4.6 Spanning Tree Protocol

4.6.1 Theory

The Spanning Tree Protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

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

The **IEEE 802.1D Spanning Tree** Protocol and **IEEE 802.1w Rapid Spanning Tree** Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port

- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN to which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- **Blocking** – the port is blocked from forwarding or receiving packets
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets
- **Forwarding** – the port is forwarding packets
- **Disabled** – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

- From disabled to blocking

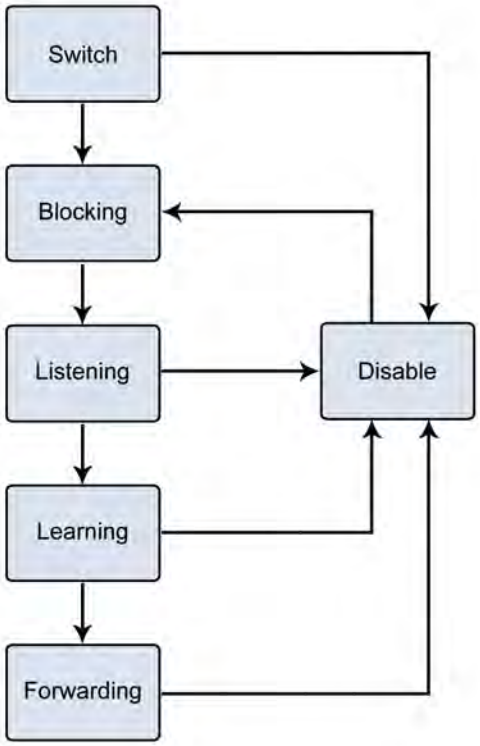


Figure 4-6-1 STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

2. STP Parameters

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note

On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges. On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier(Not user configurable	A combination of the User-set priority and the switch's MAC address.	32768 + MAC

except by setting priority below)	The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-Changeable STA Parameters

The Switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory unless it is absolutely necessary. The user changeable parameters in the Switch are as follows:

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

Note

The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the

Switch spends in the listening state while moving from the blocking state to the forwarding state.

Note

Observe the following formulas when setting the above parameters:

Max. Age _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

3. Illustration of STP

A simple illustration of three switches connected in a loop is depicted in the diagram below. In this example, you can anticipate some major network problems if the STP assistance is not applied.

If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings.

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting up STP using values other than the defaults can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straightforward.

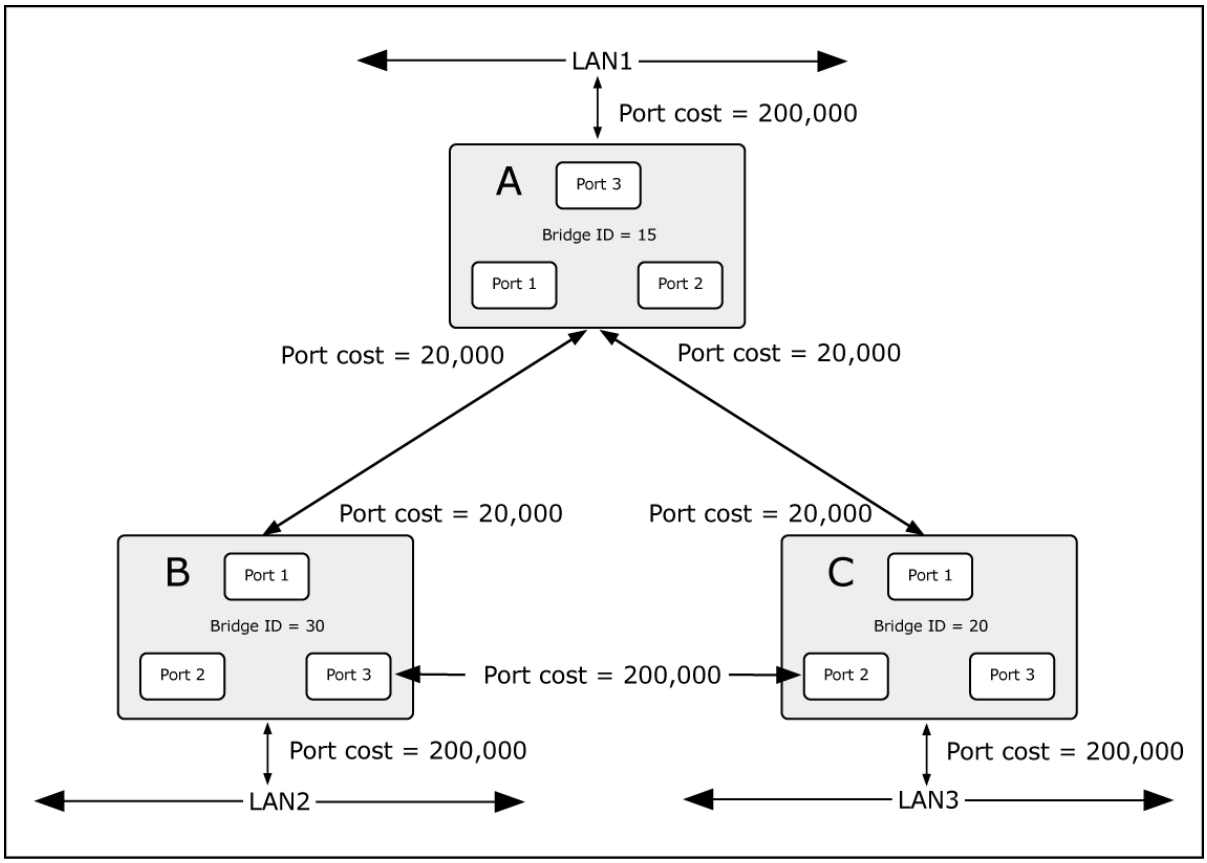


Figure 4-6-2 Before Applying the STA Rules

In this example, only the default STP values are used.

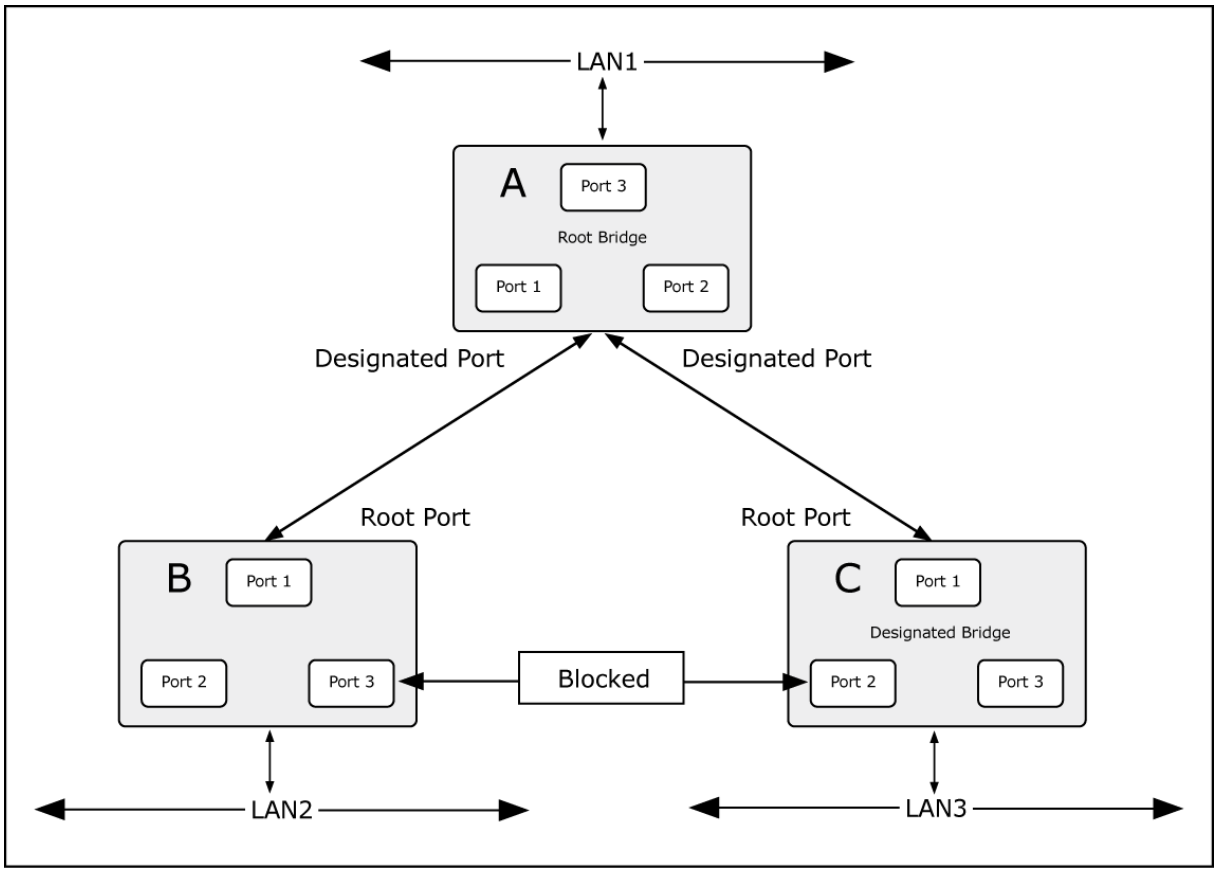


Figure 4-6-3 After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected as the root bridge, and the ports were selected to give a high port cost between switch B and switch C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switches B and C. The redundant link between switches B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

This section has the following items:

- **STP Global Setting** Configures STP system settings
- **STP Port Setting** Configuration per port STP setting
- **CIST Instance Setting** Configures system configuration
- **CIST Port Setting** Configures CIST port setting
- **MST Instance Setting** Configuration each MST instance setting
- **MST Port Setting** Configuration per port MST setting
- **STP Statistics** Displays the STP statistics

4.6.2 STP Global Settings

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch. The Managed Switch supports the following Spanning Tree protocols:

- **Compatible -- Spanning Tree Protocol (STP):** Provides a single path between end stations, avoiding and eliminating loops.
- **Normal -- Rapid Spanning Tree Protocol (RSTP):** Detects and uses network topologies that provide faster spanning tree convergence, without creating forwarding loops.
- **Extension – Multiple Spanning Tree Protocol (MSTP):** Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

The STP Global Settings screens in Figure 4-6-4 and Figure 4-6-5 appear.

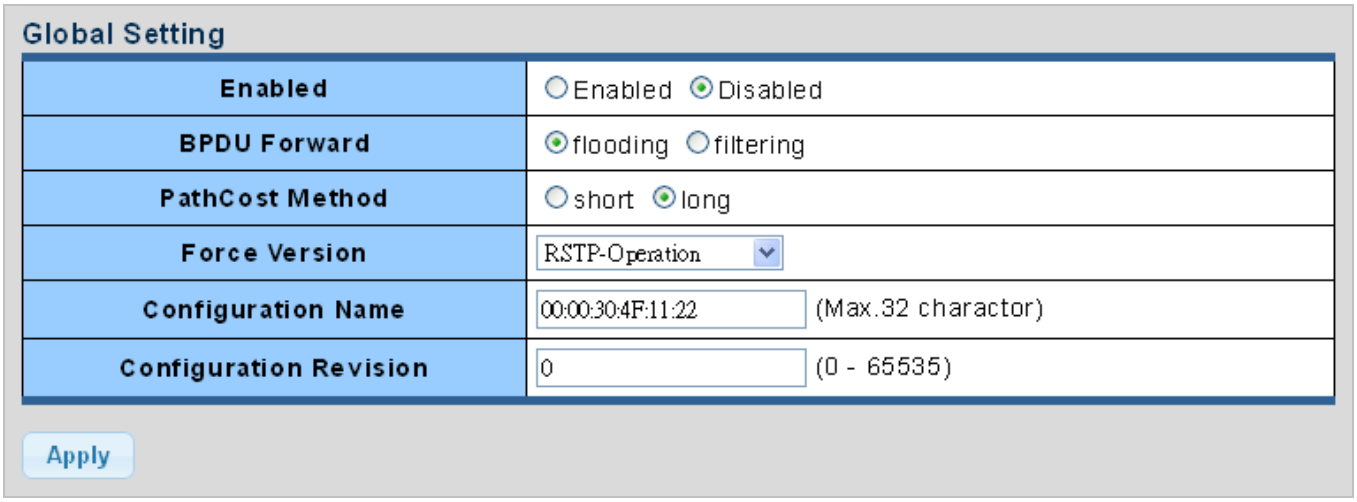


Figure 4-6-4 Global Settings Screenshot

The page includes the following fields:

Object	Description
• **Enable**	Enable or disable the STP function. The default value is "Disabled".
• **BPDU Forward**	Set the BPDU forward method.
• **PathCost Method**	The path cost method is used 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.
• **Force Version**	The STP protocol version setting. Valid values are **STP-Compatible**,

	RSTP-Operation and **MSTP-Operation**.
• **Configuration Name**	Identifier used to identify the configuration currently being used.
• **Configuration Revision**	Identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is **0**.

Buttons

Apply: Click to apply changes.

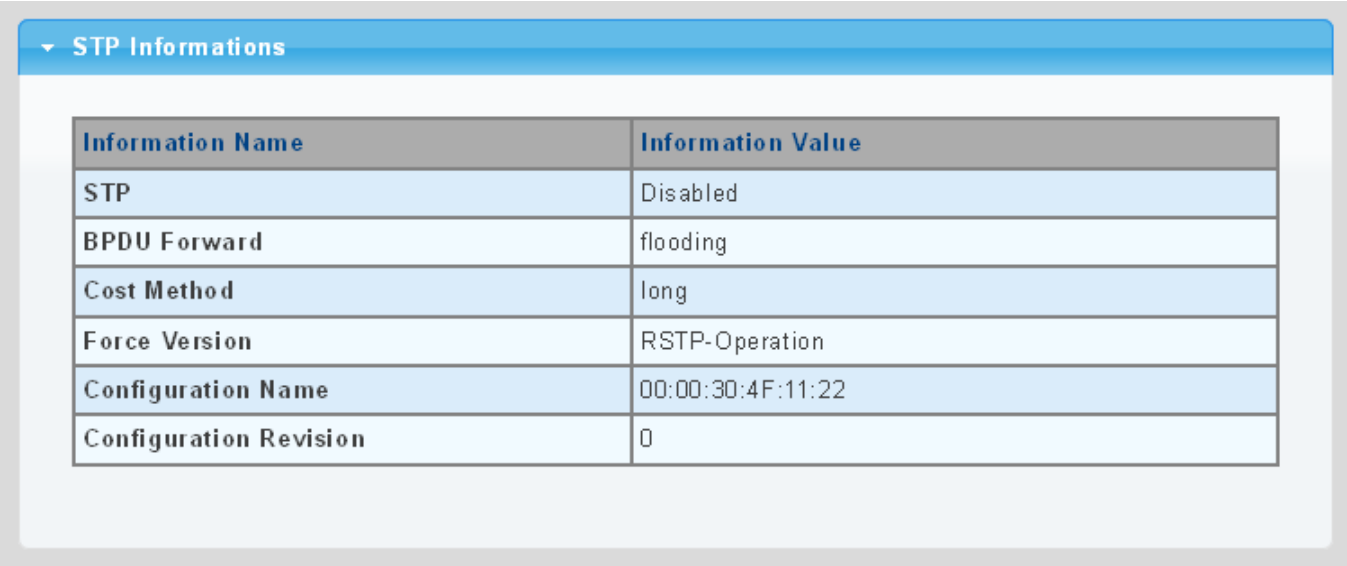


Figure 4-6-5 STP Information Screenshot

The page includes the following fields:

Object	Description
• **STP**	Display the current STP state
• **BPDU Forward**	Display the current BPDU forward mode
• **Cost Method**	Display the current cost method
• **Force Version**	Display the current force version
• **Configuration Name**	Display the current configuration name
• **Configuration Revision**	Display the current configuration revision

4.6.3 STP Port Setting

This page allows you to configure per port STP settings. The STP Port Setting screens in Figure 4-6-6 and Figure 4-6-7 appear.

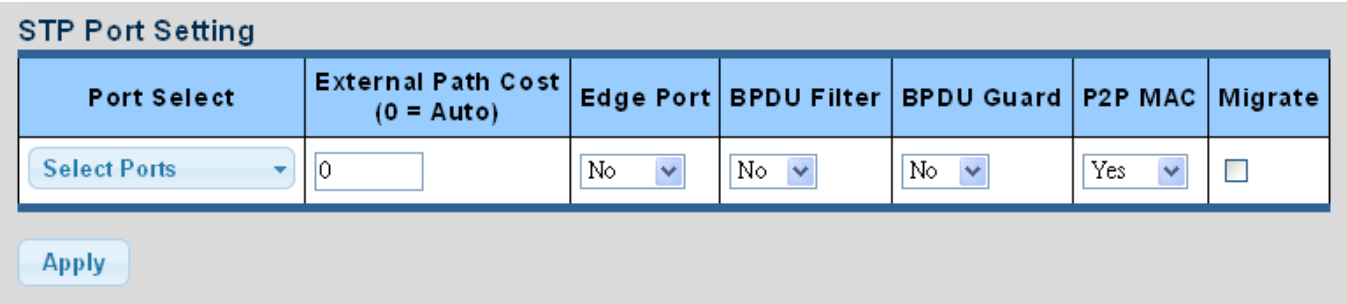


Figure 4-6-6 STP Port Configuration Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number from this drop-down list.
• **External Cost (0 = Auto)**	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range from 1 to 200000000.
• **Edge Port**	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).
• **BPDU Filter**	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
• **BPDU Guard**	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
• **P2P MAC**	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always *forced Point2Point*).
• **Migrate**	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**)

Buttons

Apply: Click to apply changes.

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.

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

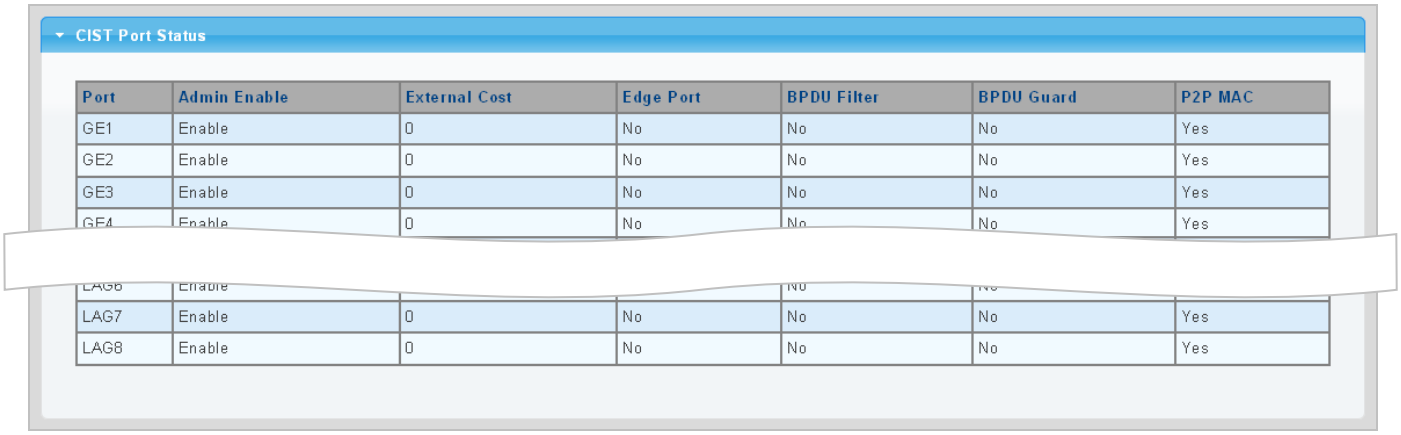
Table 4-6-1 Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 4-6-2 Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Table 4-6-3 Default STP Path Costs



CIST Port Status

Port	Admin Enable	External Cost	Edge Port	BPDU Filter	BPDU Guard	P2P MAC
GE1	Enable	0	No	No	No	Yes
GE2	Enable	0	No	No	No	Yes
GE3	Enable	0	No	No	No	Yes
GE4	Enable	0	No	No	No	Yes
LAG6	Enable			No		
LAG7	Enable	0	No	No	No	Yes
LAG8	Enable	0	No	No	No	Yes

Figure 4-6-7 STP Port Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **Admin Enable**	Display the current STP port mode status
• **External Cost**	Display the current external cost.
• **Edge Port**	Display the current edge port status.
• **BPDU Filter**	Display the current BPDU filter configuration.
• **BPDU Guard**	Display the current BPDU guard configuration.
• **P2P MAC**	Display the current P2P MAC status.

4.6.4 CIST Instance Setting

This page allows you to configure CIST instance settings. The CIST Instance Setting and Information screens in Figure 4-6-8 and Figure 4-6-9 appear.

