- **Level** – Authorized maintenance level for this domain.
- **Direction** – Direction in which the MEP communicates CFM messages:
 - Down indicates that the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.
 - Up indicates that the MEP faces inward toward the switch crossconnect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism.
- **Primary VLAN** – Service VLAN ID.
- **Interface** – Physical interface of this entry (either a port or trunk).
- **CC Status** – Shows administrative status of CCMs.
- **MAC Address** – MAC address of this MEP entry.



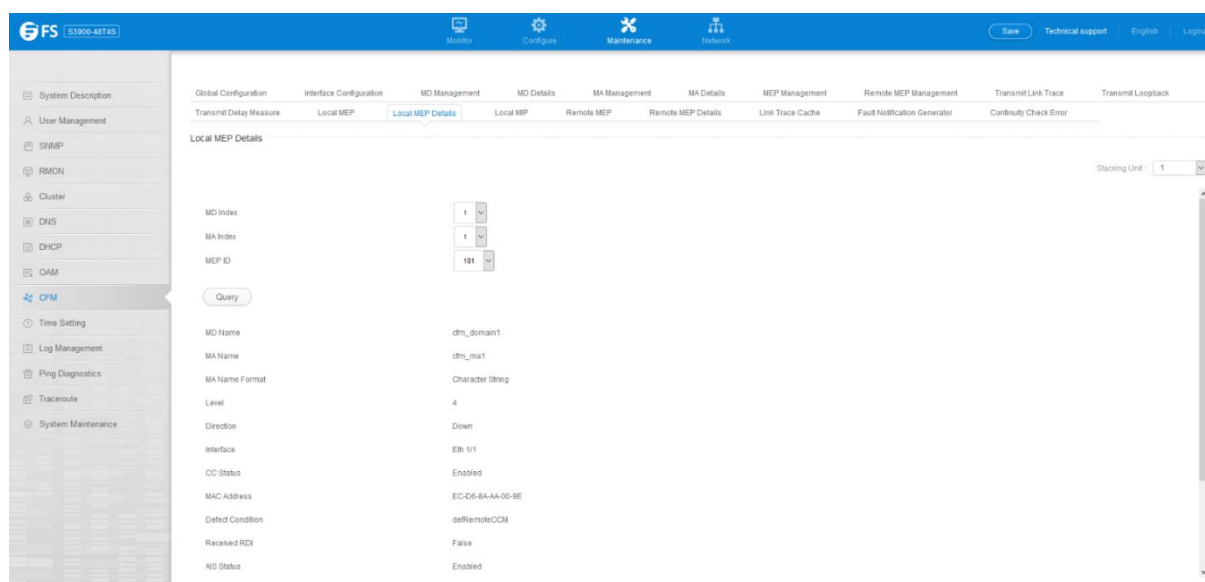
MEP ID	MD Name	Level	Direction	Primary VLAN	Interface	CC Status	MAC Address
101	dm_domain1	4	Down	1	Unit 1/Port 1	Enabled	EC-D8-8A-AA-00-9E

CFM Local Maintenance Association End Point Information Total: 1

6.9.13 Local MEP Details

Maintenance >CFM >Local MEP Details page is used to show detailed CFM information about a local MEP in the continuity check database.

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- **MD Name** – The maintenance domain for this entry.
- **MA Name** – Maintenance association to which this remote MEP belongs.
- **MA Name Format** – The format of the Maintenance Association name, including primary VID, character string, unsigned Integer 16, or RFC 2865 VPN ID.
- **Level** – Maintenance level of the local maintenance point.
- **Direction** – The direction in which the MEP faces on the Bridge port (up or down).
- **Interface** – The port to which this MEP is attached.
- **CC Status** – Shows if the MEP will generate CCM messages.
- **MAC Address** – MAC address of the local maintenance point. (If a CCM for the specified remote MEP has never been received or the local MEP record times out, the address will be set to the initial value of all FS.)
- **Defect Condition** – Shows the defect detected on the MEP.
- **Received RDI** – Receive status of remote defect indication (RDI) messages on the MEP.
- **AIS Status** – Shows if MEPs within the specified MA are enabled to send frames with AIS information following detection of defect conditions.
- **AIS Period** – The interval at which AIS information is sent.
- **AIS Transmit Level** – The maintenance level at which AIS information will be sent for the specified MEP.
- **Suppress Alarm** – Shows if the specified MEP is configured to suppress sending frames containing AIS information following the detection of defect conditions.
- **Suppressing Alarms** – Shows if the specified MEP is currently suppressing sending frames containing AIS information following the detection of defect conditions.



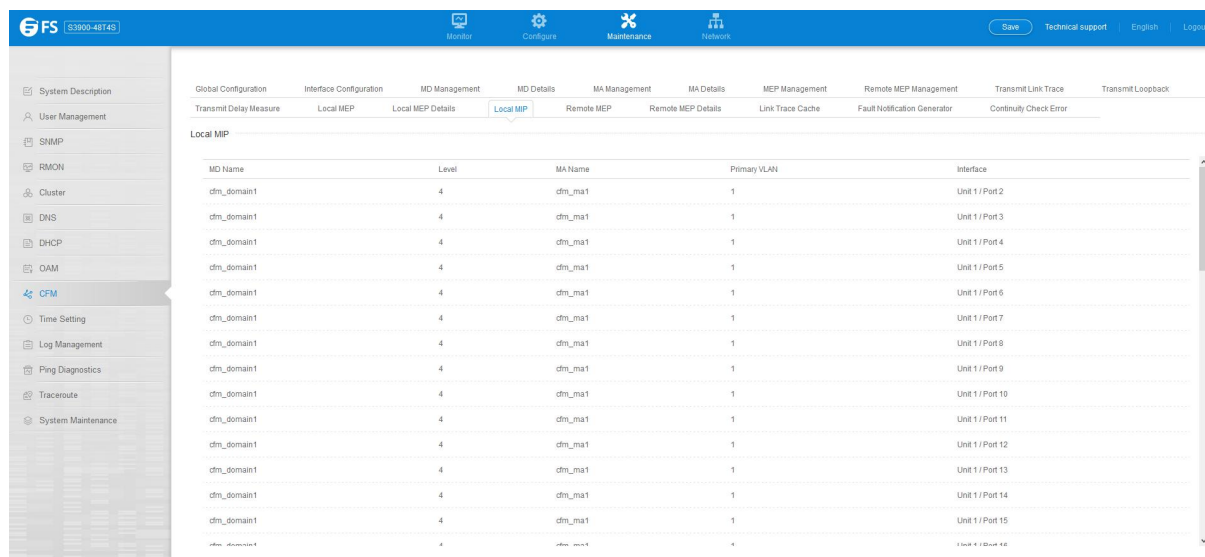
The screenshot shows the 'Local MEP Details' page in the FS web management interface. The page has a blue header with the FS logo and navigation tabs: Monitor, Configure, Maintenance, and Network. The 'Maintenance' tab is active. On the left, there is a sidebar menu with categories like System Description, User Management, SHMP, RMON, Cluster, DNS, DHCP, QAM, CFM, Time Setting, Log Management, Ping Diagnostics, Traceroute, and System Maintenance. The 'CFM' category is expanded, showing 'Local MEP Details' as the selected option. The main content area displays the configuration for a specific Local MEP. It includes input fields for MD Index (1), MA Index (1), and MEP ID (101). Below these are fields for MD Name (dm_domain1), MA Name (dm_ma1), MA Name Format (Character String), Level (4), Direction (Down), Interface (E8/1/1), CC Status (Enabled), MAC Address (EC-D6-8A-AA-00-8E), Defect Condition (defRemoteCCM), Received RDI (False), and AIS Status (Enabled). A 'Query' button is located below the input fields. On the right side of the page, there is a 'Stacking Unit' dropdown menu set to '1'.