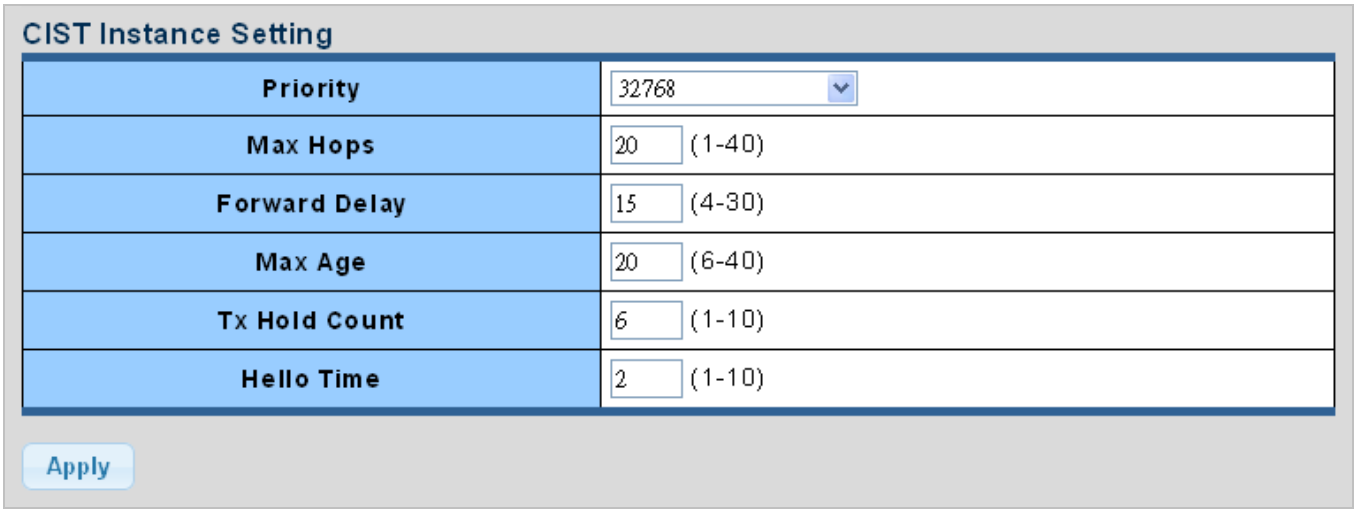


Figure 4-6-8: CIST Instance Setting Screenshot

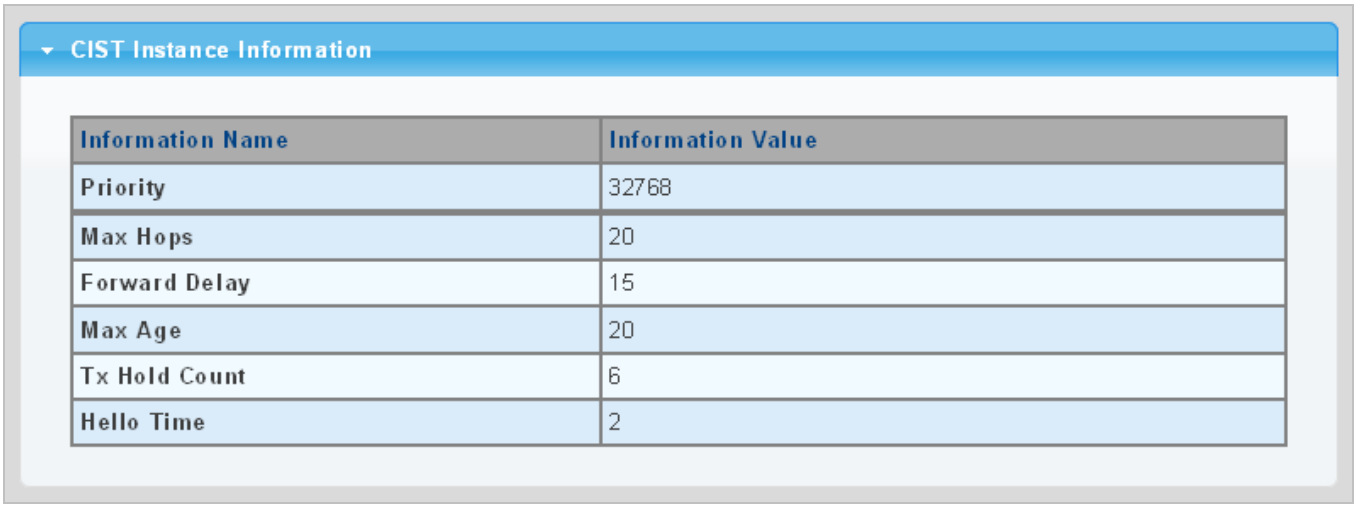
The page includes the following fields:

Object	Description
• **priority**	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
• **Max Hops**	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range from 6 to 40 hops.
• **Forward Delay**	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range from 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
• **Max Age**	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range from 6 to 40 seconds. -Default: 20 -Minimum: The higher of 6 or [2 x (Hello Time + 1)]. -Maximum: The lower of 40 or [2 x (Forward Delay -1)]

• **Tx Hold Count**	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range from 1 to 10 BPDU's per second.
• **Hello Time**	The time that controls the switch to send out the BPDU packet to check STP current status. Enter a value between 1 and10.

Buttons

Apply: Click to apply changes.



Information Name	Information Value
Priority	32768
Max Hops	20
Forward Delay	15
Max Age	20
Tx Hold Count	6
Hello Time	2

Figure 4-6-9 CIST Instance Information Screenshot

The page includes the following fields:

Object	Description
• **Priority**	Display the current CIST priority
• **Max Hop**	Display the current Max. hop
• **Forward Delay**	Display the current forward delay
• **Max Age**	Display the current Max.Age
• **Tx Hold Count**	Display the current Tx hold count
• **Hello Time**	Display the current hello time

4.6.5 CIST Port Setting

This page allows you to configure per port CIST priority and cost. The CIST Port Setting and Status screens in Figure 4-6-10 and Figure 4-6-11 appear.

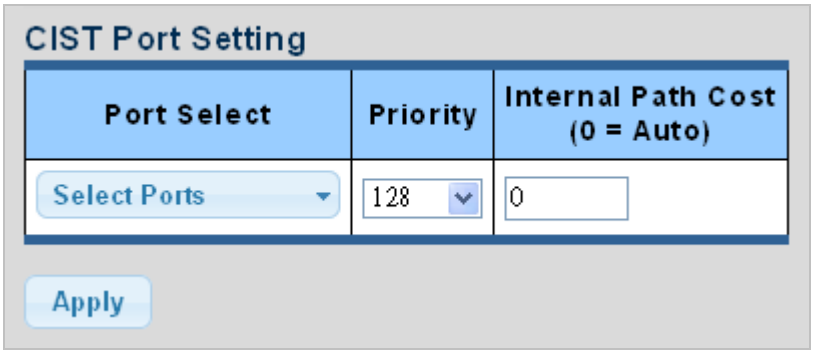


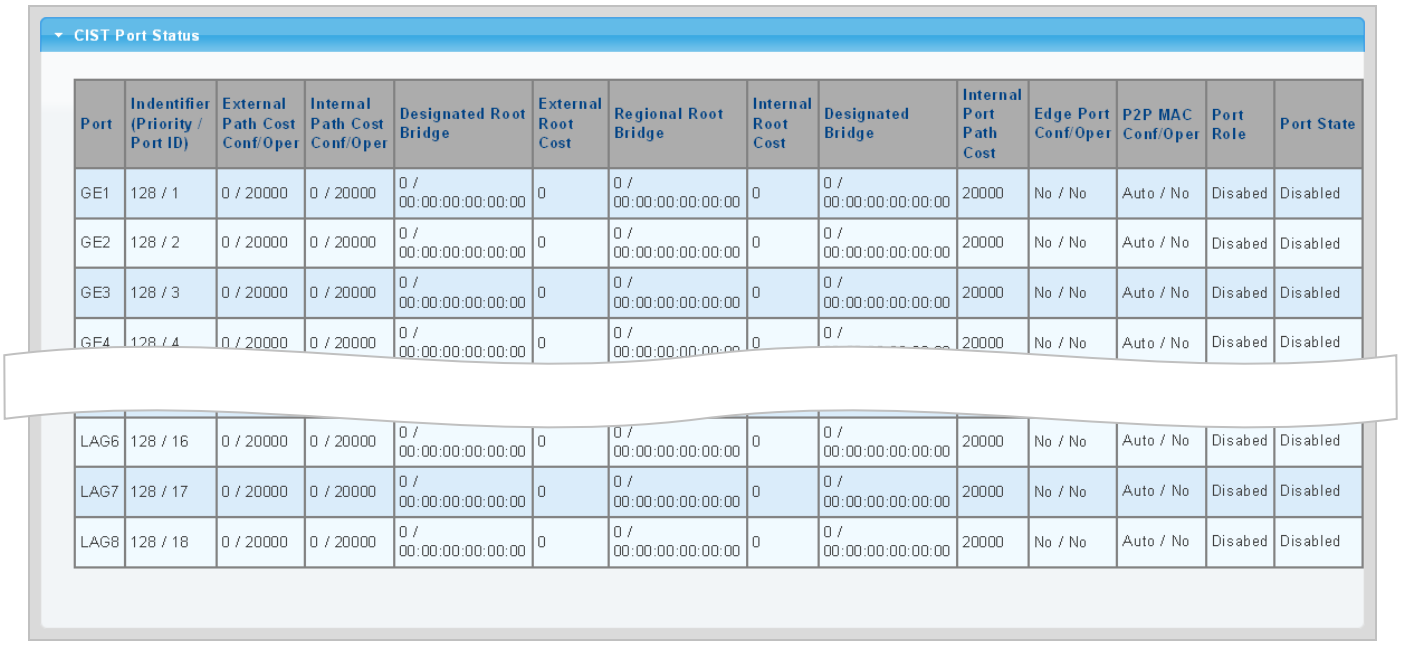
Figure 4-6-10 CIST Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number from this drop-down list.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: **128** Range: 0-240, in steps of 16
• **Internal Path Cost (0 = Auto)**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. By using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range from 1 to 200000000.

Buttons

Apply: Click to apply changes.



CIST Port Status

Port	Indentifier (Priority / Port ID)	External Path Cost Conf/Oper	Internal Path Cost Conf/Oper	Designated Root Bridge	External Root Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Port Path Cost	Edge Port Conf/Oper	P2P MAC Conf/Oper	Port Role	Port State
GE1	128 / 1	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE2	128 / 2	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE3	128 / 3	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE4	128 / 4	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 /	20000	No / No	Auto / No	Disabed	Disabled
LAG6	128 / 16	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG7	128 / 17	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG8	128 / 18	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled

Figure 4-6-11 CIST Port Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port
• **Identifier (Priority/ Port ID)**	Display the current identifier (Priority/Port ID)
• **External Path Cost Conf/Oper**	Display the current external path cost conf/oper
• **Internal Path Cost Conf/Oper**	Display the current internal path cost/oper
• **Designated Root Bridge**	Display the current designated root bridge
• **External Root Cost**	Display the current external root cost
• **Regional Root Bridge**	Display the current regional root bridge
• **Internal Root Cost**	Display the current internal root cost
• **Designated Bridge**	Display the current designated bridge
• **Internal Port Path Cost**	Display the current internal port path cost
• **Edge Port Conf/Oper**	Display the current edge port conf/oper
• **P2P MAC Conf/Oper**	Display the current P2P MAC conf/oper
• **Port Role**	Display the current port role
• **Port State**	Display the current port state

4.6.6 MST Instance Configuration

This page allows the user to configure MST Instance Configuration. The MST Instance Setting, Information and Status screens in Figure 4-6-12, Figure 4-6-13 and Figure 4-6-14 appear.

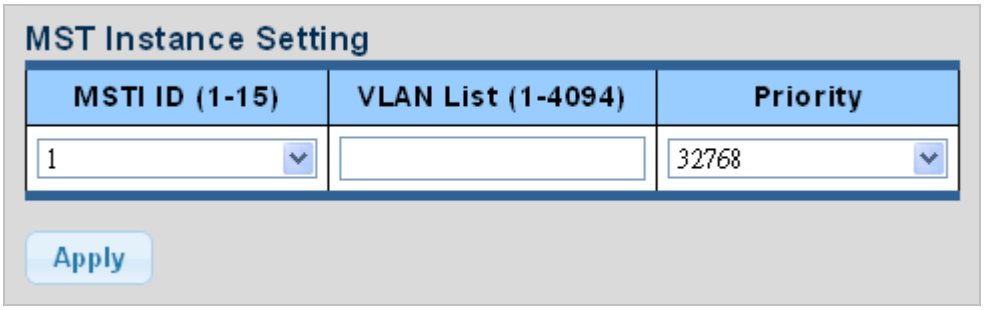


Figure 4-6-12 MST Instance Setting Screenshot

The page includes the following fields:

Object	Description
• **MSTI ID**	Allow to assign MSTI ID. The range for the MSTI ID is 1-15.
• **VLAN List (1-4096)**	Allow to assign VLAN list to special MSTI ID. The range for the VLAN list is 1-4094.
• **Priority**	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

Apply: Click to apply changes.

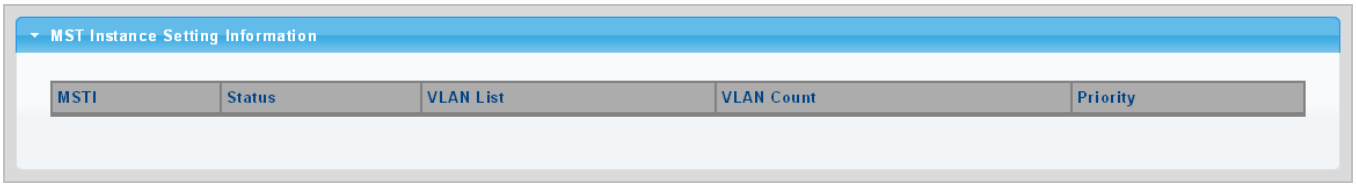


Figure 4-6-13 MSTI Instance Setting Information Screenshot

The page includes the following fields:

Object	Description
• **MSTI**	Display the current MSTI entry
• **Status**	Display the current MSTI status

• **VLAN List**	Display the current VLAN list
• **VLAN Count**	Display the current VLAN count
• **Priority**	Display the current MSTI priority

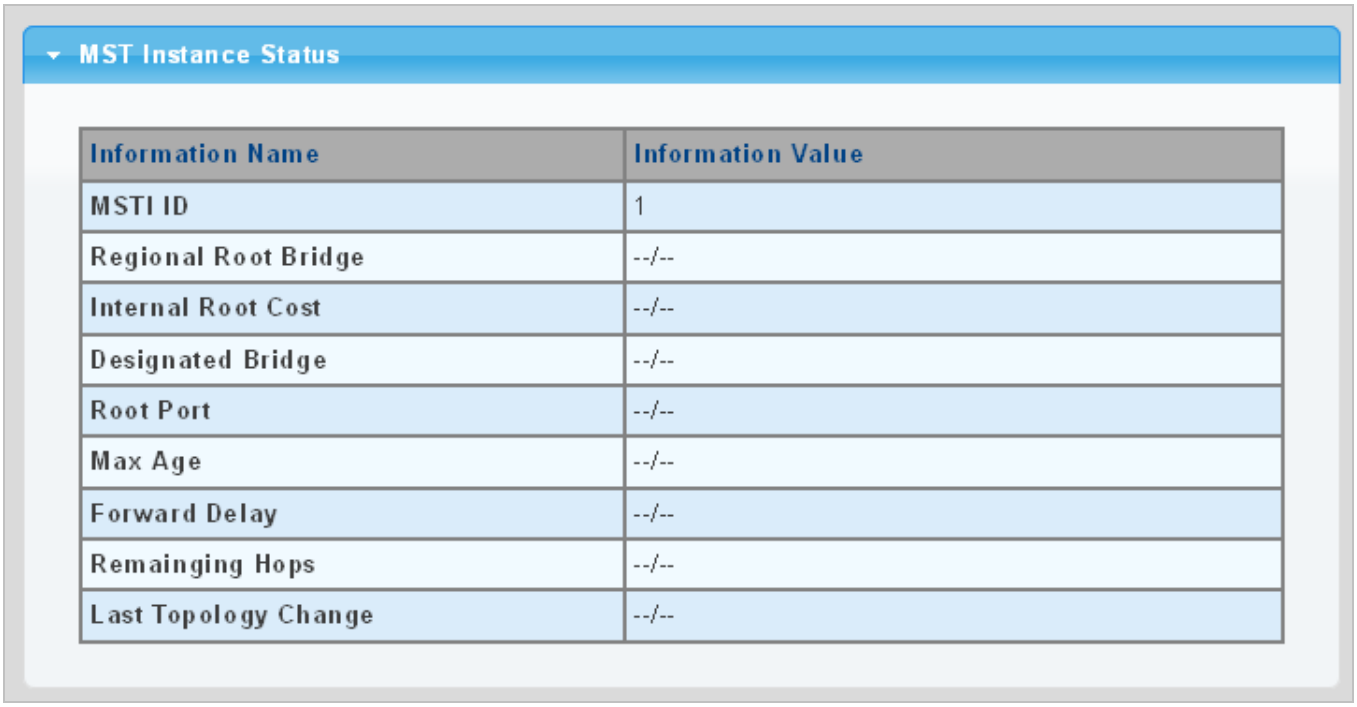


Figure 4-6-14 MST Instance Status Screenshot

The page includes the following fields:

Object	Description
• **MSTI ID**	Display the MSTI ID.
• **Regional Root Bridge**	Display the current designated root bridge
• **Internal Root Cost**	Display the current internal root cost
• **Designated Bridge**	Display the current designated bridge
• **Root Port**	Display the current root port.
• **Max Age**	Display the current max. age.
• **Forward Delay**	Display the current forward delay.
• **Remaining Hops**	Display the current remaining hops.
• **Last Topology Change**	Display the current last topology change.

4.6.7 MST Port Setting

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are global. The MSTI Ports Setting screens in Figure 4-6-15 and Figure 4-6-16 appear.

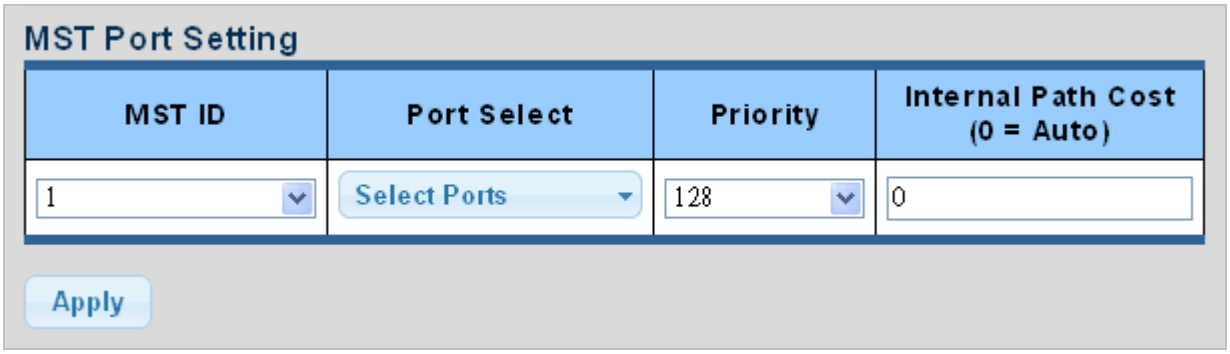


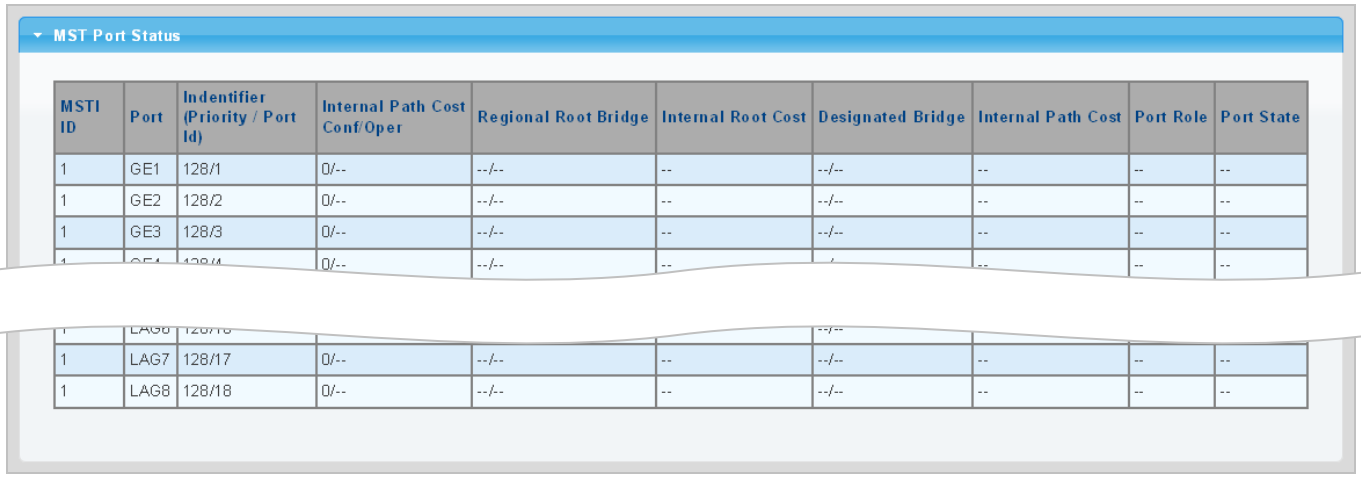
Figure 4-6-15 MST Port Configuration Screenshot

The page includes the following fields:

Object	Description
• **MST ID**	Enter the special MST ID to configure path cost and priority.
• **Port Select**	Select port number from this drop-down list.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost.
• **Internal Path Cost (0 = Auto)**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range from 1 to 200000000.

Buttons

Apply: Click to apply changes.