6.9.14 Local MIP

Maintenance >CFM >Local MIP page is used to show the MIPs on this device discovered by the CFM protocol.

- **MD Name** – Maintenance domain name.

- **Level** – Authorized maintenance level for this domain.
- **MA Name** – Maintenance association name.
- **Primary VLAN** – Service VLAN ID.
- **Interface** – Physical interface of this entry (either a port or trunk).

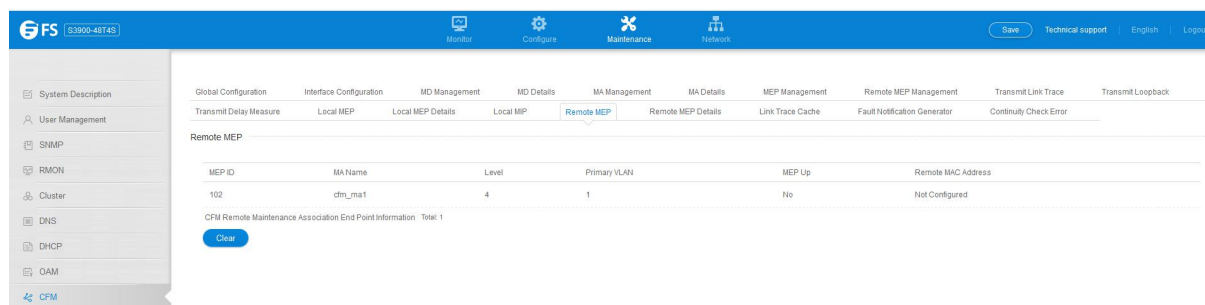


MD Name	Level	MA Name	Primary VLAN	Interface
dm_domain1	4	dm_ma1	1	Unit 1 / Port 2
dm_domain1	4	dm_ma1	1	Unit 1 / Port 3
dm_domain1	4	dm_ma1	1	Unit 1 / Port 4
dm_domain1	4	dm_ma1	1	Unit 1 / Port 5
dm_domain1	4	dm_ma1	1	Unit 1 / Port 6
dm_domain1	4	dm_ma1	1	Unit 1 / Port 7
dm_domain1	4	dm_ma1	1	Unit 1 / Port 8
dm_domain1	4	dm_ma1	1	Unit 1 / Port 9
dm_domain1	4	dm_ma1	1	Unit 1 / Port 10
dm_domain1	4	dm_ma1	1	Unit 1 / Port 11
dm_domain1	4	dm_ma1	1	Unit 1 / Port 12
dm_domain1	4	dm_ma1	1	Unit 1 / Port 13
dm_domain1	4	dm_ma1	1	Unit 1 / Port 14
dm_domain1	4	dm_ma1	1	Unit 1 / Port 15

6.9.15 Remote MEP

Maintenance >CFM >Remote MEP page is used to show MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.

- **MEP ID** – Maintenance end point identifier.
- **MA Name** – Maintenance association name.
- **Level** – Authorized maintenance level for this domain.
- **Primary VLAN** – Service VLAN ID.
- **MEP Up** – Indicates whether or not this MEP is functioning normally.
- **Remote MAC Address** – MAC address of the remote maintenance point. (If a CCM for the specified remote MEP has never been received or the remote MEP record times out, the address will be set to the initial value of all FS.)



MEP ID	MA Name	Level	Primary VLAN	MEP Up	Remote MAC Address
102	dm_ma1	4	1	No	Not Configured

CFM Remote Maintenance Association End Point Information Total: 1

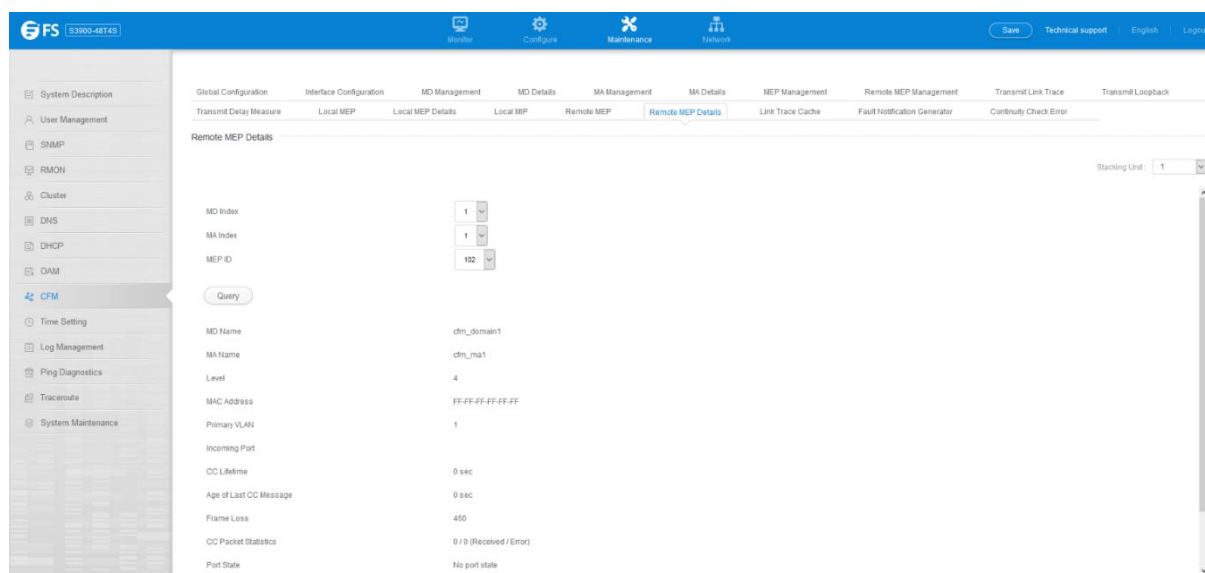
[Clear](#)

6.9.16 Remote MEP Details

Maintenance >CFM >Remote MEP Details is used page to show detailed information for MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MEP ID** – Maintenance end point identifier. (Range: 1-8191)