MST Port Status

MSTI ID	Port	Indentifier (Priority / Port Id)	Internal Path Cost Conf/Oper	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Path Cost	Port Role	Port State
1	GE1	128/1	0/--	--/--	--	--/--	--	--	--
1	GE2	128/2	0/--	--/--	--	--/--	--	--	--
1	GE3	128/3	0/--	--/--	--	--/--	--	--	--
1	GE4	128/4	0/--	--/--	--	-/-	--	--	--
1	LAG6	128/16				--/--			
1	LAG7	128/17	0/--	--/--	--	--/--	--	--	--
1	LAG8	128/18	0/--	--/--	--	--/--	--	--	--

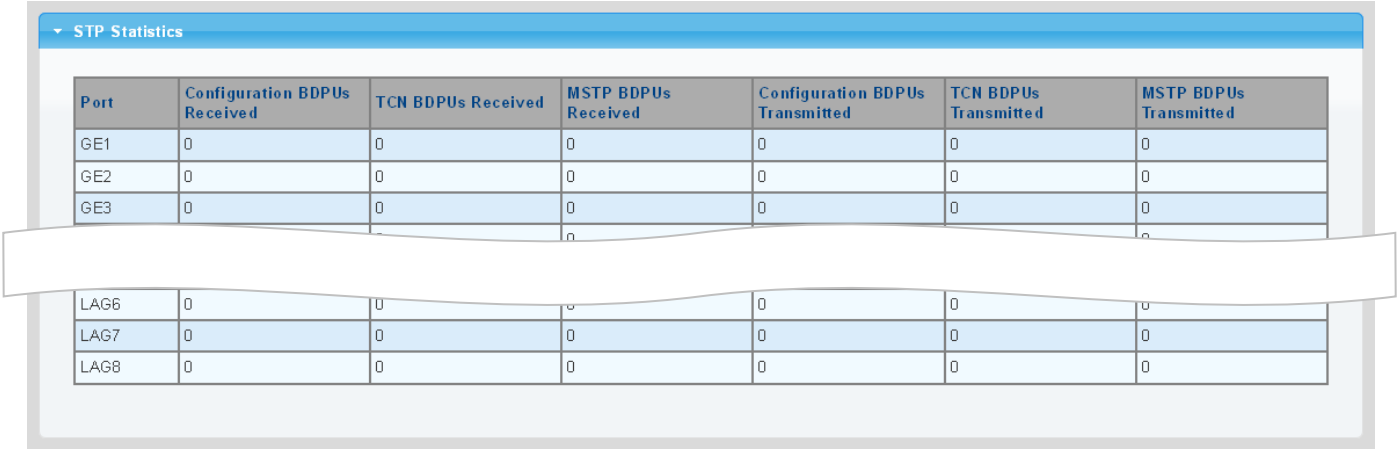
Figure 4-6-16 MST Port Status Screenshot

The page includes the following fields:

Object	Description
• **MSTI ID**	Display the current MSTI ID
• **Port**	The switch port number of the logical STP port
• **Indentifier (Priority / Port ID)**	Display the current indentifier (priority / port ID)
• **Internal Path Cost Conf/Oper**	Display the current internal path cost configuration / operation
• **Regional Root Bridge**	Display the current regional root bridget
• **Internal Root Cost**	Display the current internal root cost
• **Designated Bridge**	Display the current designated bridge
• **Internal Path Cost**	Display the current internal path cost
• **Port Role**	Display the current port role
• **Port State**	Display the current port state

4.6.8 STP Statistics

This page displays STP statistics. The STP statistics screen in Figure 4-6-17 appears.



STP Statistics

Port	Configuration BDPUs Received	TCN BDPUs Received	MSTP BDPUs Received	Configuration BDPUs Transmitted	TCN BDPUs Transmitted	MSTP BDPUs Transmitted
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
LAG6	0	0	0	0	0	0
LAG7	0	0	0	0	0	0
LAG8	0	0	0	0	0	0

Figure 4-6-17 STP Statistics Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port
• **Configuration BPDUs Received**	Display the current configuration BPDUs received
• **TCN BPDUs Received**	Display the current TCN BPDUs received
• **MSTP BPDUs Received**	Display the current MSTP BPDUs received
• **Configuration BPDUs Transmitted**	Display the configuration BPDUs transmitted
• **TCN BPDUs Transmitted**	Display the current TCN BPDUs transmitted
• **MSTP BPDUs Transmitted**	Display the current BPDUs transmitted

4.7 Multicast

This section has the following items:

- **Properties** — Configures multicast properties
- **IGMP Snooping** — Configures IGMP snooping settings
- **IGMP Snooping Statistics** — Displays the IGMP snooping statistics
- **MLD Snooping** — Configures MLD snooping settings
- **MLD Snooping Statistics** — Displays the MLD snooping statistics
- **Multicast Throttling Setting** — Configures multicast throttling setting
- **Multicast Filter** — Configures multicast filter

4.7.1 Properties

This page provides multicast properties related configuration.

The multicast Properties and Information screen in Figure 4-7-1 and Figure 4-7-2 appear.

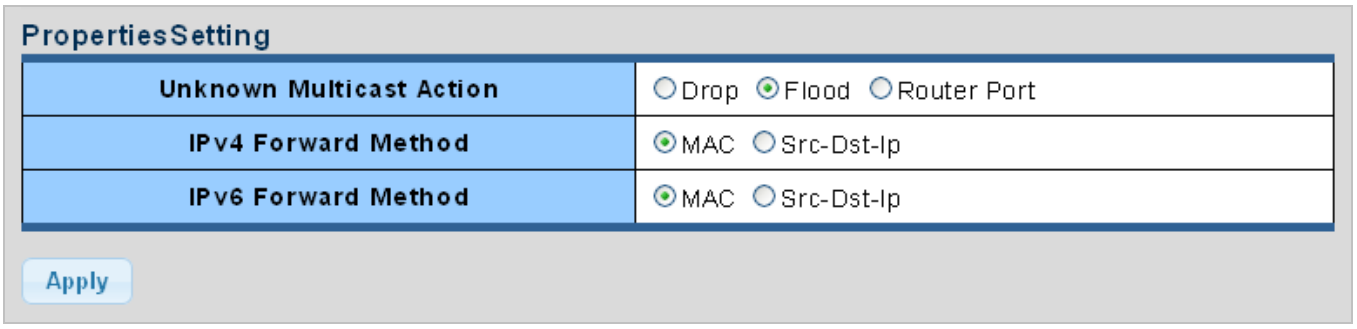


Figure 4-7-1 Properties Setting Screenshot

The page includes the following fields:

Object	Description
• **Unknown Multicast Action**	Unknown multicast traffic method: **Drop**, **flood** or send to **router port**.
• **IPv4 Forward Method**	Configure the IPv4 multicast forward method
• **IPv6 Forward Method**	Configure the IPv6 multicast forward method

Buttons

Apply: Click to apply changes.

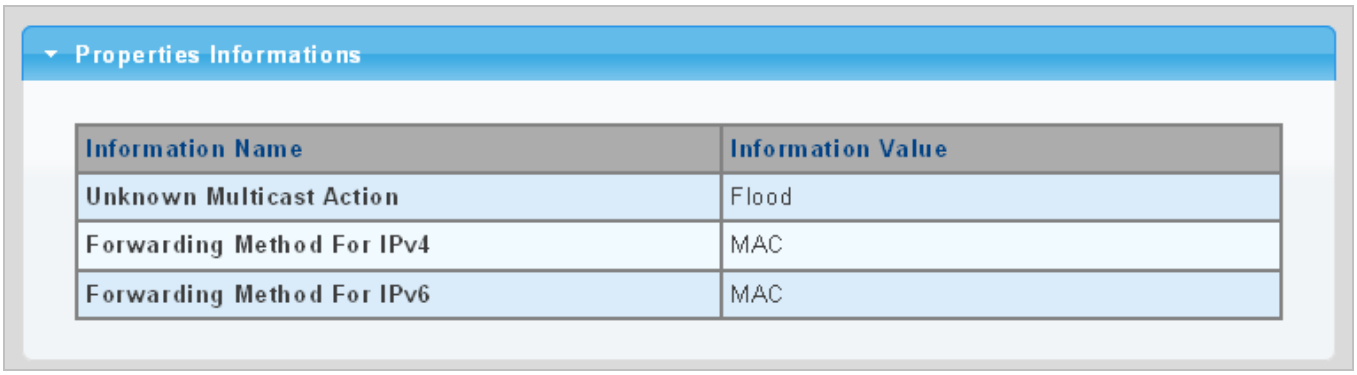


Figure 4-7-2 Properties Information Screenshot

The page includes the following fields:

Object	Description
• **Unknown Multicast Action**	Display the current unknown multicast action status
• **Forward Method For IPv4**	Display the current IPv4 multicast forward method
• **Forward Method For IPv6**	Display the current IPv6 multicast forward method

4.7.2 IGMP Snooping

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

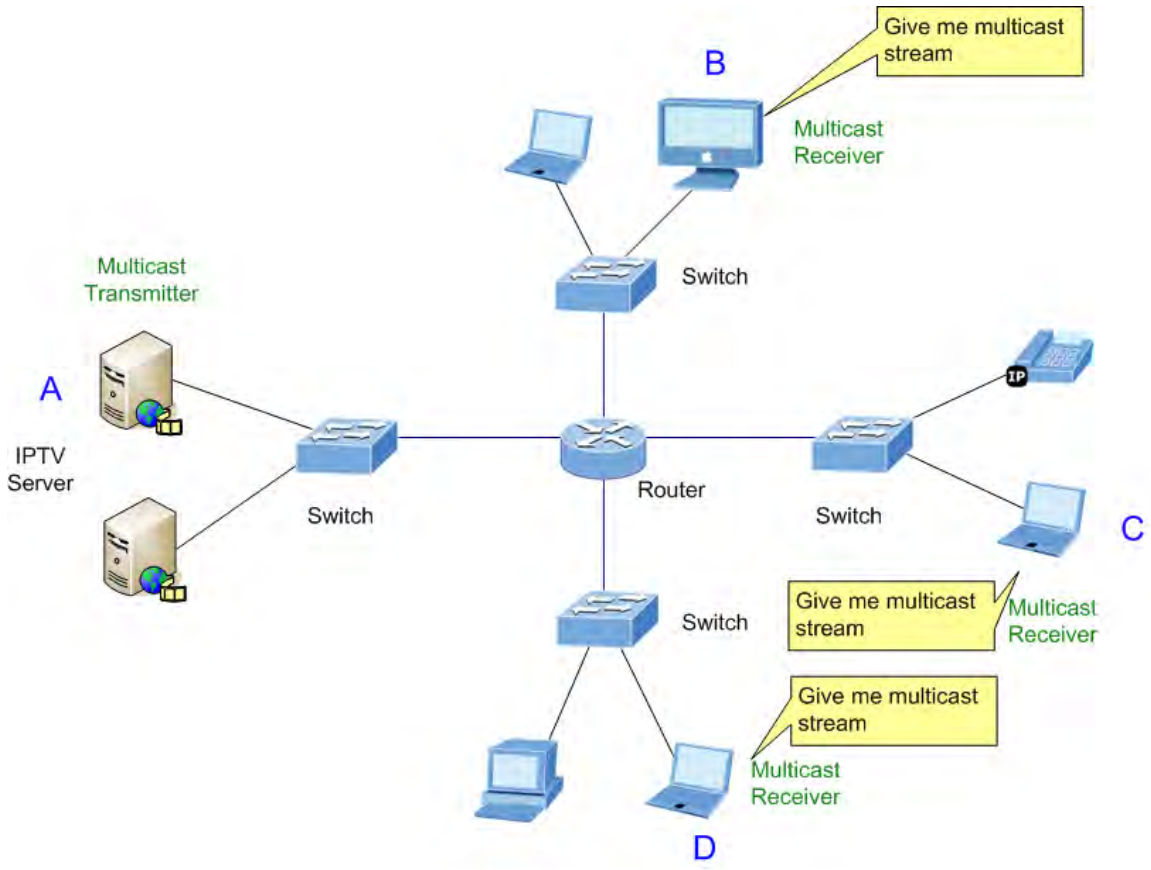


Figure 4-7-3 Multicast Service

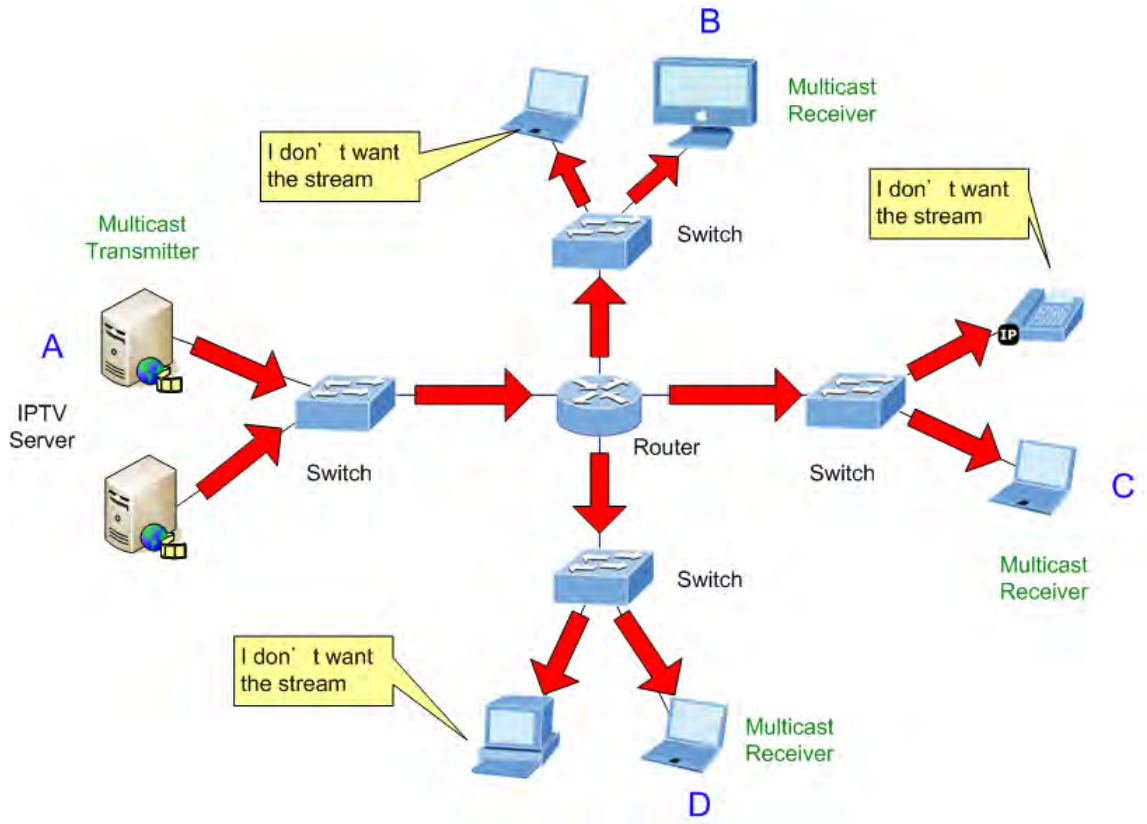


Figure 4-7-4 Multicast Flooding

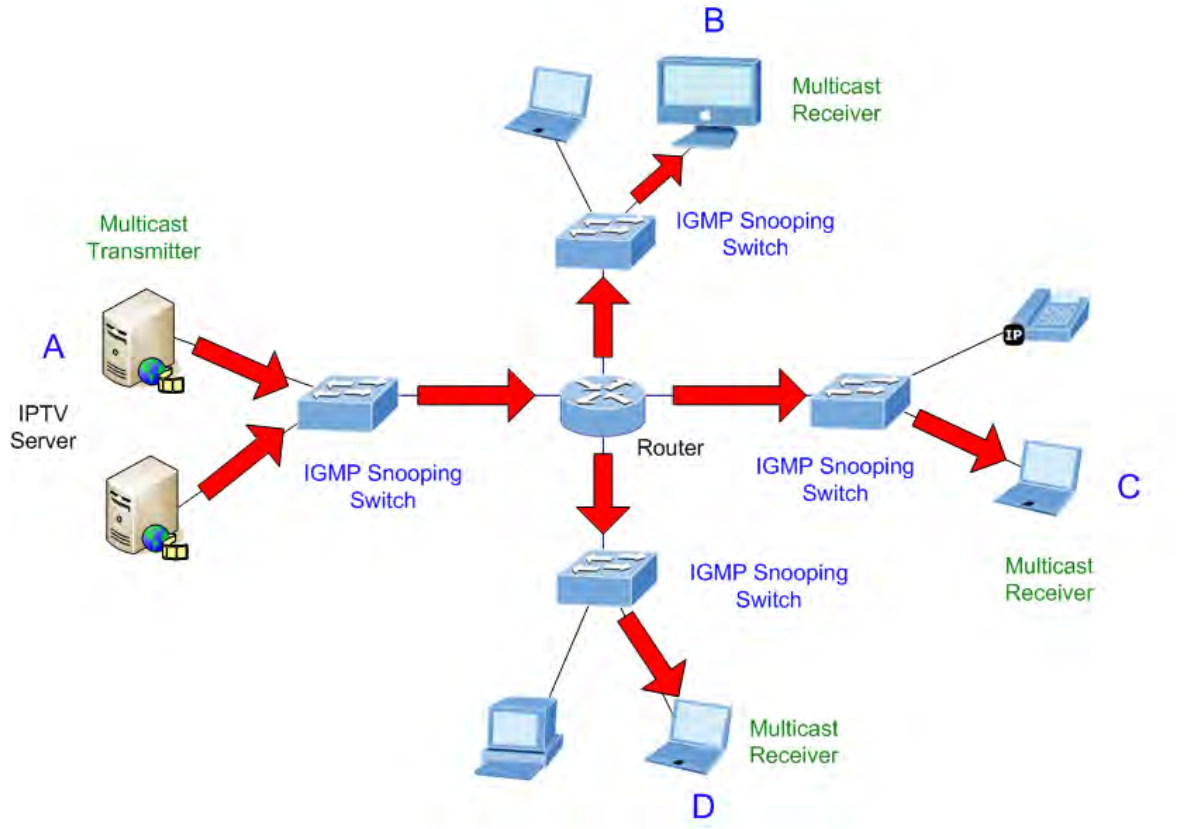


Figure 4-7-5 IGMP Snooping Multicast Stream Control

IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0	8	16	31
Type	**Response Time**	**Checksum**	
Group Address (all zeros if this is a query)			

The IGMP Type codes are shown below:

Type	Definition
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)

0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)
0x12	Membership Report (version 1)

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

A host sends an IGMP **"report"** to join a group

A host will never send a report when it wants to leave a group (for version 1).

A host will send a **"leave"** report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:

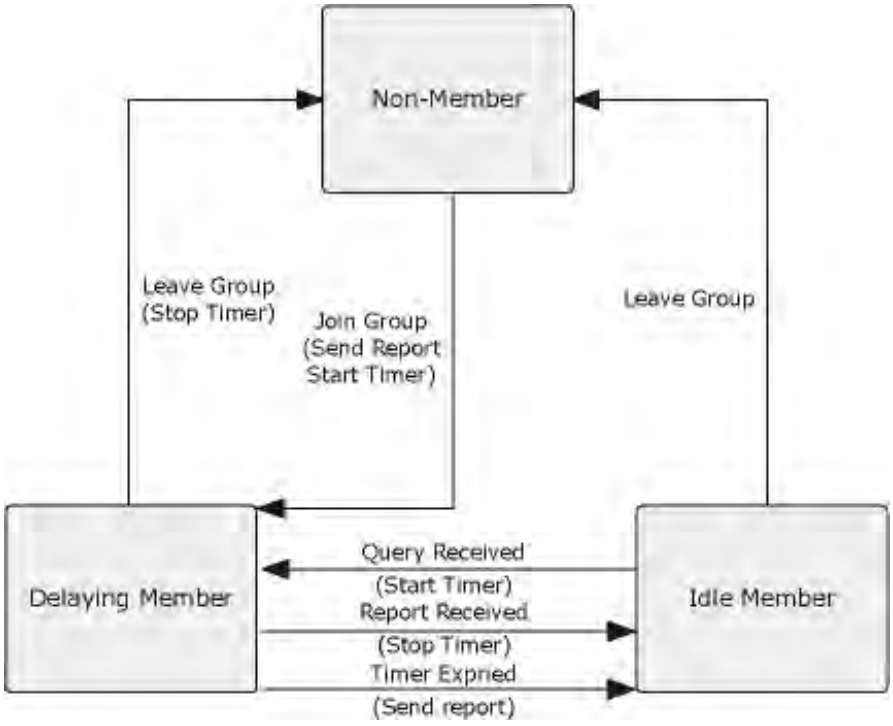


Figure 4-7-6 IGMP State Transitions

■ **IGMP Querier –**

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "**querier**" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note

Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

4.7.2.1 IGMP Setting

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header. The IGMP Snooping Setting and Information screens in Figure 4-7-7, Figure 4-7-8 and Figure 4-7-9 appear.