- **MD Name** – Maintenance domain name.
- **MA Name** – Maintenance association name.
- **Level** – Authorized maintenance level for this domain.
- **MAC Address** – MAC address of this MEP entry.
- **Primary VLAN** – Service VLAN ID.
- **Incoming Port** – Port to which this remote MEP is attached.
- **CC Lifetime** – Length of time to hold messages about this MEP in the CCM database.
- **Age of Last CC Message** – Length of time the last CCM message about this MEP has been in the CCM database.
- **Frame Loss** – Percentage of transmitted frames lost.
- **CC Packet Statistics** – The number of CCM packets received successfully and those with errors.
- **Port State** – Port states include:
 - Up – The port is functioning normally.
 - Blocked – The port has been blocked by the Spanning Tree Protocol.
 - No port state – Either no CCM has been received, or no port status TLV was received in the last CCM.
- **Interface State** – Interface states include:
 - No Status – Either no CCM has been received, or no interface status TLV was received in the last CCM.
 - Up – The interface is ready to pass packets.
 - Down – The interface cannot pass packets.
 - Testing – The interface is in some test mode.
 - Unknown – The interface status cannot be determined for some reason.
 - Dormant – The interface is not in a state to pass packets but is in a pending state, waiting for some external event.
 - Not Present – Some component of the interface is missing.
 - isLowerLayerDown – The interface is down due to state of the lower layer interfaces.
- **Crosscheck Status** – Shows if crosscheck function has been enabled.

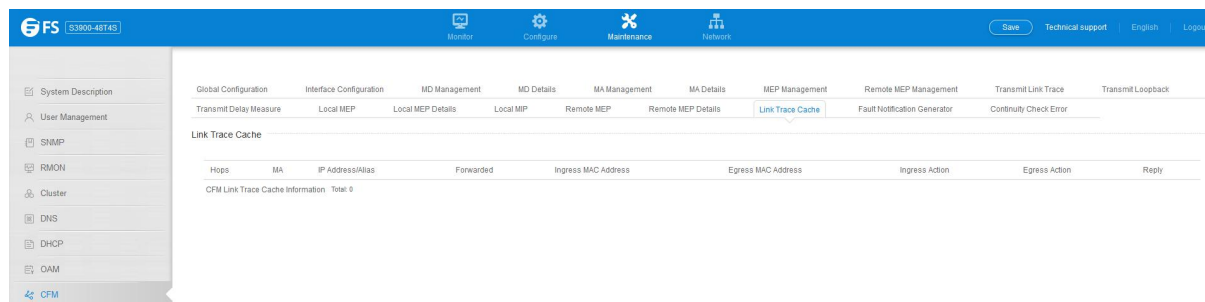


6.9.17 Link Trace Cache

Maintenance > CFM > Link Trace Cache page is used to show information about link trace operations launched from this device.

- **Hops** – The number hops taken to reach the target MEP.
- **MA** – Maintenance association name.
- **IP/Alias** – IP address or DNS alias of the target device's CPU.

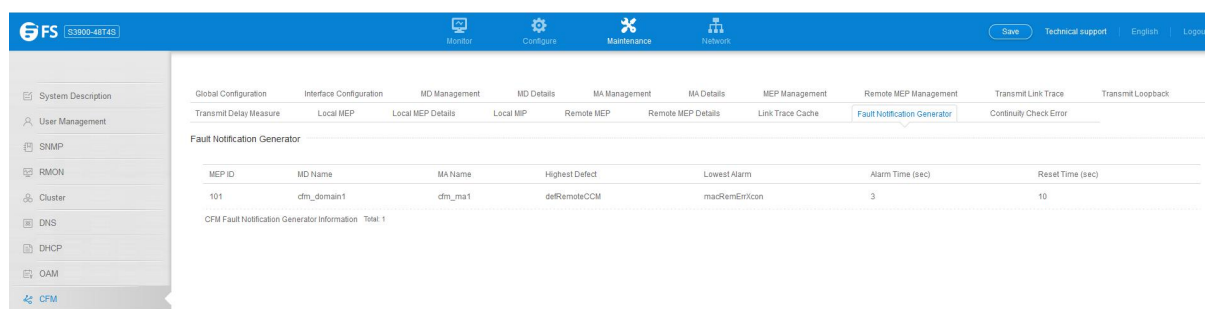
- **Forwarded** – Shows whether or not this link trace message was forwarded. A message is not forwarded if received by the target MEP.
- **Ingress MAC Address** – MAC address of the ingress port on the target device.
- **Egress MAC Address** – MAC address of the egress port on the target device.
- **Ingress Action** – Action taken on the ingress port:
 - IngOk – The target data frame passed through to the MAC Relay Entity.
 - IngDown – The bridge port's MAC_Operational parameter is false. This value could be returned, for example, by an operationally Down MEP that has another Down MEP at a higher MD level on the same bridge port that is causing the bridge port's MAC_Operational parameter to be false.
 - IngBlocked – The ingress port can be identified, but the target data frame was not forwarded when received on this port due to active topology management, i.e., the bridge port is not in the forwarding state.
 - IngVid – The ingress port is not in the member set of the LTM's VIDs, and ingress filtering is enabled, so the target data frame was filtered by ingress filtering.
- **Egress Action** – Action taken on the egress port:
 - EgrOk – The targeted data frame was forwarded.
 - EgrDown – The Egress Port can be identified, but that bridge port's MAC_Operational parameter is false.
 - EgrBlocked – The egress port can be identified, but the data frame was not passed through the egress port due to active topology management, i.e., the bridge port is not in the forwarding state.
 - EgrVid – The Egress Port can be identified, but the bridge port is not in the LTM's VID member set, and was therefore filtered by egress filtering.
- **Reply** – Reply action:
 - FDB – Target address found in forwarding database.
 - MPDB – Target address found in the maintenance point database.
 - HIT – Target located on this device.



6.9.18 Fault Notification Generator

Maintenance > CFM > Fault Notification Generator page is used to display configuration settings for the fault notification generator.

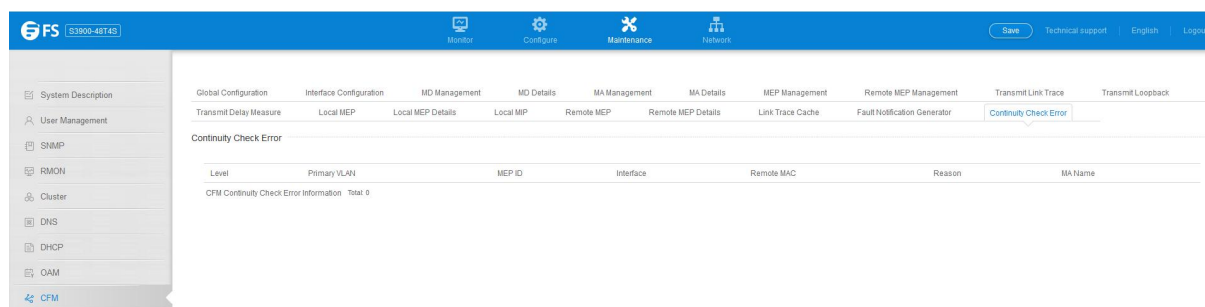
- **MEP ID** – Maintenance end point identifier.
- **MD Name** – Maintenance domain name.
- **MA Name** – Maintenance association name.
- **Highest Defect** – The highest defect that will generate a fault alarm. (This is disabled by default.)
- **Lowest Alarm** – The lowest defect that will generate a fault alarm.
- **Alarm Time** – The time a defect must exist before a fault alarm is issued.
- **Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued.