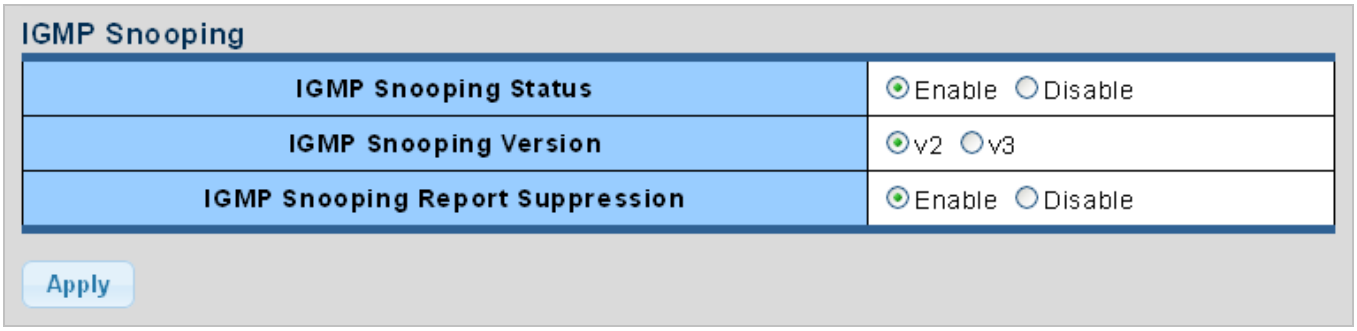


Figure 4-7-7 IGMP Snooping Screenshot

The page includes the following fields:

Object	Description
• **IGMP Snooping Status**	Enable or disable the IGMP snooping. The default value is "Disabled".
• **IGMP Snooping Version**	Sets the IGMP Snooping operation version. Possible versions are: ■ **v2**: Set IGMP Snooping supported IGMP version 2. ■ **v3**: Set IGMP Snooping supported IGMP version 3.
• **IGMP Snooping Report Suppression**	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.

Buttons

Apply: Click to apply changes.

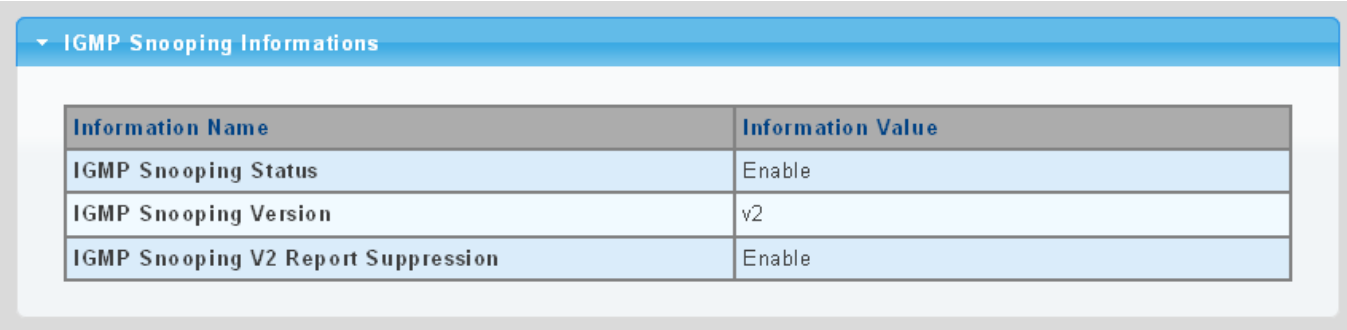


Figure 4-7-8 IGMP Snooping Information Screenshot

The page includes the following fields:

Object	Description
• **IGMP Snooping Status**	Display the current IGMP snooping status.
• **IGMP Snooping Version**	Display the current IGMP snooping version.
• **IGMP Snooping V2 Report Suppression**	Display the current IGMP snooping v2 report suppression.

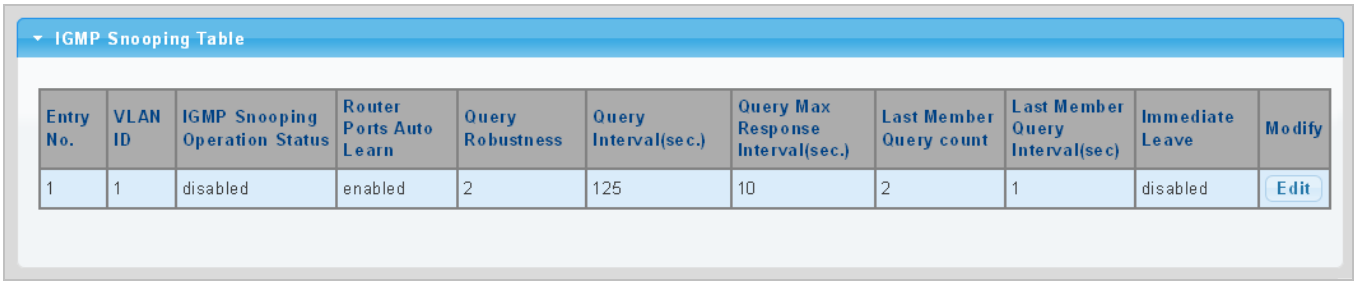


Figure 4-7-9 IGMP Snooping Information Screenshot

The page includes the following fields:

Object	Description
• **Entry No.**	Display the current entry number
• **VLAN ID**	Display the current VLAN ID
• **IGMP Snooping Operation Status**	Display the current IGMP snooping operation status
• **Router Ports Auto Learn**	Display the current router ports auto learning
• **Query Robustness**	Display the current query robustness
• **Query Interval (sec.)**	Display the current query interval
• **Query Max Response Interval (sec.)**	Display the current query max response interval

• **Last Member Query Count**	Display the current last member query count
• **Last Member Query Interval (sec)**	Display the current last member query interval
• **Immediate Leave**	Display the current immediate leave
• **Modify**	Click Edit to edit parameter

4.7.2.2 IGMP Querier Setting

This page provides IGMP Querier Setting. The IGMP Querier Setting screens in Figure 4-7-10 and Figure 4-7-11 appear.

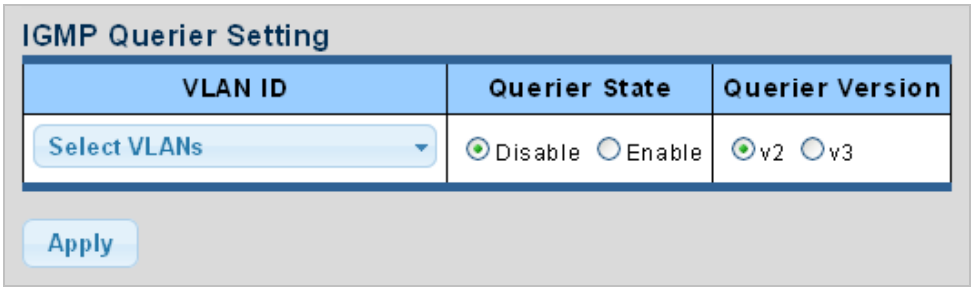


Figure 4-7-10 IGMP VLAN Setting Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Select VLAN ID from this drop-down list.
• **Querier State**	Enable or disable the querier state. The default value is "Disabled".
• **Querier Version**	Sets the querier version for compatibility with other devices on the network. Version: 2 or 3; Default: **2**

Buttons

Apply: Click to apply changes.

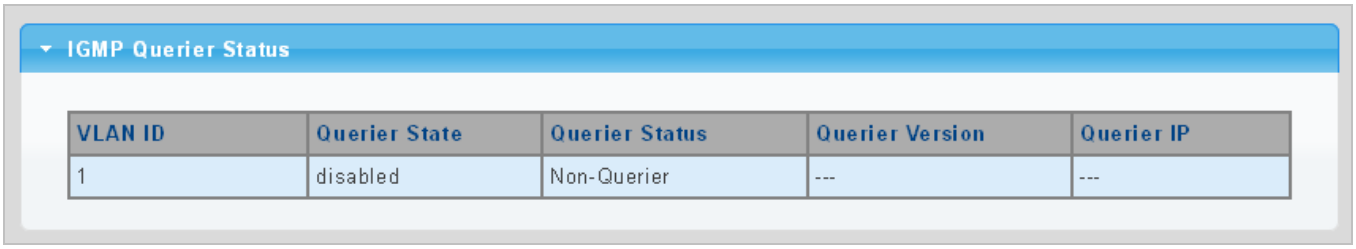


Figure 4-7-11 IGMP Querier Status Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Querier State**	Display the current querier state
• **Querier Status**	Display the current querier status
• **Querier Version**	Display the current querier version
• **Querier IP**	Display the current querier IP

4.7.2.3 IGMP Static Group

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in above sections. For certain applications that require tighter control, you may need to statically configure a multicast service on the Managed Switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

The IGMP Static Group configuration screens in Figure 4-7-12 and Figure 4-7-13 appear.

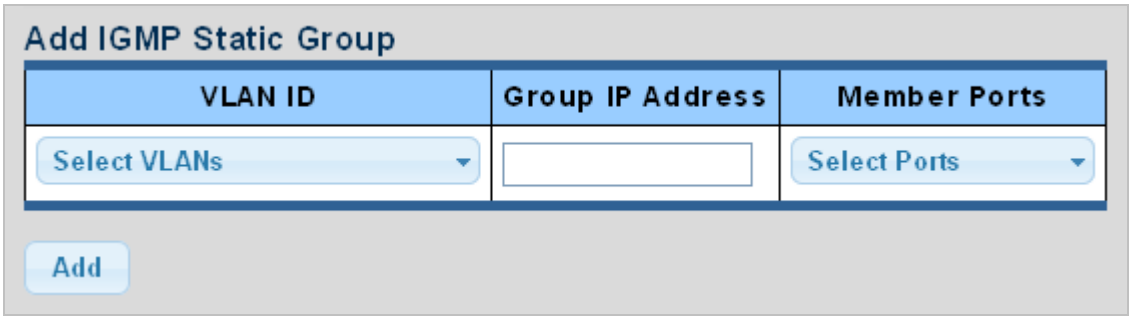


Figure 4-7-12 Add IGMP Static Group Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Select VLAN ID from this drop-down list
• **Group IP Address**	The IP address for a specific multicast service
• **Member Ports**	Select port number from this drop-down list

Buttons

Add: Click to add IGMP router port entry.

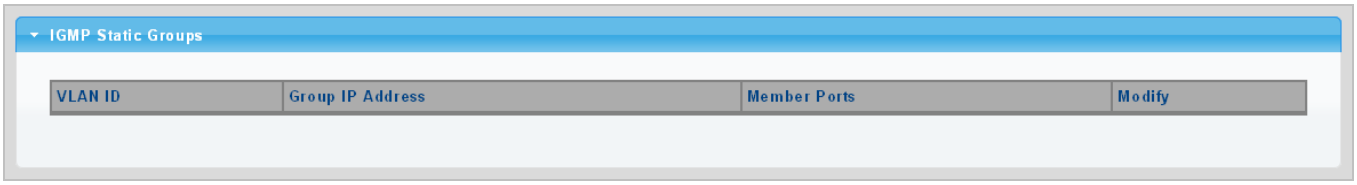


Figure 4-7-13 IGMP Static Groups Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Group IP Address**	Display the current group IP address
• **Member Ports**	Display the current member ports
• **Modify**	Click Edit to edit parameter

4.7.2.4 IGMP Group Table

This page provides Multicast Database. The IGMP Group Table screen in Figure 4-7-14 appears.

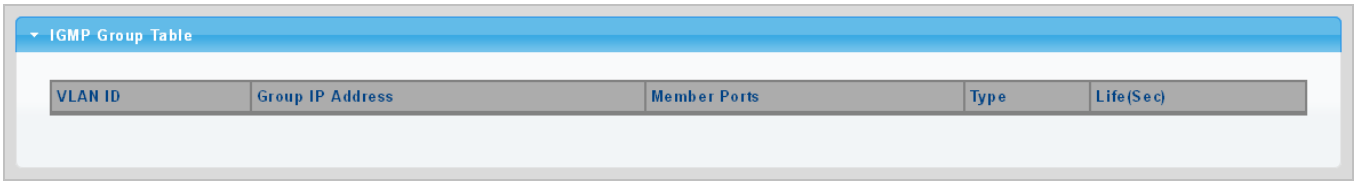


Figure 4-7-14 IGMP Group Table Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VID
• **Group IP Address**	Display multicast IP address for a specific multicast service
• **Member Port**	Display the current member port
• **Type**	Member types displayed include Static or Dynamic, depending on selected options
• **Life(Sec)**	Display the current life

4.7.2.5 IGMP Router Setting

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your Managed Switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the Managed Switch. The IGMP Router Setting and Status screens in Figure 4-7-15 and Figure 4-7-16 appear.

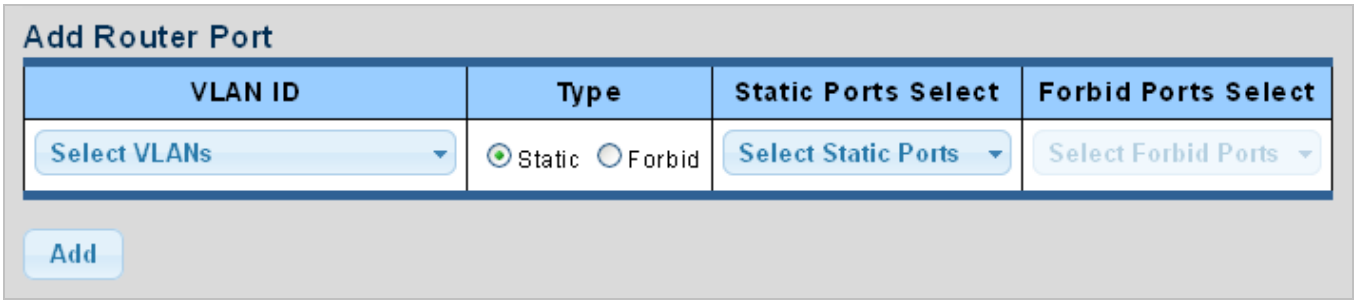


Figure 4-7-15 Add Router Port Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
• **Type**	Sets the Router port type. The types of Router port as below: ■ **Static** ■ **Forbid**
• **Static Ports Select**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
• **Forbid Port Select**	Specify which ports un-act as router ports

Buttons

Add: Click to add IGMP router port entry.

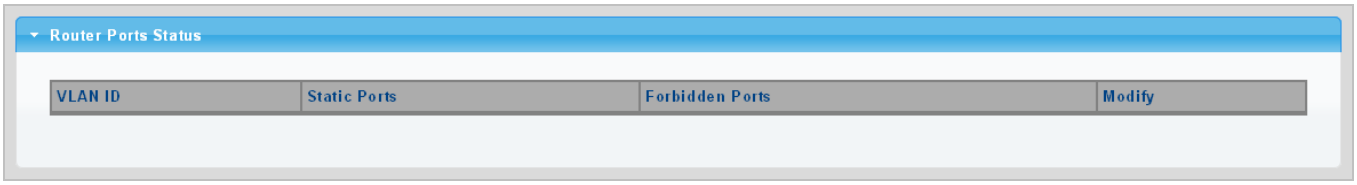


Figure 4-7-16 Router Port Status Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Static Ports**	Display the current static ports
• **Forbidden Ports**	Display the current forbidden ports
• **Modify**	Click Edit to edit parameter Click Delete to delete the group ID entry

4.7.2.6 IGMP Router Table

This page provides Router Table. The Dynamic, Static and Forbidden Router Table screens in Figure 4-7-17, Figure 4-7-18 and Figure 4-7-19 appear.

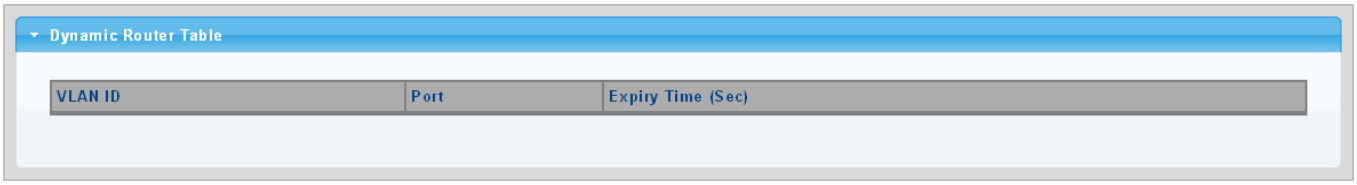


Figure 4-7-17 Dynamic Router Table Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Port**	Display the current dynamic router ports
• **Expiry Time (Sec)**	Display the current expiry time

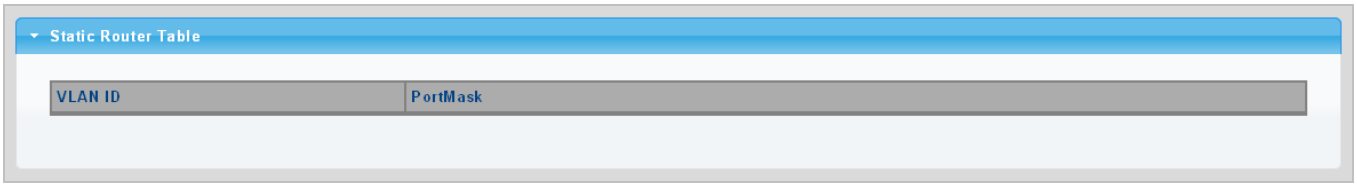


Figure 4-7-18 Static Router Table Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Port Mask**	Display the current port mask

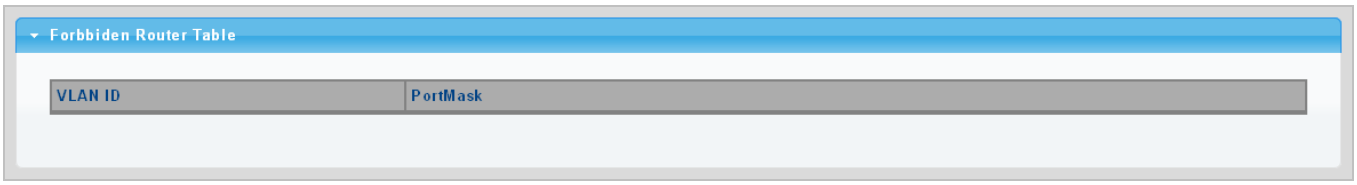


Figure 4-7-19 Forbidden Router Table Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Port Mask**	Display the current port mask

4.7.2.7 IGMP Forward All

This page provides IGMP Forward All. The Forward All screen in Figure 4-7-20 appears.

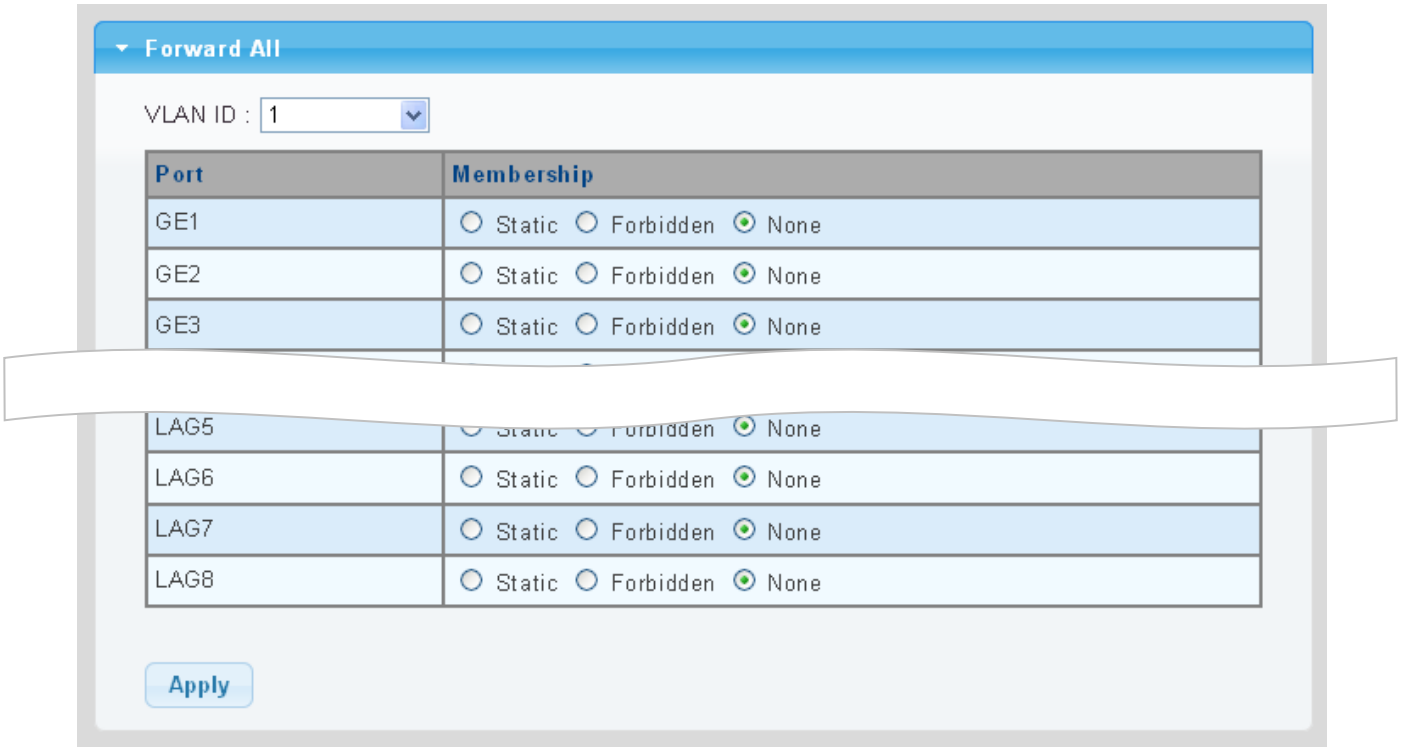


Figure 4-7-20 Forward All Setting Screenshot

The page includes the following fields:

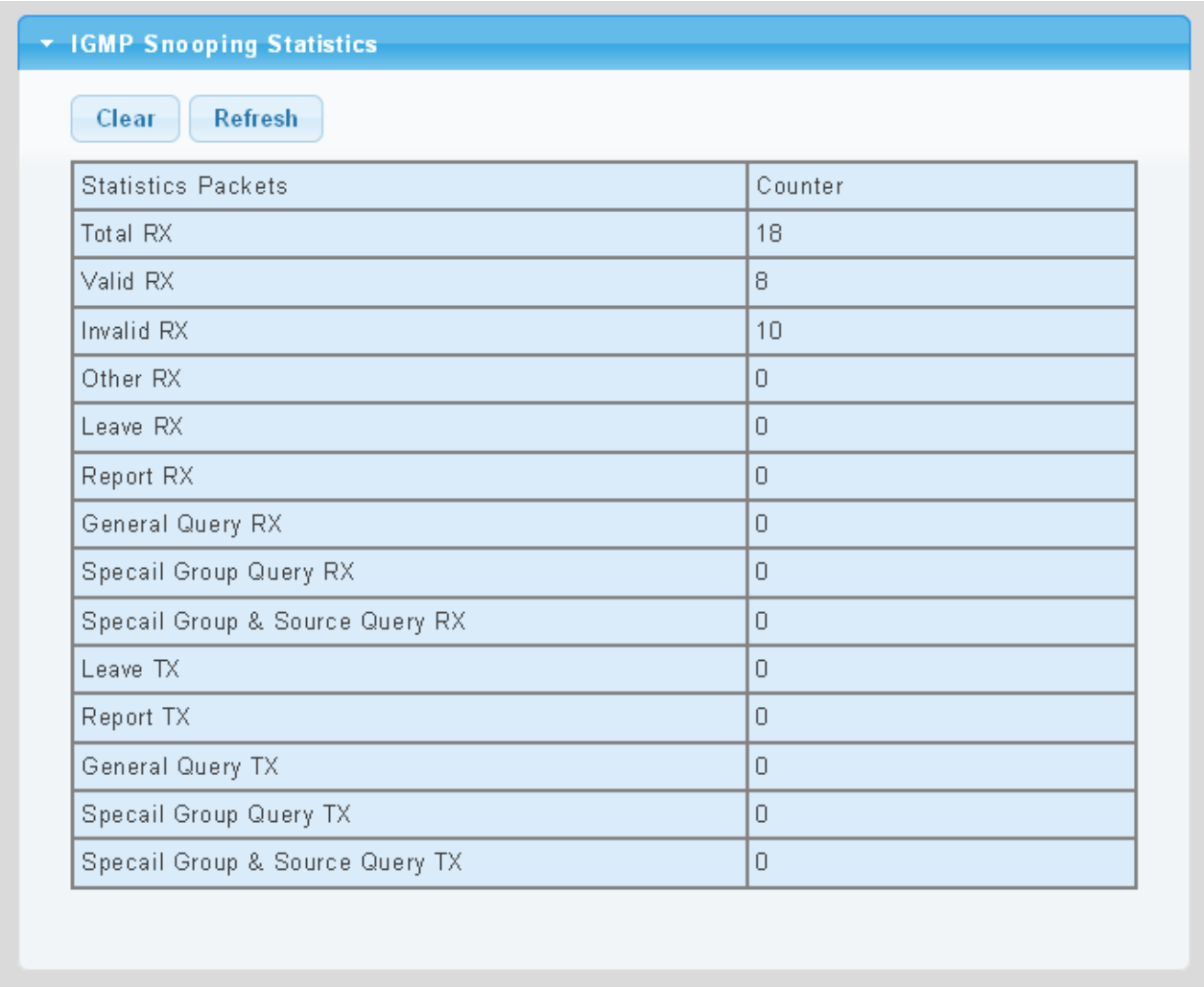
Object	Description	
• **VLAN ID**	Select VLAN ID from this drop-down list to assign IGMP membership	
• **Port**	The switch port number of the logical port	
• **Membership**	Select IGMP membership for each interface:	
	Forbidden:	Interface is forbidden from automatically joining the IGMP via MVR.
	None:	Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
	Static:	Interface is a member of the IGMP.

Buttons

Apply: Click to apply changes.

4.7.3 IGMP Snooping Statics

This page provides IGMP Snooping Statics. The IGMP Snooping Statics screen in Figure 4-7-20 appears.



Statistics Packets	Counter
Total RX	18
Valid RX	8
Invalid RX	10
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Specail Group Query RX	0
Specail Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specail Group Query TX	0
Specail Group & Source Query TX	0

Figure 4-7-20 Forward All Setting Screenshot

The page includes the following fields:

Object	Description
• **Total RX**	Display current total RX
• **Valid RX**	Display current valid RX
• **Invalid RX**	Display current invalid RX
• **Other RX**	Display current other RX
• **Leave RX**	Display current leave RX
• **Report RX**	Display current report RX
• **General Query RX**	Display current general query RX
• **Special Group Query RX**	Display current special group query RX
• **Special Group and Source Query RX**	Display current special group and source query RX

• **Leave TX**	Display current leave TX
• **Report TX**	Display current report TX
• **General Query TX**	Display current general query TX
• **Special Group Query TX**	Display current special group query TX
• **Special Group and Source Query TX**	Display current special group and source query TX

Buttons

Clear: Click to clear the IGMP Snooping Statistics.

Refresh: Click to refresh the IGMP Snooping Statistics.

4.7.4 MLD Snooping

4.7.4.1 MLD Setting

This page provides MLD Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header. The MLD Snooping Setting, Information and Table screens in Figure 4-7-21, Figure 4-7-22 and Figure 4-7-23 appear.

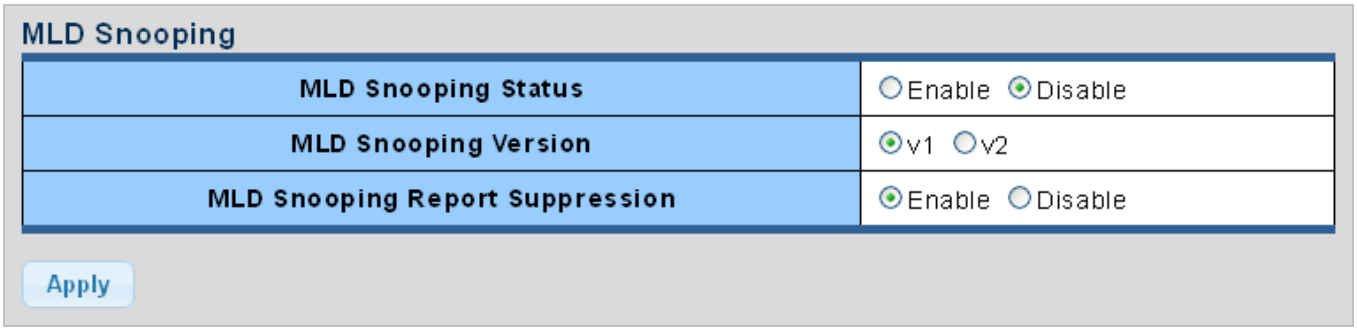


Figure 4-7-21 MLD Snooping Screenshot

The page includes the following fields:

Object	Description
• **MLD Snooping Status**	Enable or disable the MLD snooping. The default value is "Disabled".
• **MLD Snooping Version**	Sets the MLD Snooping operation version. Possible versions are: **v1**: Set MLD Snooping supported MLD version 1. **v2**: Set MLD Snooping supported MLD version 2.
• **MLD Snooping Report Suppression**	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all MLD reports are sent as is to multicast-capable routers. The default is enabled.

Buttons

Apply: Click to apply changes.

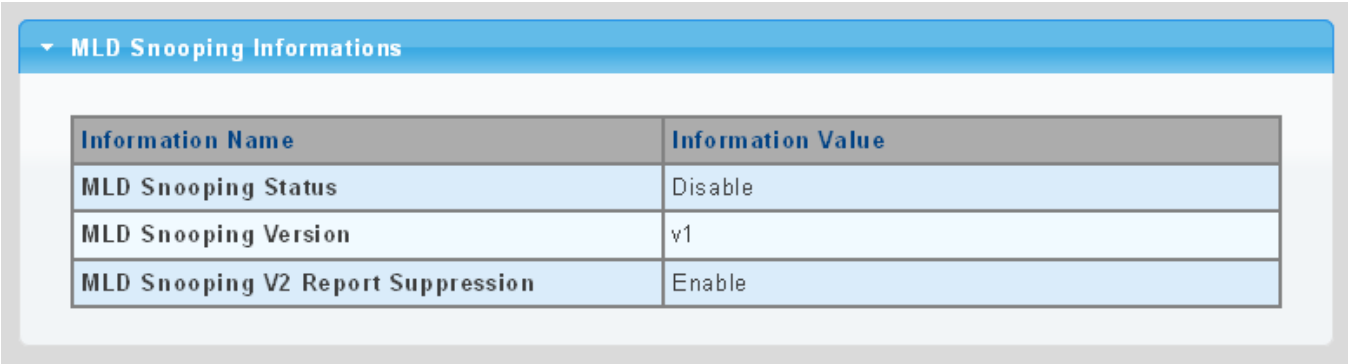


Figure 4-7-22 MLD Snooping information Screenshot

The page includes the following fields:

Object	Description
• **MLD Snooping Status**	Display the current MLD snooping status
• **MLD Snooping Version**	Display the current MLD snooping version
• **MLD Snooping Report Suppression**	Display the current MLD snooping report suppression

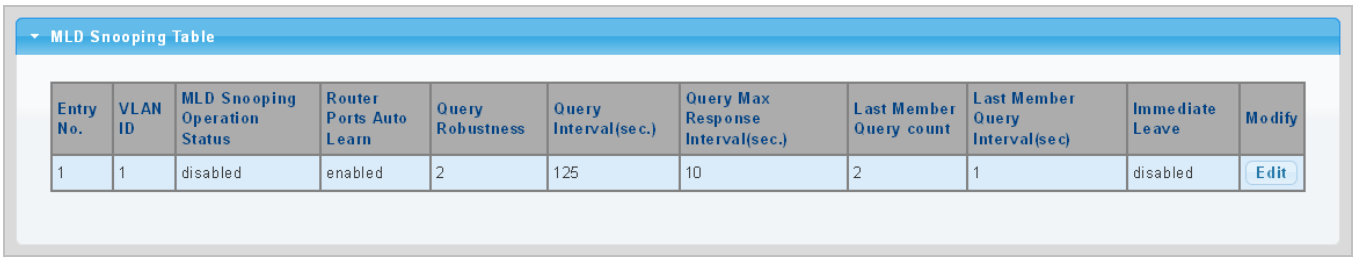


Figure 4-7-23 MLD Snooping Table Screenshot

The page includes the following fields:

Object	Description
• **Entry No.**	Display the current entry number
• **VLAN ID**	Display the current VLAN ID
• **MLD Snooping Operation Status**	Display the current MLD snooping operation status
• **Router Ports Auto Learn**	Display the current router ports auto learning
• **Query Robustness**	Display the current query robustness
• **Query Interval (sec.)**	Display the current query interval
• **Query Max Response Interval (sec.)**	Display the current query max response interval
• **Last Member Query count**	Display the current last member query count
• **Last Member Query Interval (sec)**	Display the current last member query interval
• **Immediate Leave**	Display the current immediate leave
• **Modify**	Click Edit to edit parameter

4.7.4.2 MLD Static Group

The MLD Static Group configuration screens in Figure 4-7-24 and Figure 4-7-25 appear.

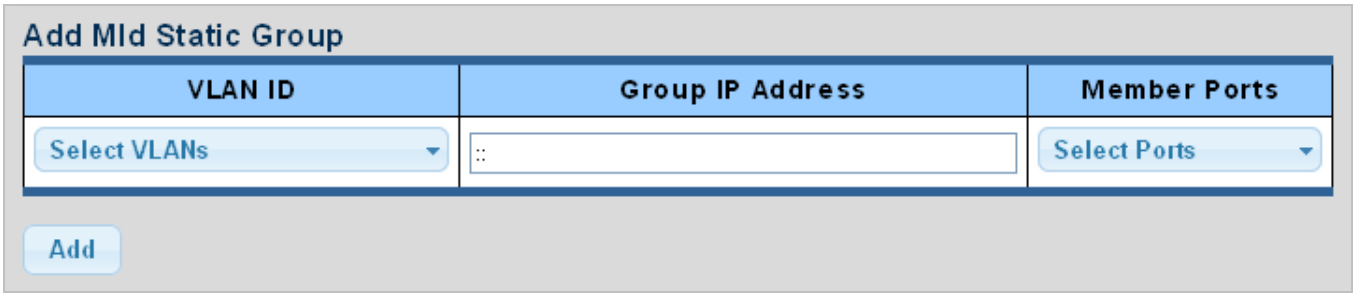


Figure 4-7-24 Add MLD Static Group Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Select VLAN ID from this drop-down list
• **Group IP Address**	The IP address for a specific multicast service
• **Member Ports**	Select port number from this drop-down list

Buttons

Add: Click to add IGMP router port entry.

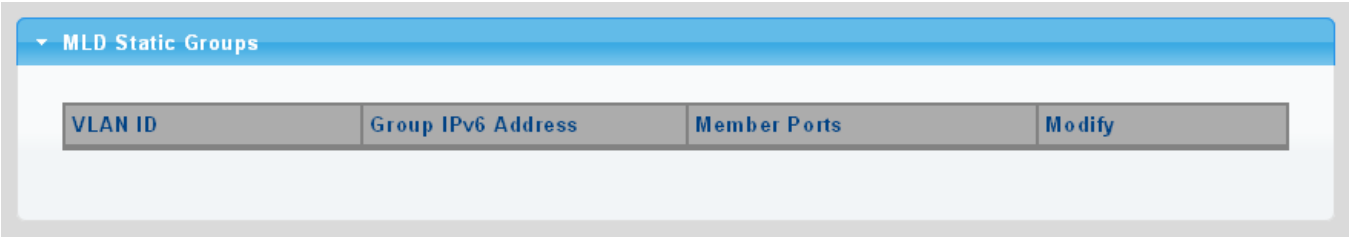


Figure 4-7-25 MLD Static Groups Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Group IPv6 Address**	Display the current group IPv6 address
• **Member Ports**	Display the current member ports
• **Modify**	Click Edit to edit parameter.

4.7.4.3 MLD Group Table

This page provides MLD Group Table. The MLD Group Table screen in Figure 4-7-26 appears.

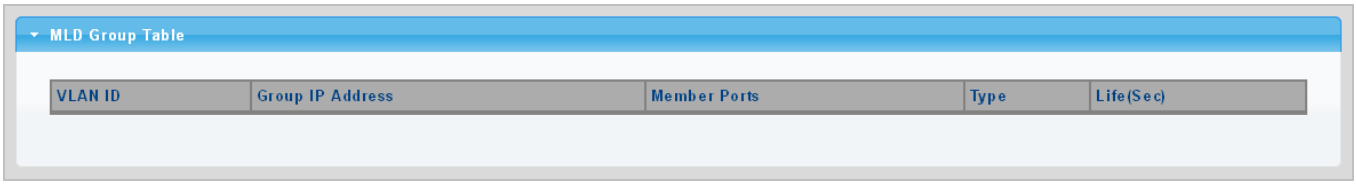


Figure 4-7-26 MLD Group Table Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VID
• **Group IP Address**	Display multicast IP address for a specific multicast service
• **Member Port**	Display the current member port
• **Type**	Member types displayed include Static or Dynamic, depending on selected options
• **Life(Sec)**	Display the current life

4.7.4.4 MLD Router Setting

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your Managed Switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the Managed Switch. The MLD Router Setting screens in Figure 4-7-27 and Figure 4-7-28 appear.

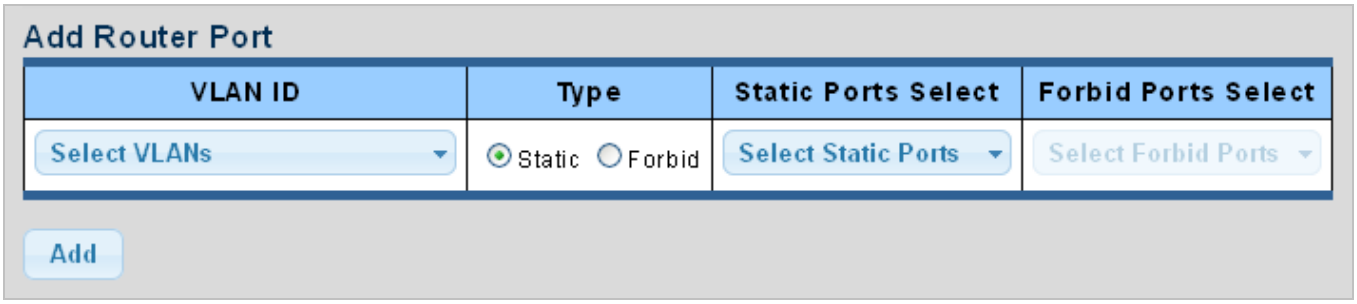


Figure 4-7-27 Add Router Port Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router
• **Type**	Sets the Router port type. The types of Router port as below: **Static** **Forbid**
• **Static Ports Select**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.
• **Forbid Port Select**	Specify which ports un-act as router ports

Buttons

Add: Click to add MLD router port entry.

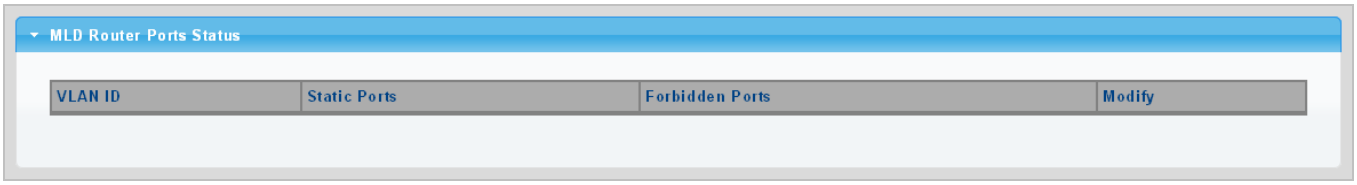


Figure 4-7-28 Router Port Status Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Static Ports**	Display the current static ports
• **Forbidden Ports**	Display the current forbidden ports
• **Modify**	Click Edit to edit parameter Click Delete to delete the group ID entry

4.7.4.5 MLD Router Table

This page provides Router Table. The Dynamic, Static and Forbidden Router Table screens in Figure 4-7-29, Figure 4-7-30 and Figure 4-7-31 appear.

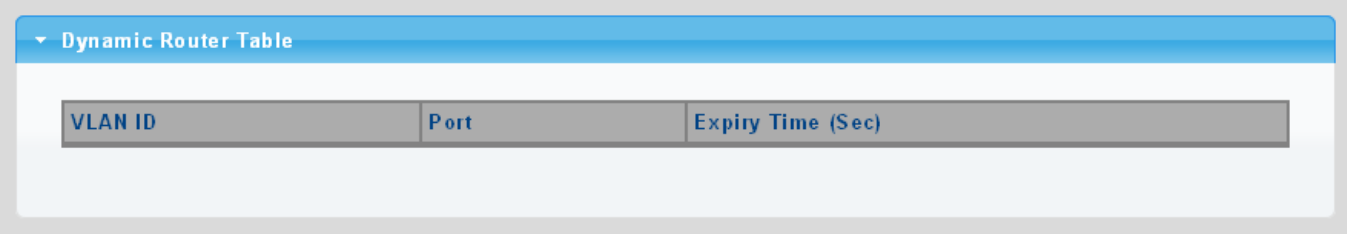


Figure 4-7-29 Dynamic Router Table Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Port**	Display the current dynamic router ports
• **Expiry Time (Sec)**	Display the current expiry time

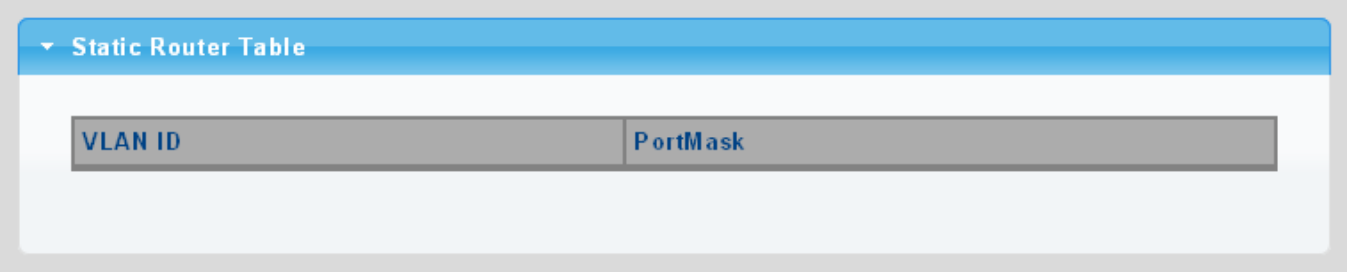


Figure 4-7-30 Static Router Table Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Port Mask**	Display the current port mask

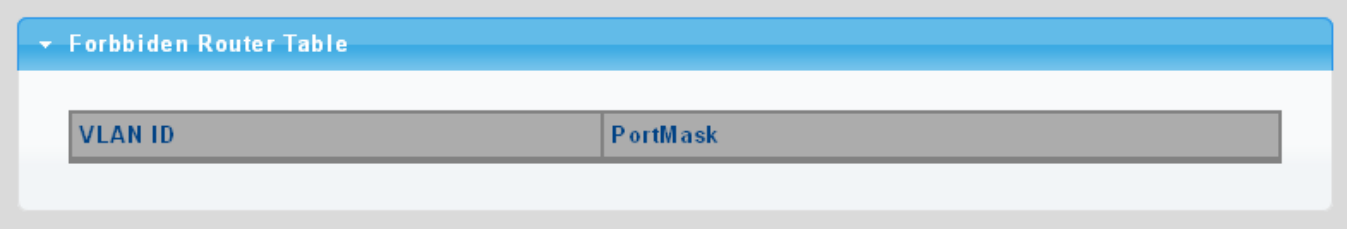


Figure 4-7-31 Forbidden Router Table Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Port Mask**	Display the current port mask

4.7.4.6 MLD Forward All

This page provides MLD Forward All. The Forward All screen in Figure 4-7-32 appears.