6.9.19 Continuity Check Error

Maintenance >CFM >Continuity Check Error page is used to display the CFM continuity check errors logged on this device.

- **Level** – Maintenance level associated with this entry.
- **Primary VLAN** – VLAN in which this error occurred.
- **MEP ID** – Identifier of remote MEP.
- **Interface** – Port at which the error was recorded.
- **Remote MAC** – MAC address of remote MEP.
- **Reason** – Error types include:
 - **LEAK** – MA x is associated with a specific VID list14, one or more of the VIDs in this MA can pass through the bridge port, no MEP is configured facing outward (down) on any bridge port for this MA, and some other MA y, at a higher maintenance level, and associated with at least one of the VID(s) also in MA x, does have a MEP configured on the bridge port.
 - **VIDS** – MA x is associated with a specific VID list14, an MEP is configured facing inward (up) on this MA on the bridge port, and some other MA y, associated with at least one of the VID(s) also in MA x, also has an Up MEP configured facing inward (up) on some bridge port.
 - **EXCESS_LEV** – The number of different MD levels at which MIPs are to be created on this port exceeds the bridge's capabilities.
 - **OVERLAP_LEV** – A MEP is created for one VID at one maintenance level, but a MEP is configured on another VID at an equivalent or higher level, exceeding the bridge's capabilities.
- **MA Name** – The maintenance association for this entry.



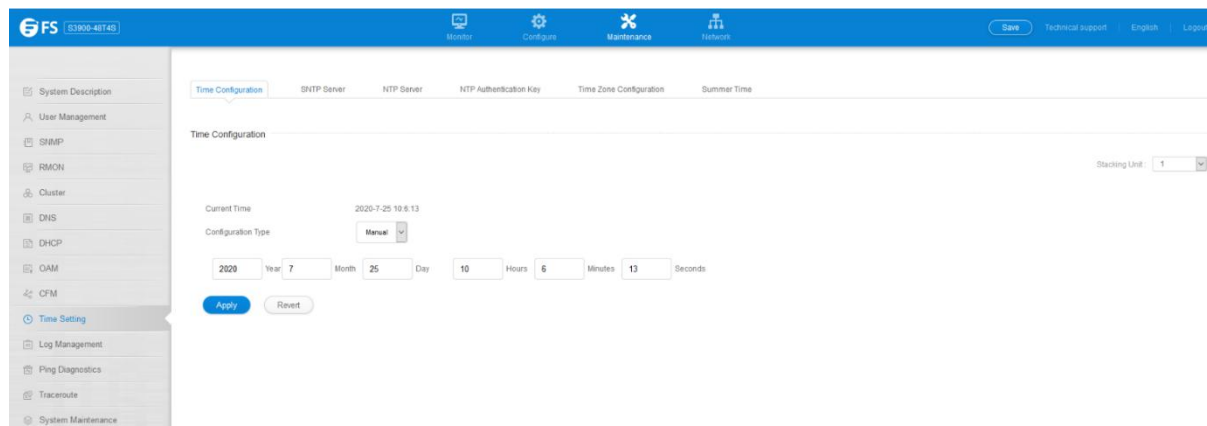
6.10 Time Setting

6.10.1 Time Configuration

The Maintenance >Time Setting >Time Configuration page is used to set the system time on the switch manually without using SNTP.

- **Current Time** – Shows the current time set on the switch.
- **Hours** – Sets the hour. (Range: 0-23)

- **Minutes** – Sets the minute value. (Range: 0-59)
- **Seconds** – Sets the second value. (Range: 0-59)
- **Month** – Sets the month. (Range: 1-12)
- **Day** – Sets the day of the month. (Range: 1-31)
- **Year** – Sets the year. (Range: 1970-2037)



6.10.2 SNTP Server

The Maintenance >Time Setting >SNTP Server page is used to specify the IP address for up to three SNTP time servers.

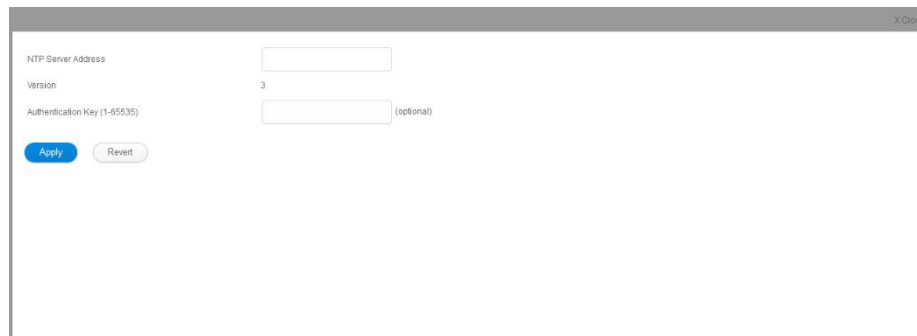
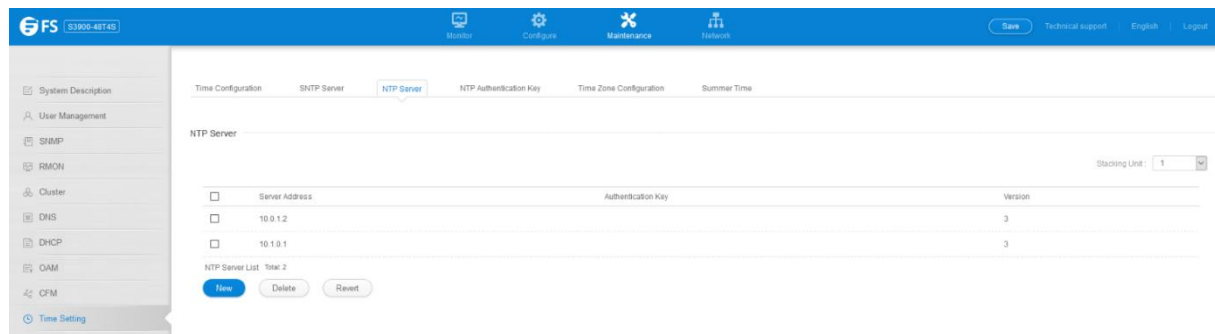
- **SNTP Server IP Address** – Sets the IPv4 or IPv6 address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.



6.10.3 NTP Server

The Maintenance >Time Setting >NTP Server page is used to add the IP address for up to 50 NTP time servers.

- **NTP Server IP Address** – Adds the IPv4 or IPv6 address for up to 50 time servers. The switch will poll the specified time servers for updates when the clock maintenance type is set to NTP on the System > Time (Configure General) page. It issues time synchronization requests at a fixed interval of 1024 seconds. The switch will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.
- **Version** – Specifies the NTP version supported by the server.(Fixed: Version 3)
- **Authentication Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with the configured server. NTP authentication is optional. If enabled on the System > Time (Configure General) page, you must also configure at least one key on the System > Time (Add NTP Authentication Key) page.(Range: 1-65535)



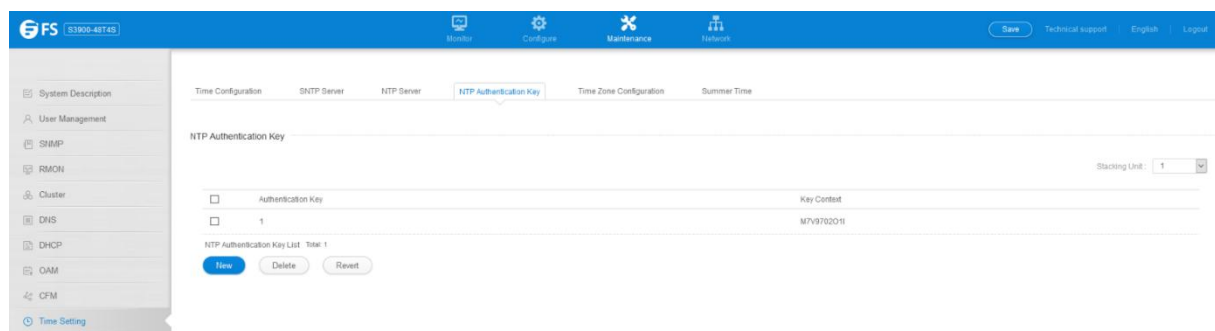
6.10.4 NTP Authentication Key

The Maintenance >Time Setting >NTP Authentication Key page is used to add an entry to the authentication key list.

- **Authentication Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with a configured server. NTP authentication is optional. When enabled on the System >Time (Configure General) page, you must also configure at least one

key on this page. Up to 255 keys can be configured on the switch.(Range: 1-65535)

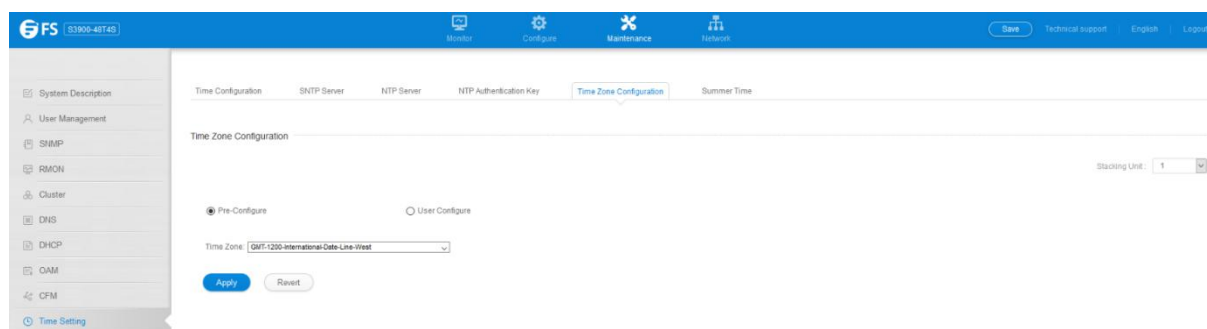
- **Key Context** – An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).NTP authentication key numbers and values must match on both the server and client.



6.10.5 Time Zone Configuration

The Maintenance >Time Setting >Time Zone Configuration page is used to set the time zone.

- **Direction**: Configures the time zone to be before (east of) or after (west of) UTC.
- **Name** – Assigns a name to the time zone. (Range: 1-30 characters)
- **Hours (0-13)** – The number of hours before/after UTC. The maximum value before UTC is 12. The maximum value after UTC is 13.
- **Minutes (0-59)** – The number of minutes before/after UTC.



6.10.6 Summer Time

The Maintenance >Time Setting >Summer Time page is used to set the system clock forward during the summer months (also known as daylight savings time). In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

- **Summer Time in Effect** – Shows if the system time has been adjusted.
- **Status** – Shows if summer time is set to take effect during the specified period.
- **Name** – Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)
- **Mode** – Selects one of the following configuration modes. (The Mode option can only be managed when the Summer Time Status option has been set to enabled for the switch.)

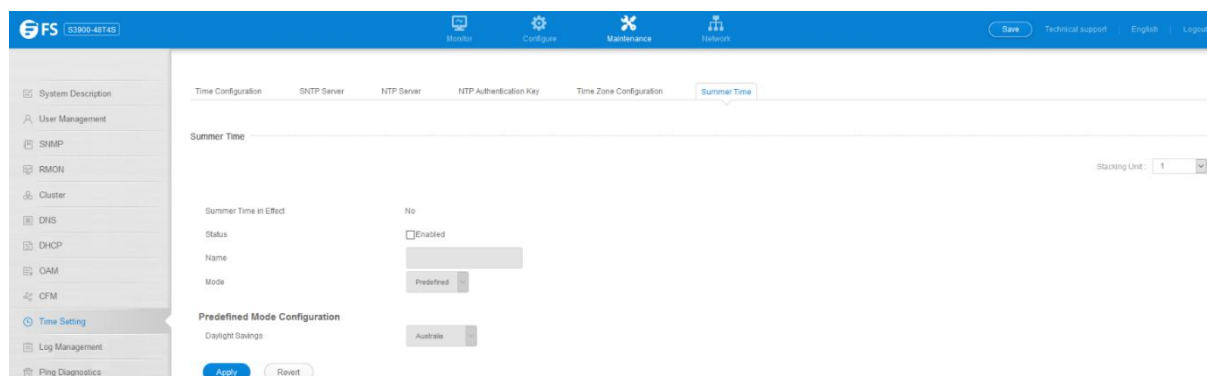
Predefined Mode – Configures the summer time status and settings for the switch using predefined configurations for several major regions of the world. To specify the time corresponding to your local time when summer time is in effect, select the predefined summer-time zone appropriate for your location.

Date Mode – Sets the start, end, and offset times of summer time for the switch on a one-time basis. This mode sets the summer-time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summertime zone deviates from your regular time zone.

- **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 1-120 minutes)
- **From** – Start time for summer-time offset.
- **To** – End time for summer-time offset.

Recurring Mode – Sets the start, end, and offset times of summer time for the switch on a recurring basis. This mode sets the summer-time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summertime zone deviates from your regular time zone.