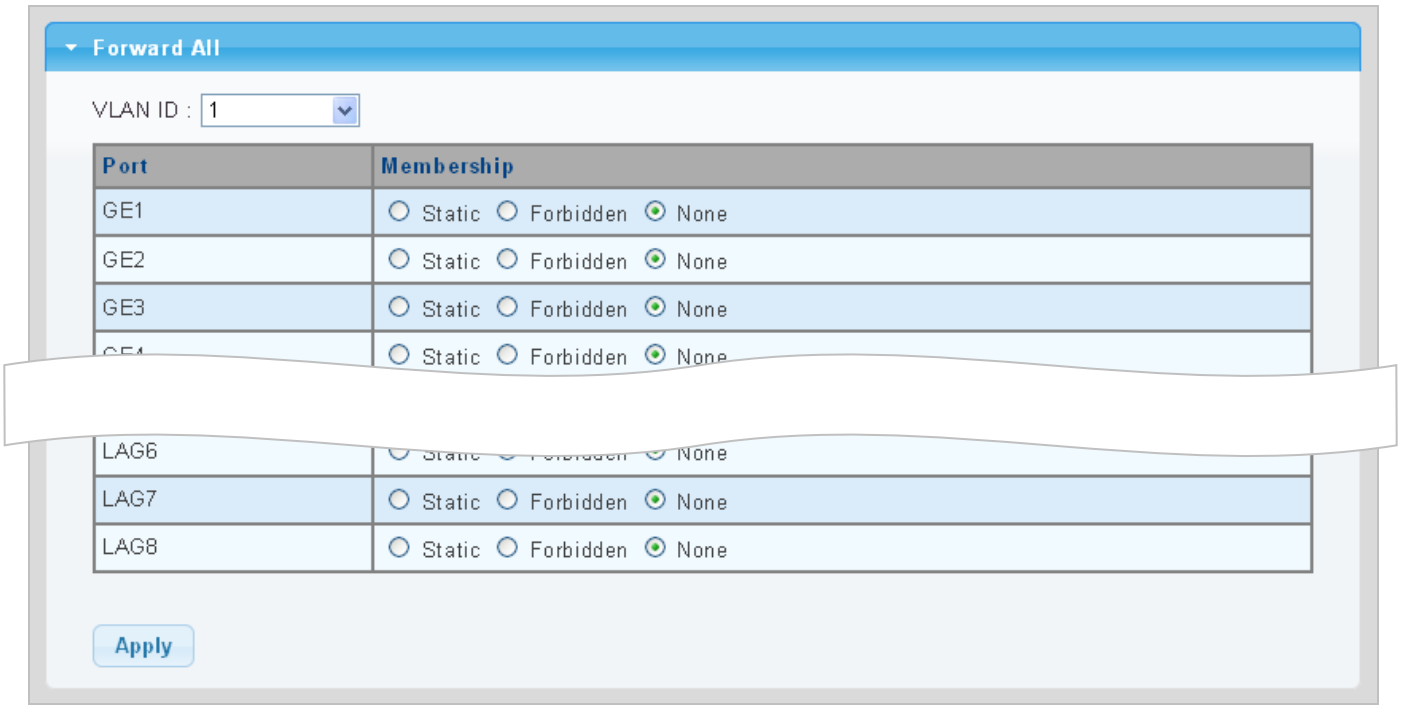


Figure 4-7-32 Forward All Setting Screenshot

The page includes the following fields:

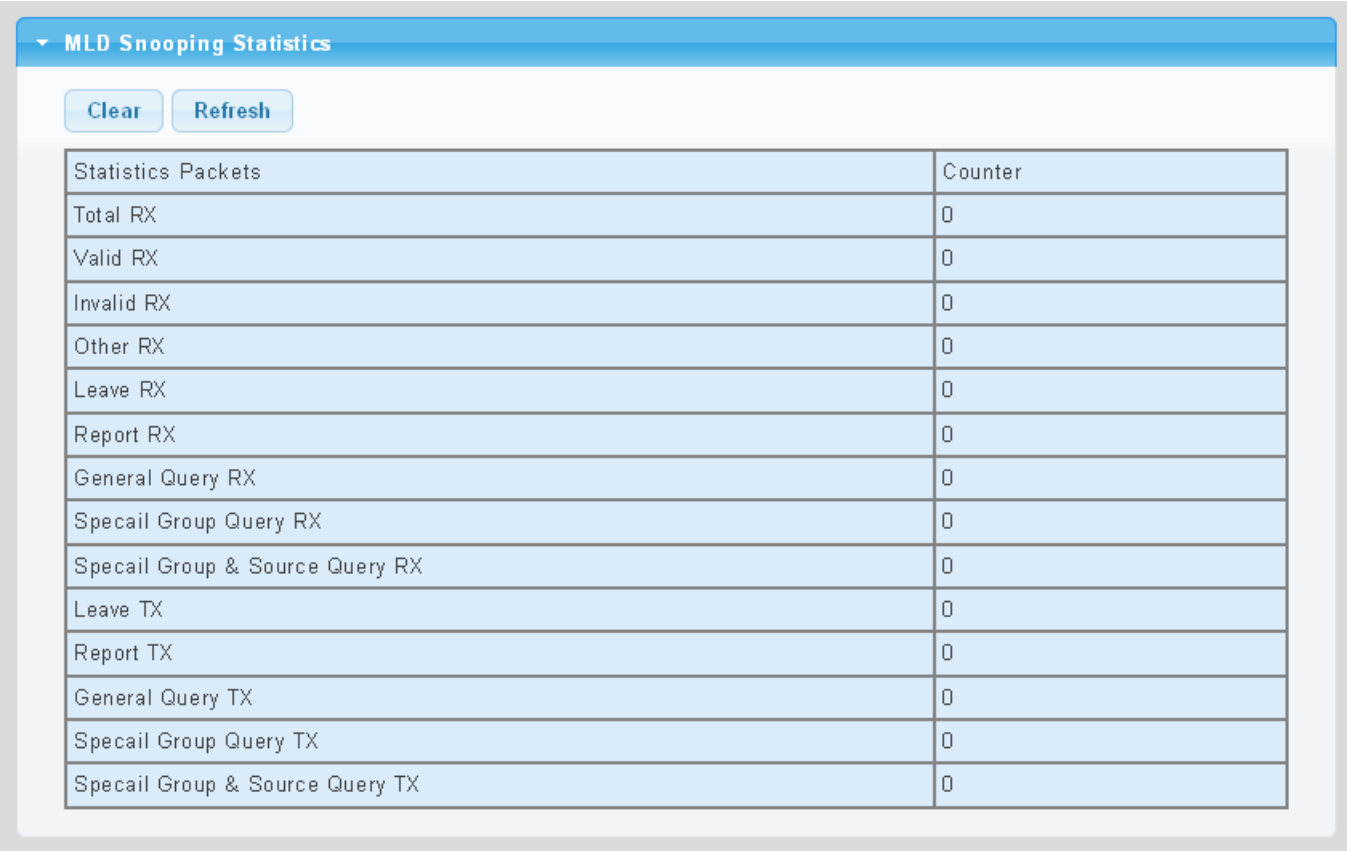
Object	Description	
• **VLAN ID**	Select VLAN ID from this drop-down list to assign MLD membership	
• **Port**	The switch port number of the logical port	
• **Membership**	Select MLD membership for each interface:	
	Forbidden:	Interface is forbidden from automatically joining the MLD via MVR.
	None:	Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
	Static:	Interface is a member of the MLD.

Buttons

Apply: Click to apply changes.

4.7.5 MLD Snooping Statics

This page provides MLD Snooping Statics. The MLD Snooping Statics screen in Figure 4-7-33 appears.



Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Specail Group Query RX	0
Specail Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specail Group Query TX	0
Specail Group & Source Query TX	0

Figure 4-7-33 Forward All Setting Screenshot

The page includes the following fields:

Object	Description
• **Total RX**	Display current total RX
• **Valid RX**	Display current valid RX
• **Invalid RX**	Display current invalid RX
• **Other RX**	Display current other RX
• **Leave RX**	Display current leave RX
• **Report RX**	Display current report RX
• **General Query RX**	Display current general query RX

• **Special Group Query RX**	Display current special group query RX
• **Special Group and Source Query RX**	Display current special group and source query RX
• **Leave TX**	Display current leave TX
• **Report TX**	Display current report TX
• **General Query TX**	Display current general query TX
• **Special Group Query TX**	Display current special group query TX
• **Special Group and Source Query TX**	Display current special group and source query TX

Buttons

Clear: Click to clear the MLD Snooping Statistics.

Refresh: Click to refresh the MLD Snooping Statistics.

4.7.6 Multicast Throttling Setting

Multicast throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace". If the action is set to deny, any new multicast join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Once you have configured multicast profiles, you can assign them to interfaces on the Managed Switch. Also you can set the multicast throttling number to limit the number of multicast groups an interface can join at the same time. The MAX Group and Information screens in Figure 4-7-34 and Figure 4-7-35 appear.

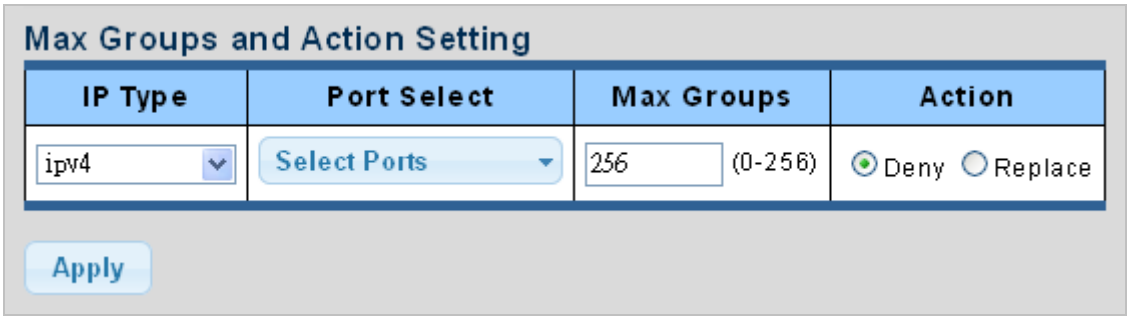


Figure 4-7-34 Max Groups and Action Setting Screenshot

The page includes the following fields:

Object	Description
• **IP Type**	Select IPv4 or IPv6 from this drop-down list
• **Port Select**	Select port number from this drop-down list
• **Max Groups**	Sets the maximum number of multicast groups an interface can join at the same time. Range: 0-256; Default: **256**
• **Action**	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

Buttons

Apply: Click to apply changes.

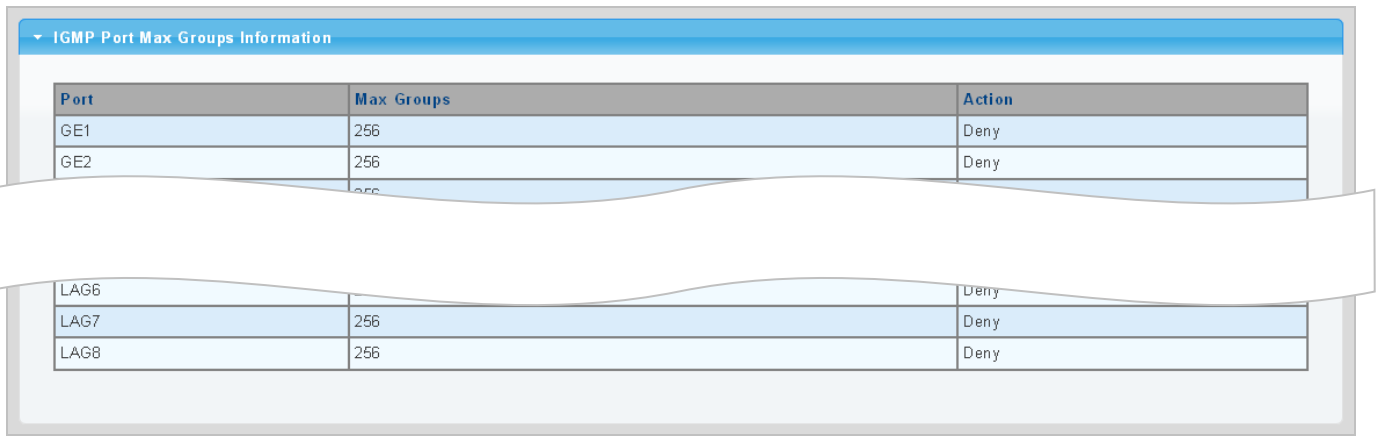


Figure 4-7-35 IGMP Port Max Groups Information Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Max Groups**	Display the current Max groups
• **Action**	Display the current action

4.7.7 Multicast Filter

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service is based on a specific subscription plan. The multicast filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port.

Multicast filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A multicast filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, multicast join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the multicast join report is forwarded as normal. If a requested multicast group is denied, the multicast join report is dropped.

When you have created a Multicast profile number, you can then configure the multicast groups to filter and set the access mode.

Command Usage

- Each profile has only one access mode; either **permit** or **deny**.
- When the access mode is set to **permit**, multicast join reports are processed when a multicast group falls within the controlled range.
- When the access mode is set to **deny**, multicast join reports are only processed when the multicast group is not in the controlled range.

4.7.7.1 Multicast Profile Setting

The Add Profile and Profile Status screens in Figure 4-7-36 and Figure 4-7-37 appear.

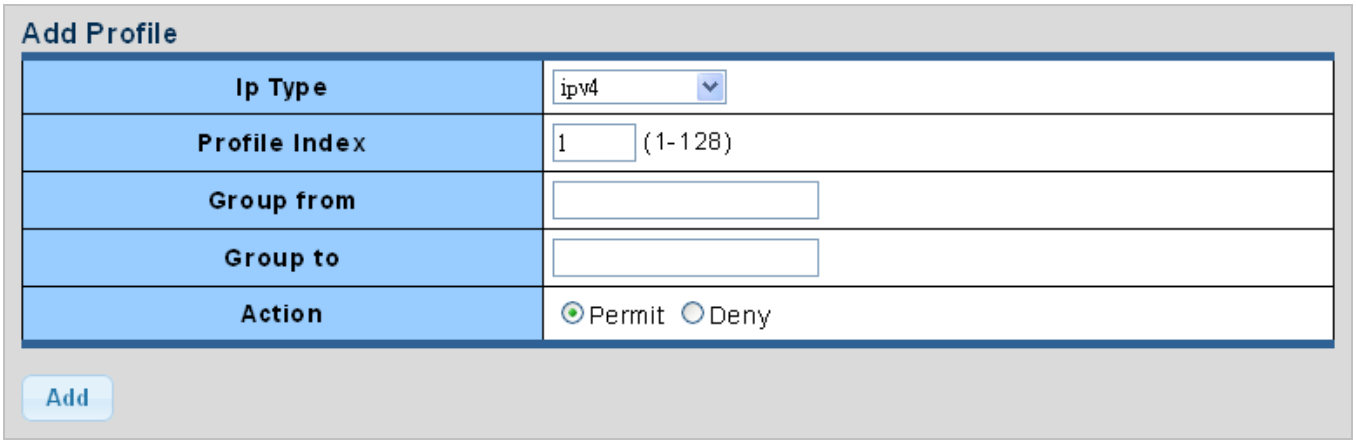


Figure 4-7-36 Add Profile Setting Screenshot

The page includes the following fields:

Object	Description	
• **IP Type**	Select IPv4 or IPv6 from this drop-down list	
• **Profile Index**	Indicates the ID of this particular profile	
• **Group from**	Specifies multicast groups to include in the profile. Specify a multicast group range by entering a start IP address.	
• **Group to**	Specifies multicast groups to include in the profile. Specify a multicast group range by entering an end IP address.	
• **Action**	Sets the access mode of the profile; either **permit** or **deny**.	
	- Permit	Multicast join reports are processed when a multicast group falls within the controlled range.
	- Deny	When the access mode is set to, multicast join reports are only processed when the multicast group is not in the controlled range.

Buttons

: Click to add multicast profile entry.

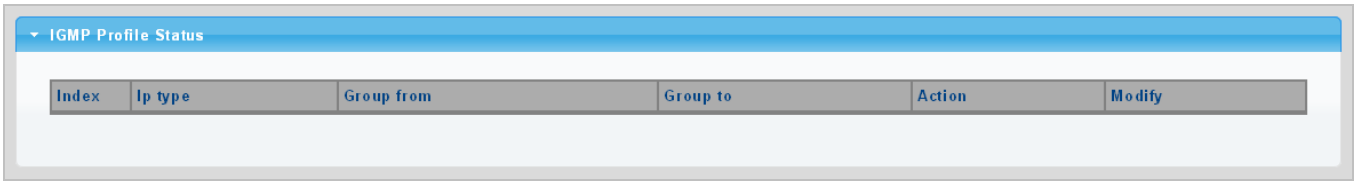


Figure 4-7-37 IGMP/MLD Profile Status Screenshot

The page includes the following fields:

Object	Description
• **Index**	Display the current index
• **IP Type**	Display the current IP Type
• **Group from**	Display the current group from
• **Group to**	Display the current group to
• **Action**	Display the current action
• **Modify**	Click Edit to edit parameter. Click Delete to delete the MLD/IGMP profile entry.

4.7.7.2 IGMP Filter Setting

The Filter Setting and Status screens in Figure 4-7-38 and Figure 4-7-39 appear.

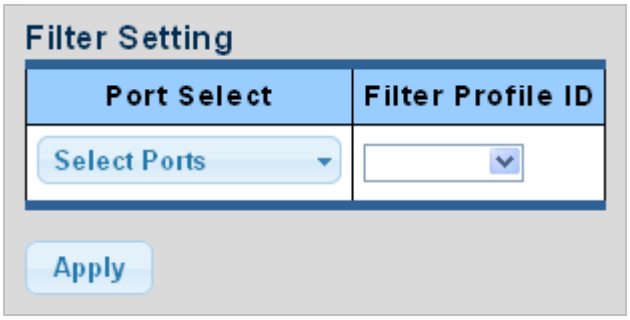


Figure 4-7-38 Filter Setting Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number from this drop-down list
• **Filter Profile ID**	Select filter profile ID from this drop-down list

Buttons

Apply: Click to apply changes.

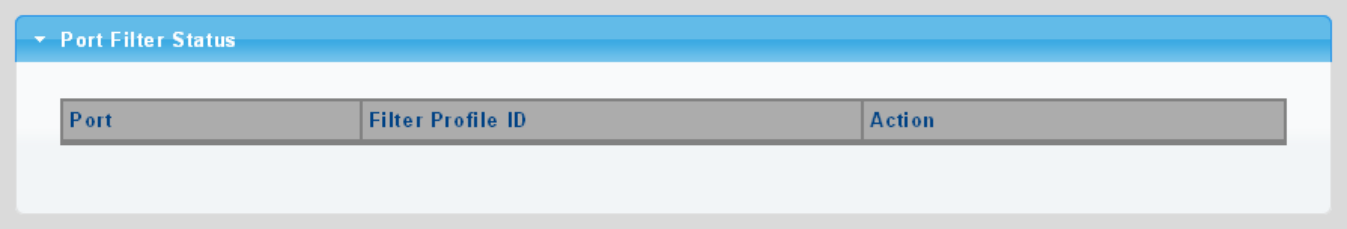


Figure 4-7-39 Port Filter Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	Display the current port
• **Filter Profile ID**	Display the current filter profile ID
• **Action**	Click Show to display detail profile parameter Click Delete to delete the IGMP filter profile entry

4.7.7.3 MLD Filter Setting

The Filter Setting and Status screens in Figure 4-7-40 and Figure 4-7-41 appear.

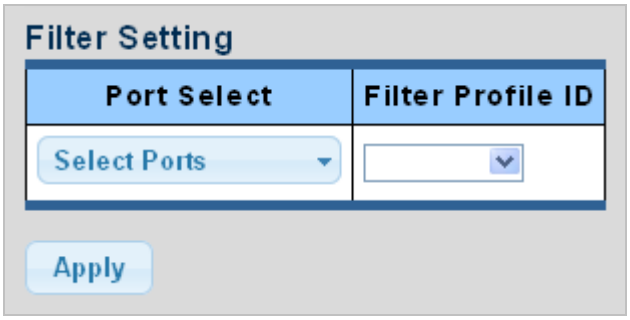


Figure 4-7-40 Filter Setting Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number from this drop-down list
• **Filter Profile ID**	Select filter profile ID from this drop-down list

Buttons

Apply: Click to apply changes.