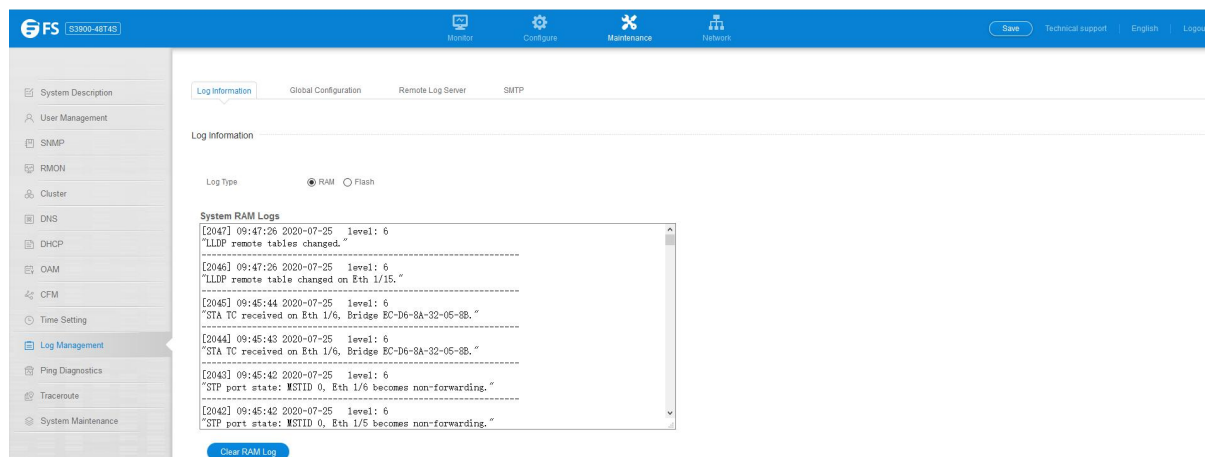
- **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 1-120 minutes)
- **From** – Start time for summer-time offset.
- **To** – End time for summer-time offset.



6.11 Log Management

6.11.1 Log Information

The Maintenance >Event Log >Log Information page is used to display System Logs.This page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset)and up to 4096 entries in permanent flash memory.

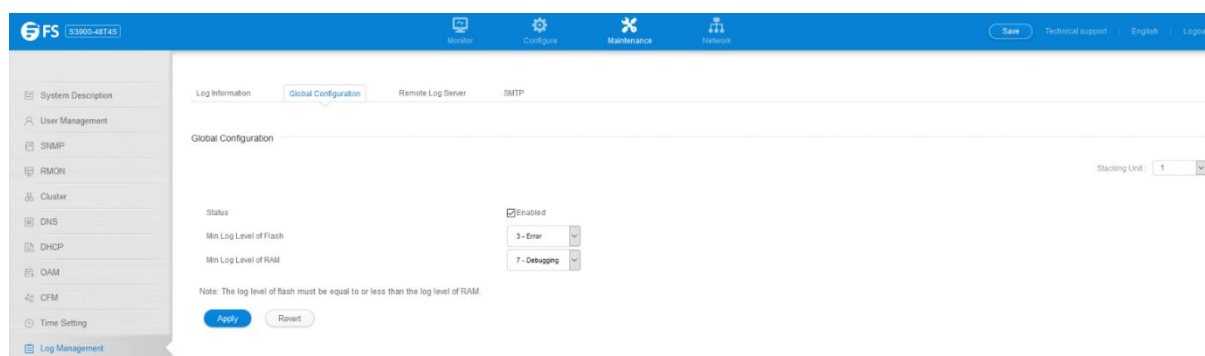


6.11.2 Global Configuration

The Maintenance >Event Log >Global Configuration page is used to enable or disable event logging, and specify which levels are logged to RAM or flash memory. Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

- **Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- **History Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)
- **History RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)



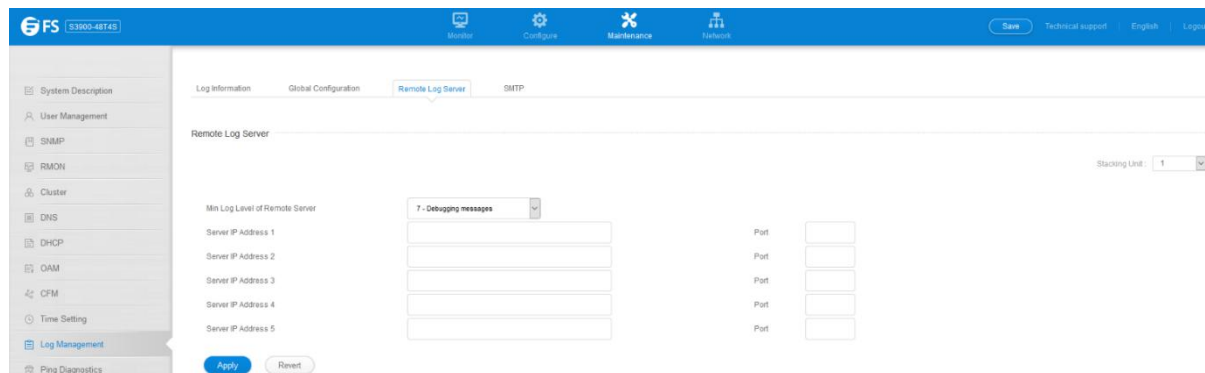
6.11.3 Remote Log Server

The Maintenance >Event Log >Remote Log Server page is used to send log messages to syslog servers or other management stations.

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service. The attribute specifies the facility type tag sent in syslog messages (see RFC 3164). This type has no effect on the kind of messages reported by the

switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)

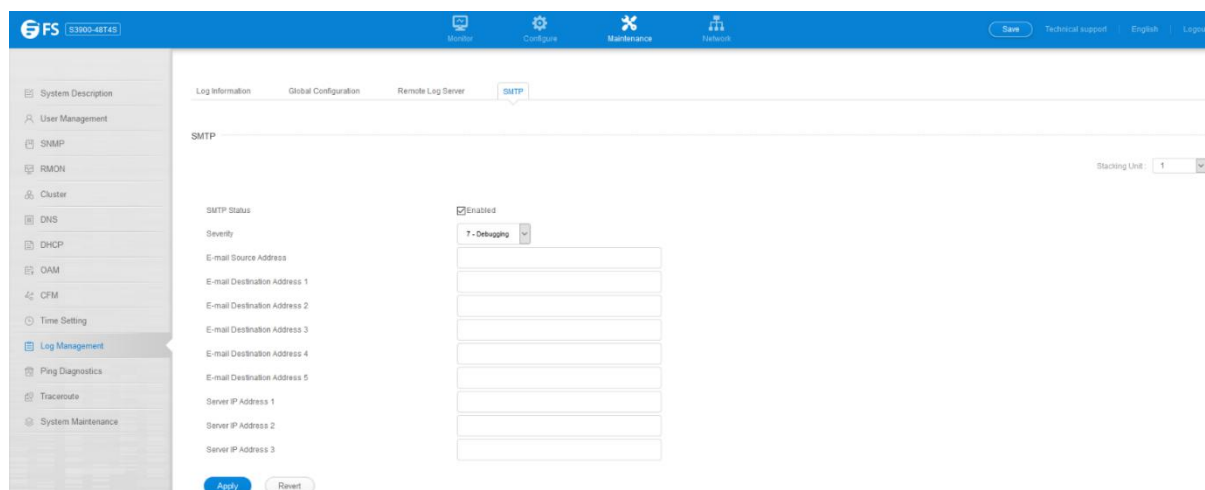
- **Logging Trap Level** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- **Server IP Address** – Specifies the IPv4 or IPv6 address of a remote server which will be sent syslog messages.