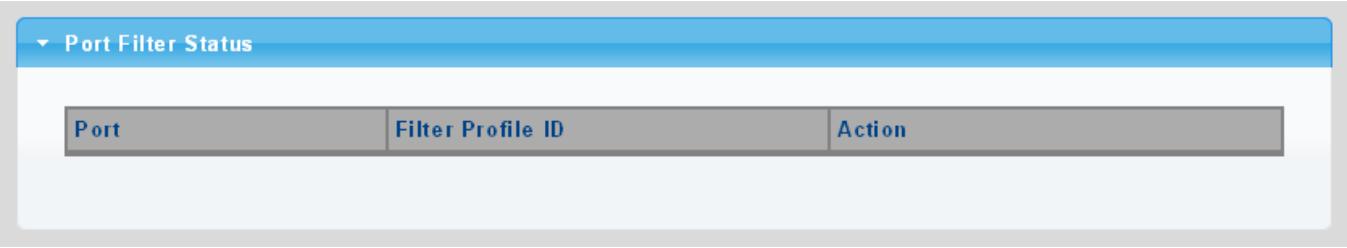


Figure 4-7-41 Port Filter Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	Display the current port
• **Filter Profile ID**	Display the current filter profile ID
• **Action**	Click Show to display detail profile parameter Click Delete to delete the MLD filter profile entry

4.8 Quality of Service

4.8.1 Understanding QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

To implement QoS on your network, you need to carry out the following actions:

1. Define a service level to determine the priority that will be applied to traffic.

2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.

3. Create a QoS profile which associates a service level and a classifier.

4. Apply a QoS profile to a port(s).

The **QoS** page of the Managed Switch contains three types of QoS mode - the **802.1p** mode, **DSCP** mode or **Port-base** mode can be selected. Both the three mode rely on predefined fields within the packet to determine the output queue.

- **802.1p Tag Priority** Mode –The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- **IP DSCP** Mode - The output queue assignment is determined by the TOS or DSCP field in the IP packets.
- **Port-Base Priority** Mode – Any packet received from the specify high priority port will treated as a high priority packet.

The Managed Switch supports **eight priority level** queue, the queue service rate is based on the **WRR**(**Weight Round Robin**) and **WFQ (Weighted Fair Queuing)** alorithm. The WRR ratio of high-priority and low-priority can be set to "**4:1** and **8:1.**

4.8.2 General

4.8.2.1 QoS Properties

The QoS Global Setting and Information screen in Figure 4-8-1 and Figure 4-8-2 appear.

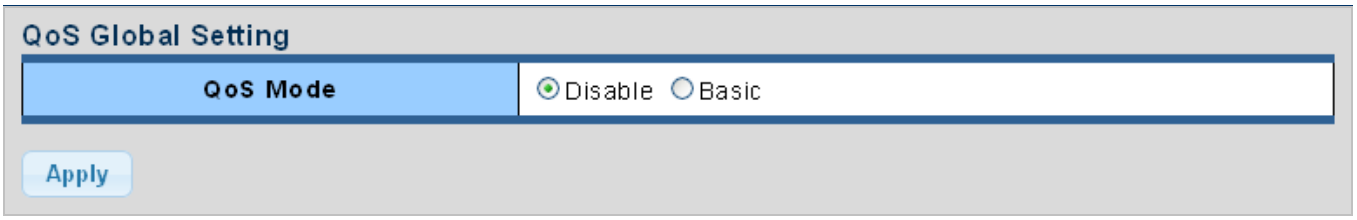


Figure 4-8-1 QoS Global Setting Screenshot

The page includes the following fields:

Object	Description
• **QoS Mode**	Enable or disable QoS mode

Buttons

Apply: Click to apply changes.

■ **QoS Information**

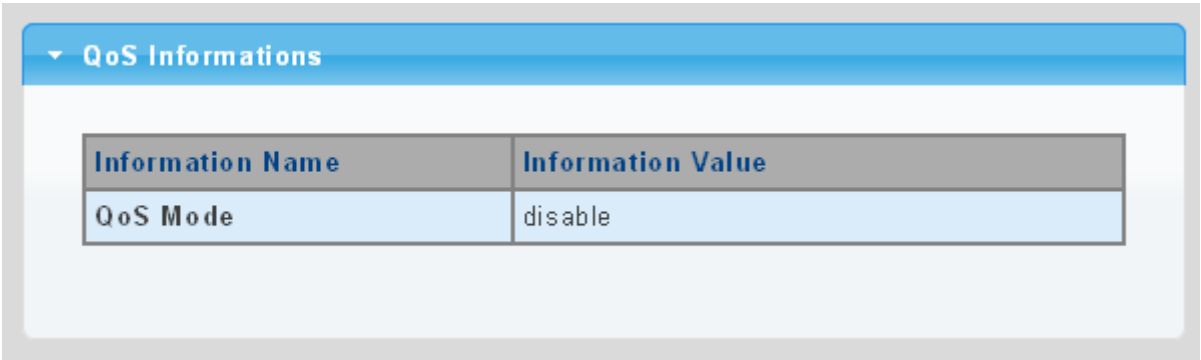


Figure 4-8-2 QoS Information Screenshot

The page includes the following fields:

Object	Description
• **QoS Mode**	Display the current QoS mode

4.8.2.2 QoS Port Settings

The QoS Port Settings and Status screen in Figure 4-8-2 and Figure 4-8-3 appear.

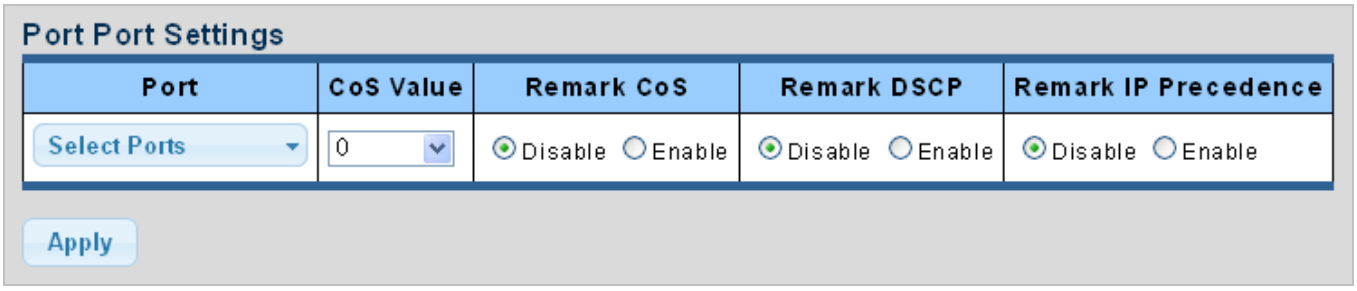


Figure 4-8-2 QoS Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number from this drop-down list
• **CoS Value**	Select CoS value from this drop-down list
• **Remark CoS**	Disable or enable remark CoS
• **Remark DSCP**	Disable or enable remark DSCP
• **Remark IP Precedence**	Disable or enable remark IP Precedence

Buttons

Apply: Click to apply changes.

■ **QoS Port Status**

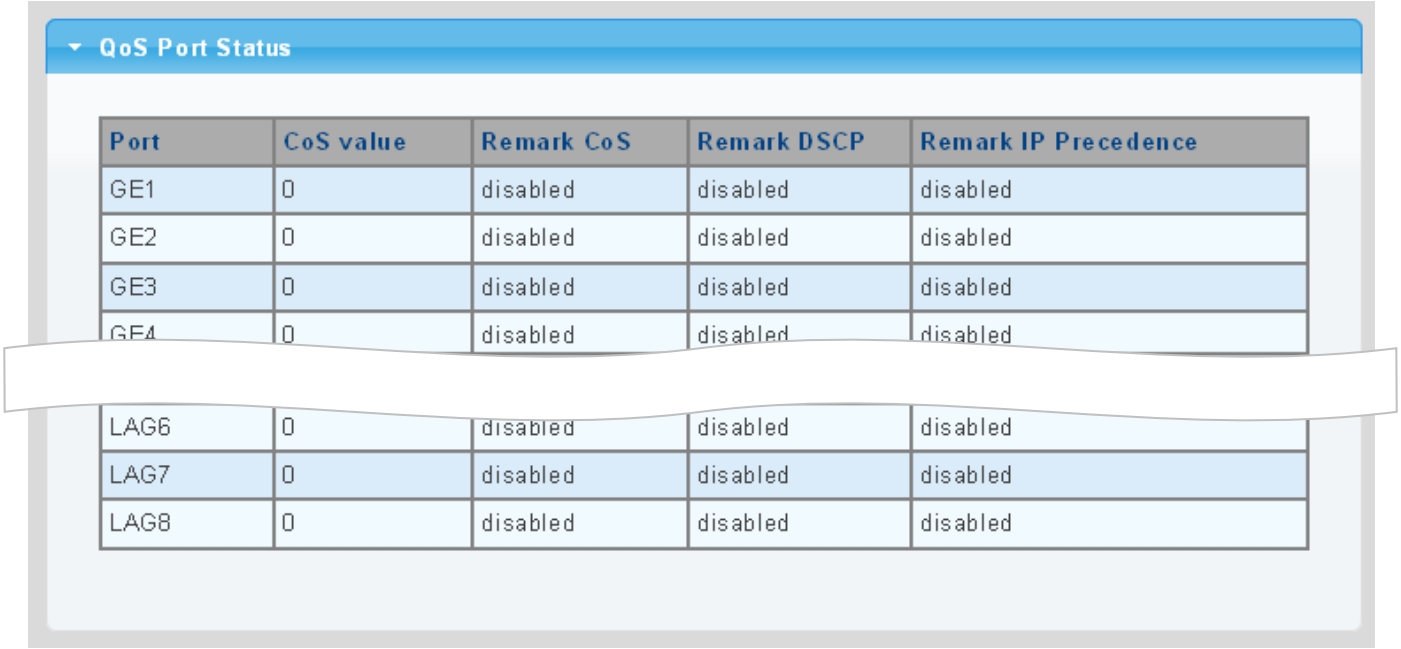


Figure 4-8-3 QoS Port Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **CoS Value**	Display the current CoS value
• **Remark CoS**	Display the current remark CoS
• **Remark DSCP**	Display the current remark DSCP
• **Remark IP Precedence**	Display the current remark IP precedence

4.8.2.3 Queue Settings

The Queue Table and Information screens in Figure 4-8-4 and Figure 4-8-5 appear.

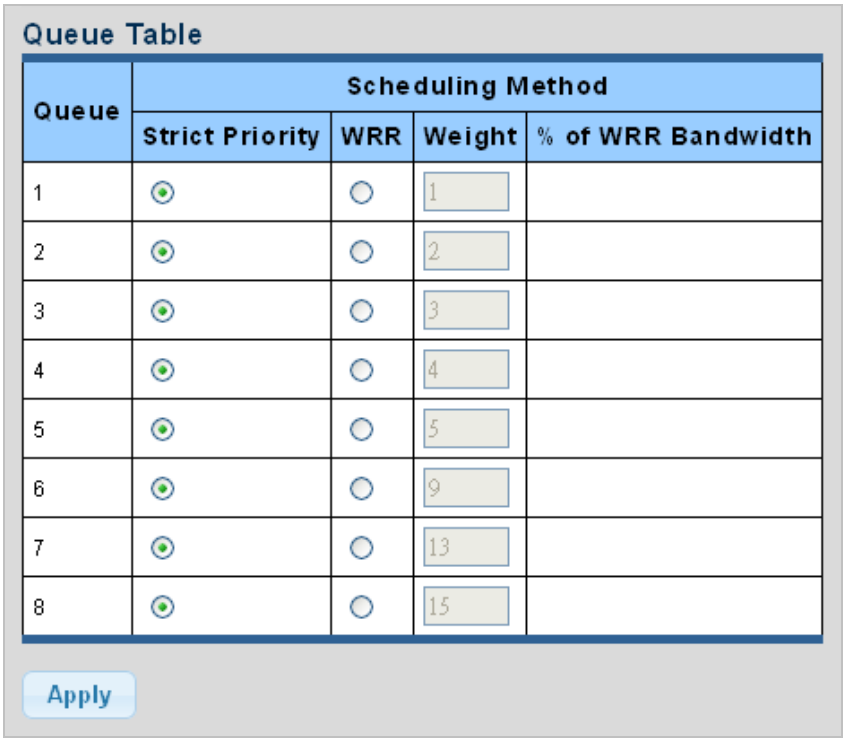


Figure 4-8-4 Queue Table Screenshot

The page includes the following fields:

Object	Description
• **Queue**	Display the current queue ID
• **Strict Priority**	Controls whether the scheduler mode is "Strict Priority" on this switch port
• **WRR**	Controls whether the scheduler mode is "Weighted" on this switch port
• **Weight**	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
• **% of WRR Bandwidth**	Display the current bandwidth for each queue

Buttons

Apply: Click to apply changes.

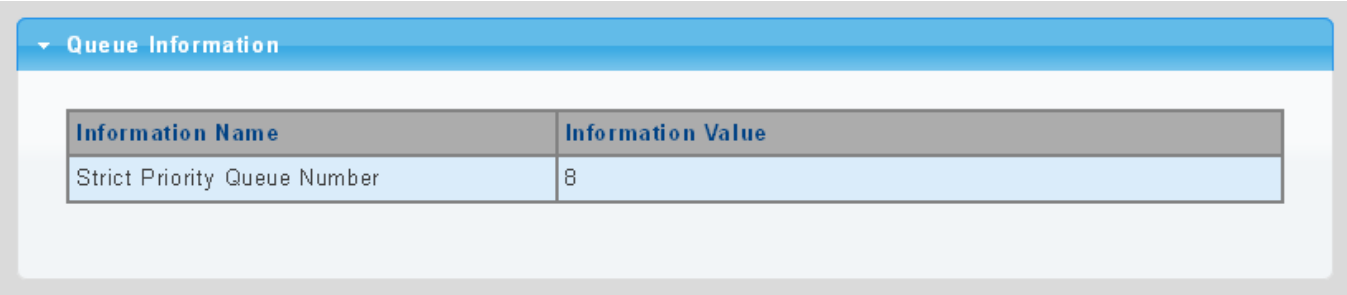


Figure 4-8-5 Queue Information Screenshot

The page includes the following fields:

Object	Description
• **Information Name**	Display the current queue method information
• **Information Value**	Display the current queue value information

4.8.2.4 CoS Mapping

The CoS to Queue and Queue to CoS Mapping screens in Figure 4-8-6 and Figure 4-8-7 appear.

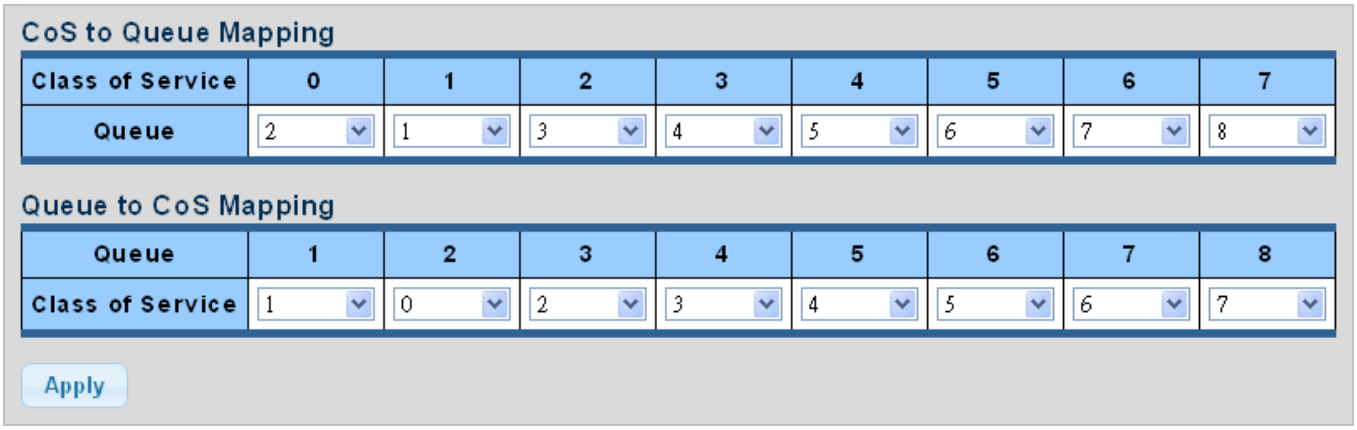


Figure 4-8-6 CoS to Queue and Queue to CoS Mapping Screenshot

The page includes the following fields:

Object	Description
• **Queue**	Select Queue value from this drop-down list
• **Class of Service**	Select CoS value from this drop-down list

Buttons

Apply: Click to apply changes.

CoS Mapping

CoS mapping

CoS	Mapping to Queue
0	2
1	1
2	3
3	4
4	5
5	6
6	7
7	8

Queue	Mapping to CoS
1	1
2	0
3	2
4	3
5	4
6	5
7	6
8	7

Figure 4-8-7 CoS Mapping Screenshot

The page includes the following fields:

Object	Description
• **CoS**	Display the current CoS value
• **Mapping to Queue**	Display the current mapping to queue
• **Queue**	Display the current queue value
• **Mapping to CoS**	Display the current mapping to CoS

4.8.2.5 DSCP Mapping

The DSCP to Queue and Queue to DSCP Mapping screens in Figure 4-8-8 and Figure 4-8-9 appear.

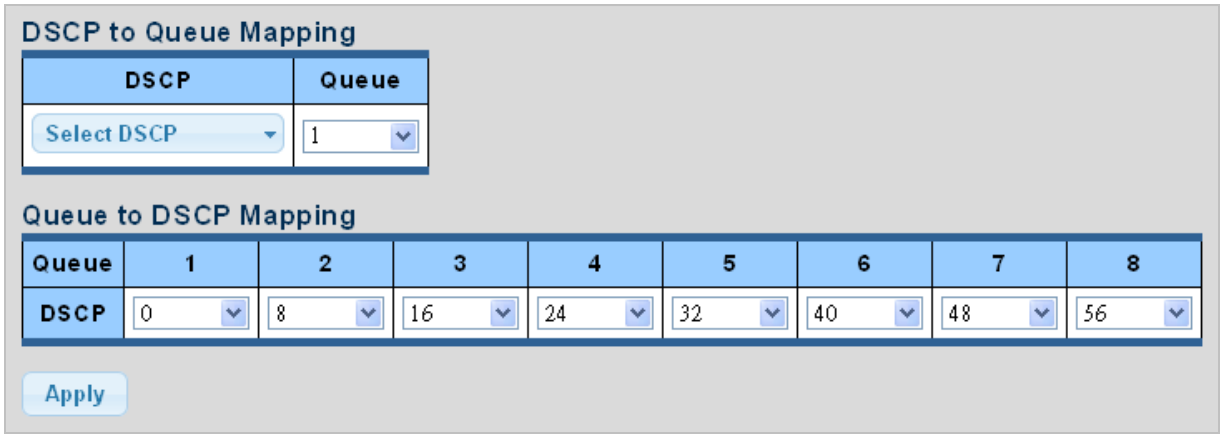


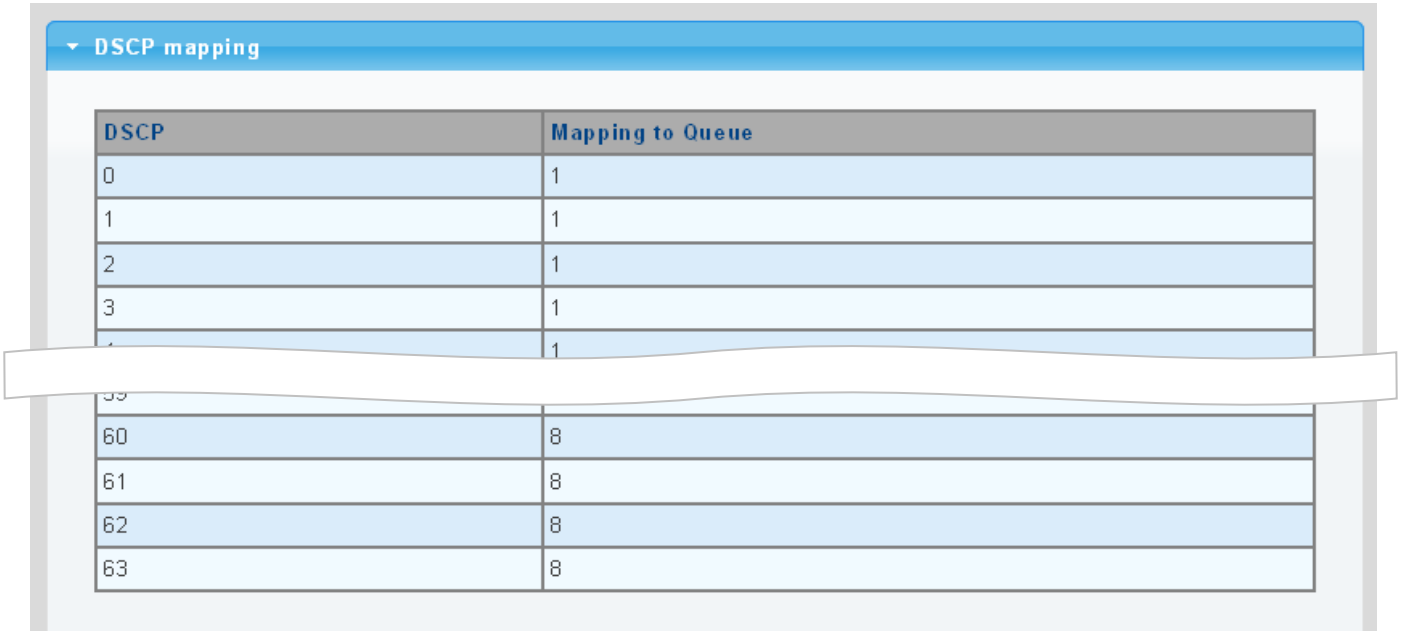
Figure 4-8-8 DSCP to Queue and Queue to DSCP Mapping Screenshot

The page includes the following fields:

Object	Description
• **Queue**	Select Queue value from this drop-down list
• **DSCP**	Select DSCP value from this drop-down list

Buttons

Apply: Click to apply changes.