6.11.4 SMTP

The Maintenance >Event Log >SMTP page is used to alert system administrators of problems by sending SMTP (Simple Mail Transfer Protocol) email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

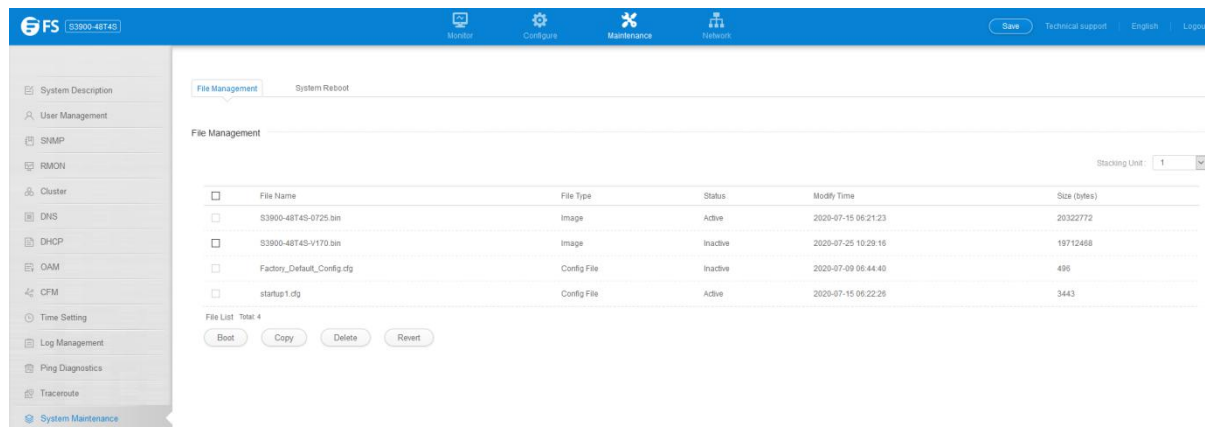
- **SMTP Status** – Enables/disables the SMTP function. (Default: Enabled)
- **Severity** – Sets the syslog severity threshold level used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)
- **Email Source Address** – Sets the email address used for the “From” field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch. (Range: 1-41 characters)
- **Email Destination Address** – Specifies the email recipients of alert messages. You can specify up to five recipients.
- **Server IP Address** – Specifies a list of up to three recipient SMTP servers. IPv4 or IPv6 addresses may be specified. The switch attempts to connect to the listed servers in sequential order if the first server fails to respond. For host name-to-IP address translation to function properly, host name lookup must be enabled, and one or more DNS servers specified.



6.12 System Maintenance

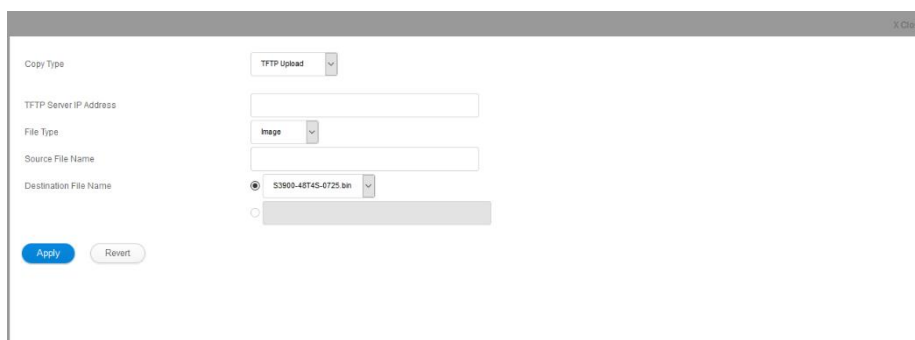
6.12.1 File Management

The Maintenance >System Maintenance >File Management page is used to manage the file in device. User can upload configuration file to PC, download runtime file to device. Copy a configuration file to another configuration file.



In the Maintenance >System Maintenance >File Management page, click copy button to download firmware or configuration settings using FTP, TFTP or HTTP.

- **Copy Type** – The firmware copy operation includes these options:
 - FTP Upload – Copies a file from an FTP server to the switch.
 - HTTP Upload – Copies a file from a management station to the switch.
 - TFTP Upload – Copies a file from a TFTP server to the switch.
- **FTP/TFTP Server IP Address** – The IP address of an FTP/TFTP server.
- **User Name** – The user name for FTP server access.
- **Password** – The password for FTP server access.
- **File Type** – Specify Operation Code to copy firmware.





Copy Type: HTTP Upload

File Type: Image

Source File Name: 浏览... 未选择文件.

Destination File Name: S3900-48T4S-0725.bin

Note: During firmware upload, the switch may not respond to commands for a couple of minutes.

Apply Revert

In the Maintenance >System Maintenance >File Management page, click copy button to save the current configuration settings to a local file on the switch. The configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to the current startup file, or to another file which can be subsequently set as the startup file.

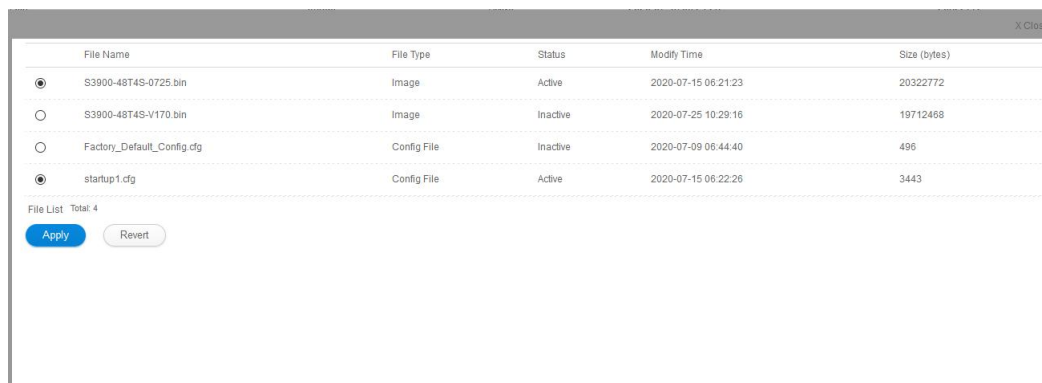


Copy Type: Running-Config

Destination File Name: startup1.cfg

Apply Revert

In the Maintenance >System Maintenance >File Management page, click Boot button to set the firmware or configuration file used for system initialization.



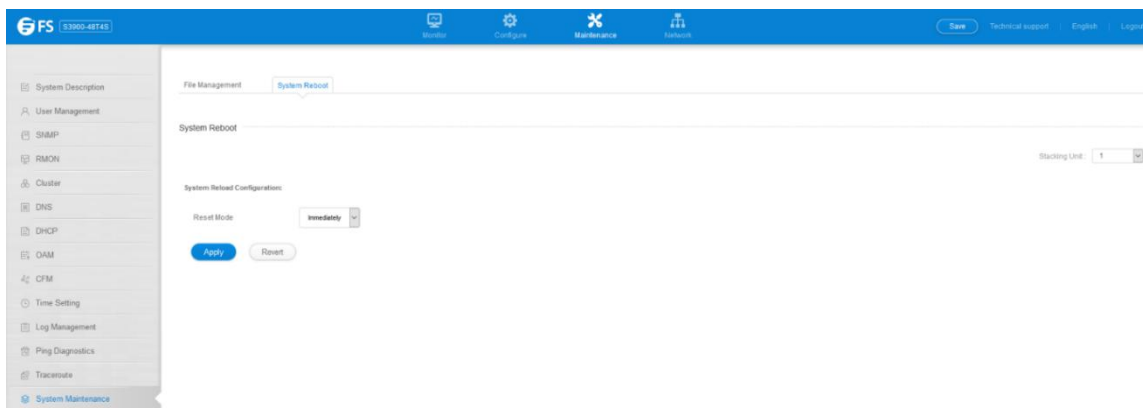
File Name	File Type	Status	Modify Time	Size (bytes)
<input checked="" type="radio"/> S3900-48T4S-0725.bin	Image	Active	2020-07-15 06:21:23	20322772
<input type="radio"/> S3900-48T4S-V170.bin	Image	Inactive	2020-07-25 10:29:16	19712468
<input type="radio"/> Factory_Default_Config.cfg	Config File	Inactive	2020-07-09 06:44:40	496
<input checked="" type="radio"/> startup1.cfg	Config File	Active	2020-07-15 06:22:26	3443

File List Total: 4

Apply Revert

6.12.2 System Reboot

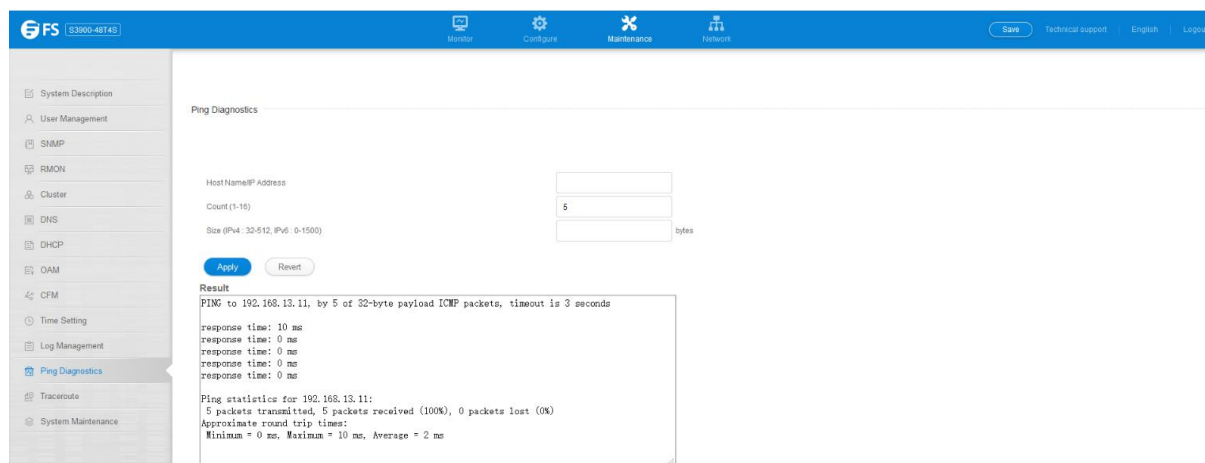
The Maintenance >System Maintenance >System Reboot page is used to restart the switch immediately, at a specified time, after a specified delay, or at a periodic interval.



6.13 Ping Diagnostics

The Maintenance >Ping page is used to send ICMP echo request packets to another node on the network.

- **Host Name/IP Address** – IP address or alias of the host.
- **Probe Count** – Number of packets to send. (Range: 1-16)
- **Packet Size** – Number of bytes in a packet. (Range: 32-512 bytes) The actual packet size will be eight bytes larger than the size specified because the switch adds header information.



6.14 Trace Route

The Maintenance >Trace Route page is used to show the route packets take to the specified destination.

- **Destination IP Address** – Alias or IPv4/IPv6 address of the host.
- **IPv4 Max Failures** – The maximum number of failures before which the trace route is terminated. (Fixed: 5)
- **IPv6 Max Failures** – The maximum number of failures before which the trace route is terminated. (Range: 1-255; Default: 5)

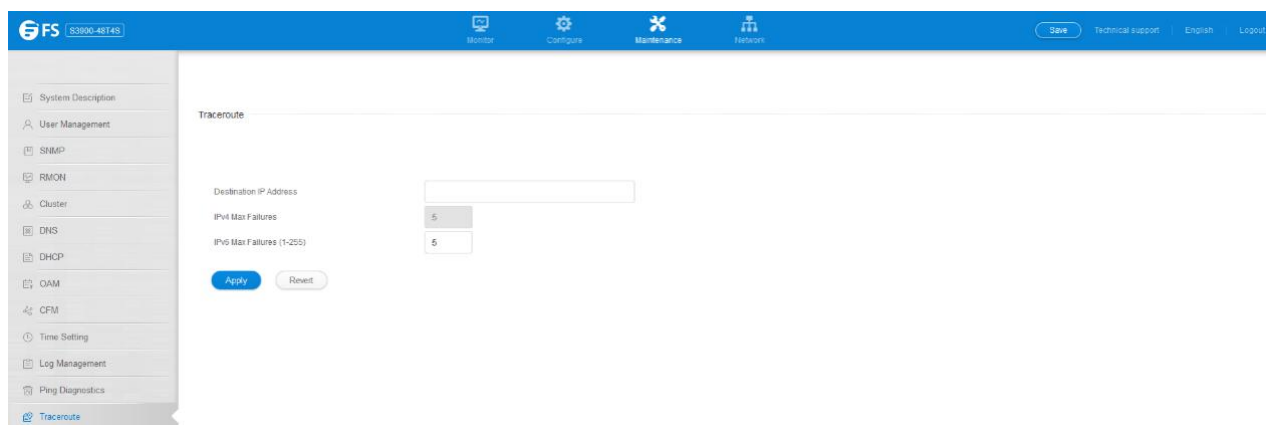
Command Usage

- Use the trace route function to determine the path taken to reach a specified destination.
- A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- The trace route function first sends probe datagrams with the TTL value set at one. This causes the first router to discard the

datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an “ICMP port unreachable” message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the “Request Timed Out” message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter.

For example, FE80::7272%1 identifies VLAN 1 as the interface from which the trace route is sent.



Traceroute Result

Tracing route over a maximum of 30 hops, or a maximum of 5 consecutive failures.

Destination IP Address: 192.168.13.11

ID	IP Address	Packet 1 Response	Packet 2 Response	Packet 3 Response
1	192.168.13.11	10ms	10ms	10ms
Trace complete				

Stop
Close Window



 <https://www.fs.com>



The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.