Queue	Mapping to DSCP
1	0
2	8
3	16
4	24
5	32
6	40
7	48
8	56

Figure 4-8-9 DSCP Mapping Screenshot

The page includes the following fields:

Object	Description
• **DSCP**	Display the current CoS value
• **Mapping to Queue**	Display the current mapping to queue
• **Queue**	Display the current queue value
• **Mapping to DSCP**	Display the current mapping to DSCP

4.8.2.6 IP Precedence Mapping

The IP Precedence to Queue and Queue to IP Precedence Mapping screens in Figure 4-8-10 and Figure 4-8-11 appear.

IP Precedence to Queue Mapping

IP Precedence	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Queue to IP Precedence Mapping

Queue	1	2	3	4	5	6	7	8
IP Precedence	0	1	2	3	4	5	6	7

Apply

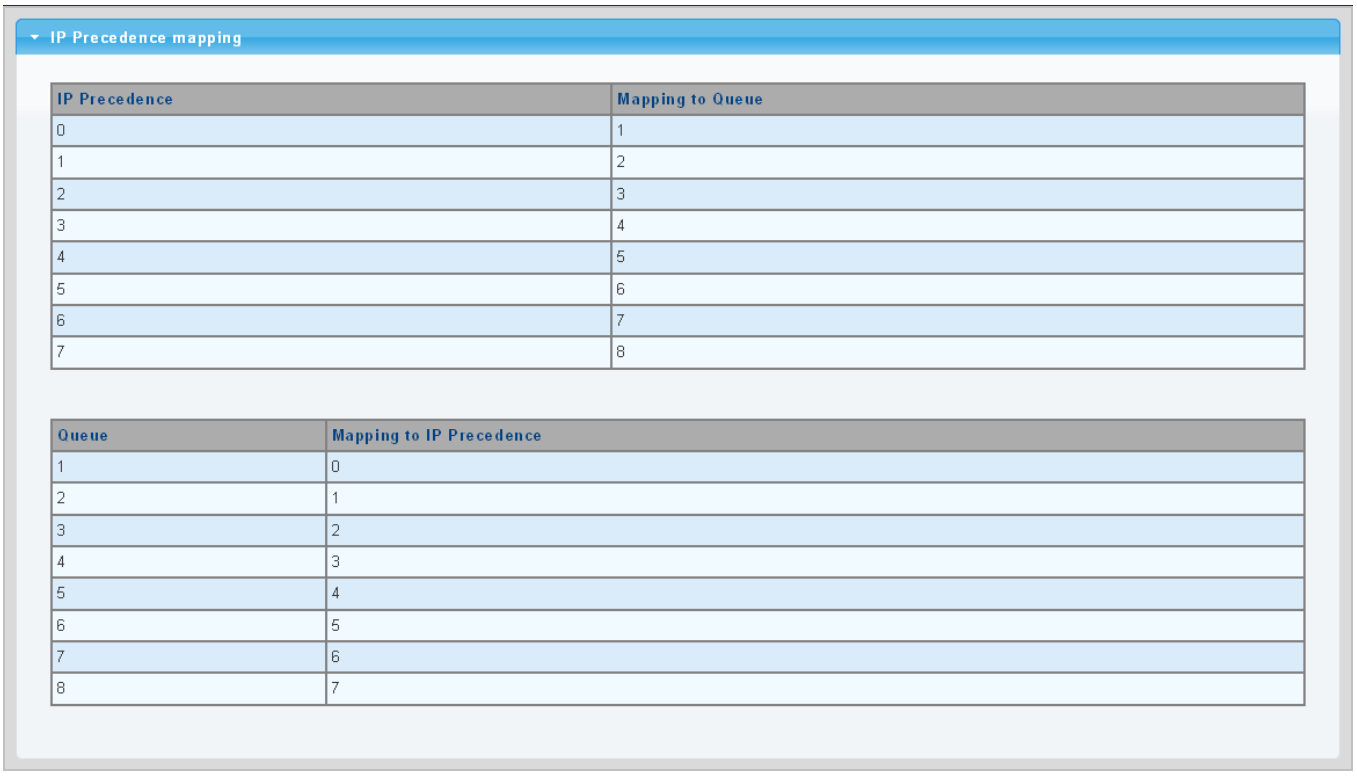
Figure 4-8-10 IP Precedence to Queue and Queue to IP Precedence Mapping Screenshot

The page includes the following fields:

Object	Description
• **Queue**	Select Queue value from this drop-down list
• **IP Precedence**	Select IP Precedence value from this drop-down list

Buttons

Apply: Click to apply changes.



IP Precedence	Mapping to Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Queue	Mapping to IP Precedence
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Figure 4-8-11 IP Precedence Mapping Screenshot

The page includes the following fields:

Object	Description
• **IP Precedence**	Display the current CoS value
• **Mapping to Queue**	Display the current mapping to queue
• **Queue**	Display the current queue value
• **Mapping to IP Precedence**	Display the current mapping to IP Precedence

4.8.3 QoS Basic Mode

4.8.3.1 Global Settings

The Basic Mode Global Settings and QoS Information screen in Figure 4-8-12 and Figure 4-8-13 appear.

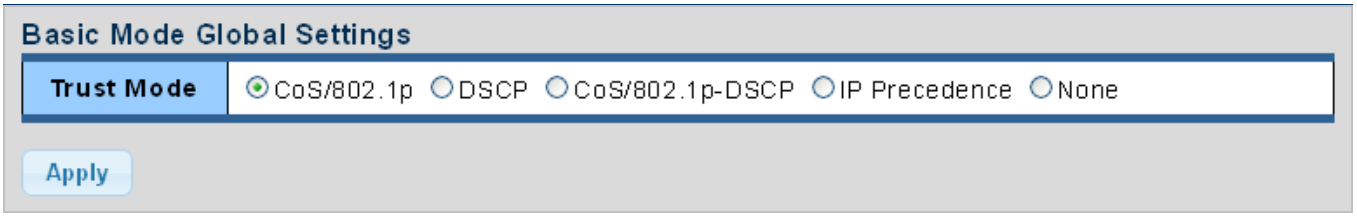


Figure 4-8-12 Basic Mode Global Settings Screenshot

The page includes the following fields:

Object	Description
• **Trust Mode**	Set the QoS mode

Buttons

Apply: Click to apply changes.

■ **QoS Information**

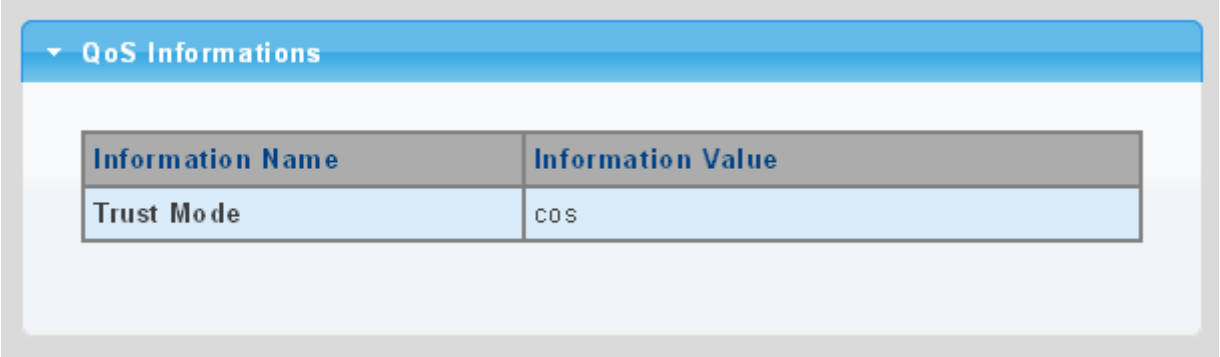


Figure 4-8-13 QoS Information Screenshot

The page includes the following fields:

Object	Description
• **Trust Mode**	Display the current QoS mode

4.8.3.2 Port Settings

The QoS Port Setting and Status screen in Figure 4-8-14 and Figure 4-8-15 appear.

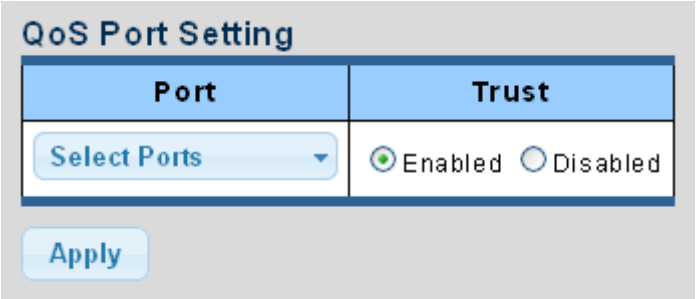


Figure 4-8-14 Basic Mode Global Settings Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number from this drop-down list
• **Trust Mode**	Enable or disable the trust mode

Buttons

Apply: Click to apply changes.

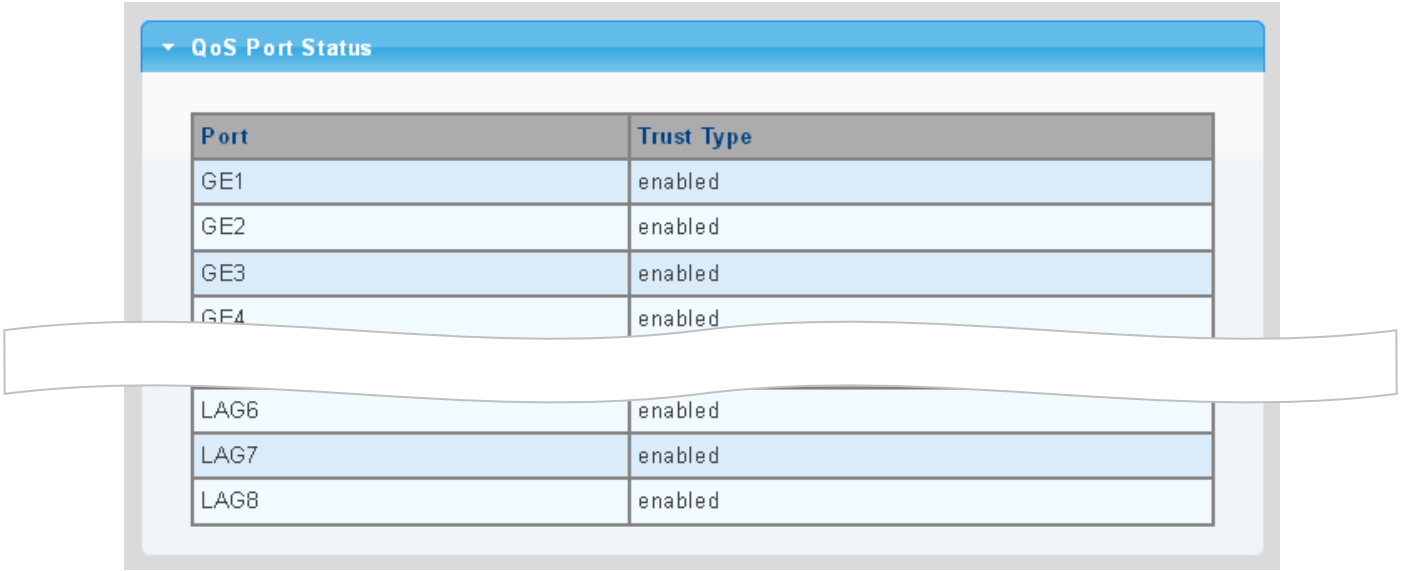


Figure 4-8-15 QoS Port Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Trust Mode**	Display the current trust type

4.8.4 Rate Limit

Configure the switch port rate limit for the switch port on this page.

4.8.4.1 Ingress Bandwidth Control

This page provides to select the ingress bandwidth preamble. The Ingress Bandwidth Control Setting and Status screens in Figure 4-8-16 and Figure 4-8-17 appear.

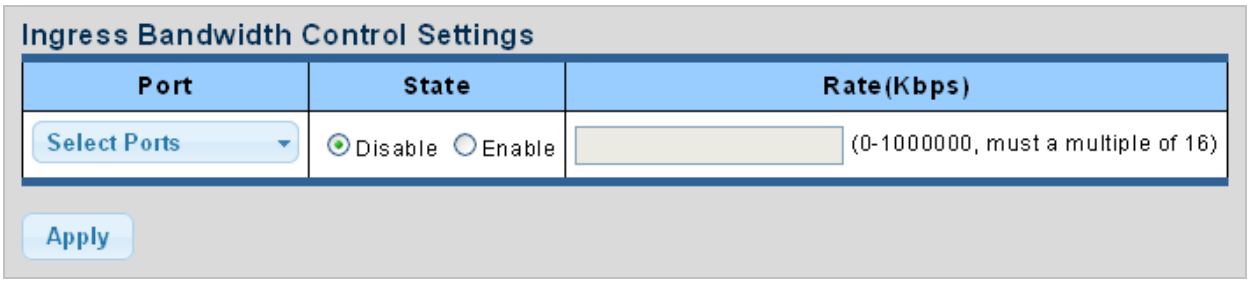


Figure 4-8-16 Ingress Bandwidth Control Settings Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number from this drop-down list
• **State**	Enable or disable the port rate policer. The default value is "Disabled".
• **Rate (Kbps)**	Configure the rate for the port policer. The default value is "unlimited". Valid values are in the range from 0 to 1000000.

Buttons

Apply: Click to apply changes.

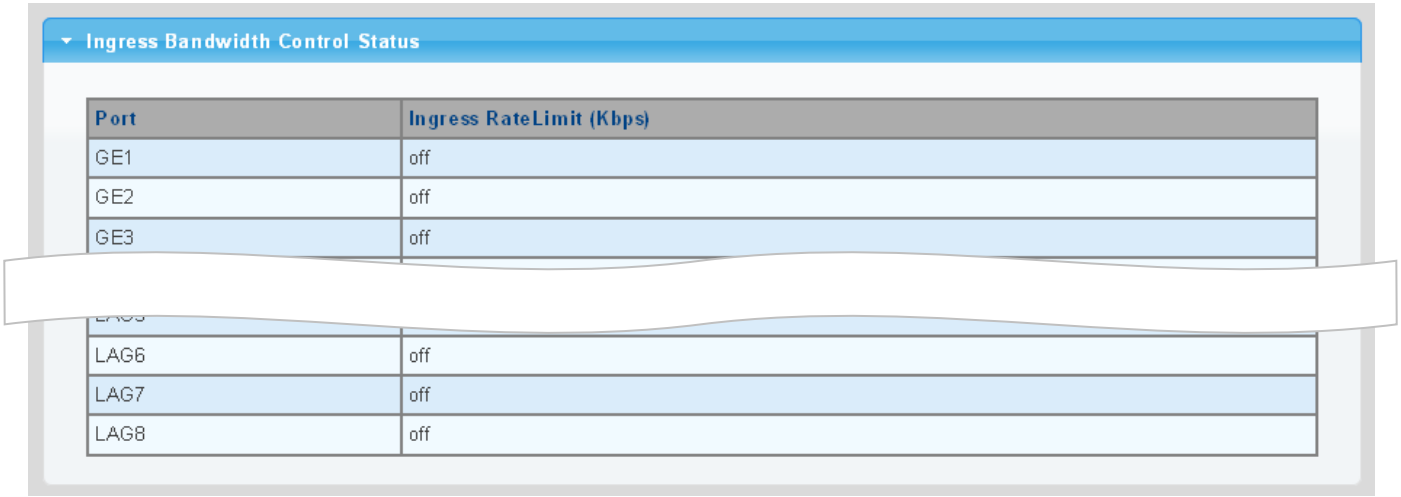


Figure 4-8-17 Ingress Bandwidth Control Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Ingress Rate Limit (Kbps)**	Display the current ingress rate limit

4.8.4.2 Egress Bandwidth Control

This page provides to select the egress bandwidth preamble. The Egress Bandwidth Control Setting and Status screens in Figure 4-8-18 and Figure 4-8-19 appear.

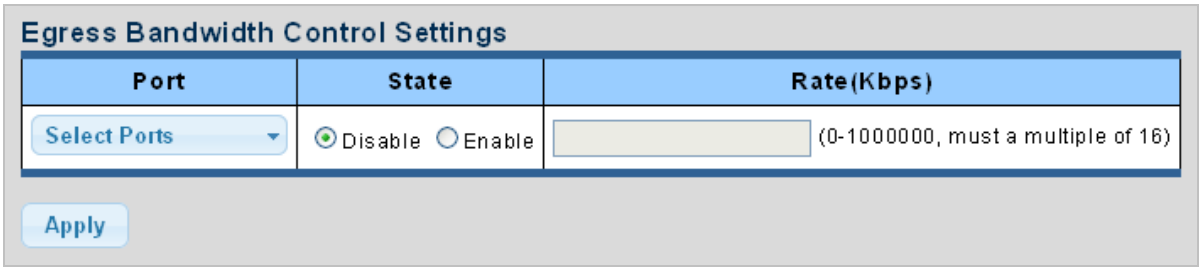


Figure 4-8-18 Egress Bandwidth Control Settings Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number from this drop-down list
• **State**	Enable or disable the port rate policer. The default value is "Disabled".
• **Rate (Kbps)**	Configure the rate for the port policer. The default value is "unlimited". Valid values are in the range from 0 to 1000000.

Buttons

Apply: Click to apply changes.

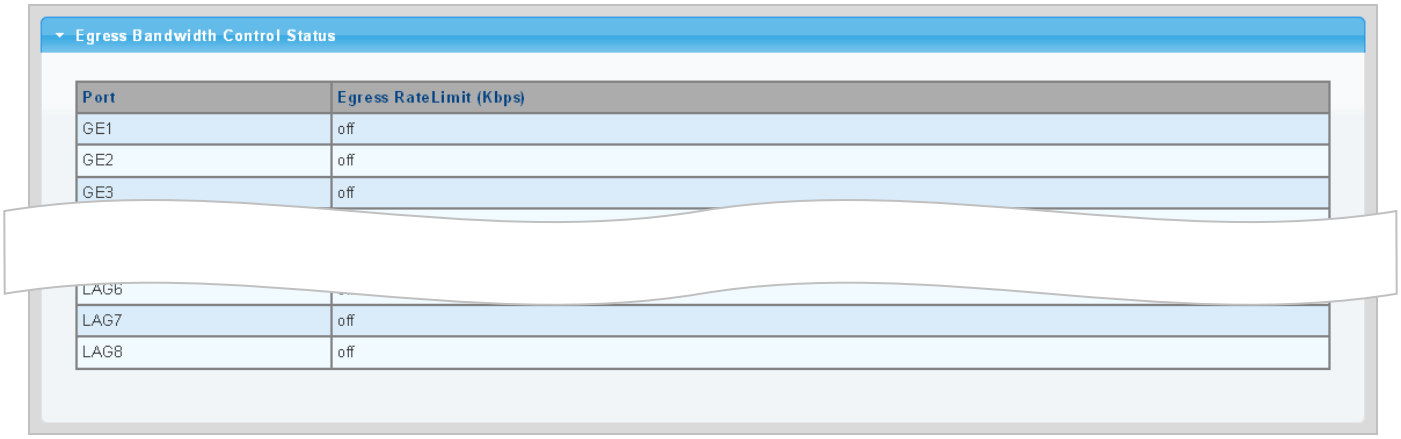


Figure 4-8-19 Egress Bandwidth Control Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Egress Rate Limit (Kbps)**	Display the current egress rate limit

4.8.4.3 Egress Queue

The Egress Queue Bandwidth Control Settings and Status screens in Figure 4-8-20 and Figure 4-8-21 appear.

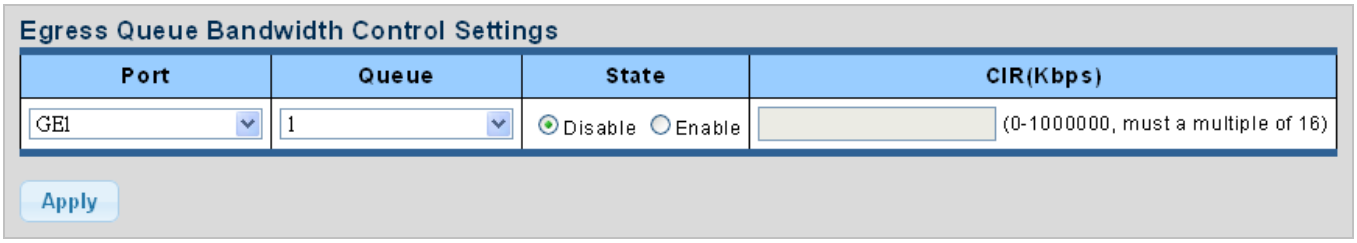


Figure 4-8-20 Egress Queue Bandwidth Settings Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number from this drop-down list
• **Queue**	Select queue number from this drop-down list
• **State**	Enable or disable the port rate policer. The default value is "Disabled".
• **CIR (Kbps)**	Configure the CIR for the port policer. The default value is "unlimited". Valid values are in the range from 0 to 1000000.

Buttons

Apply: Click to apply changes.

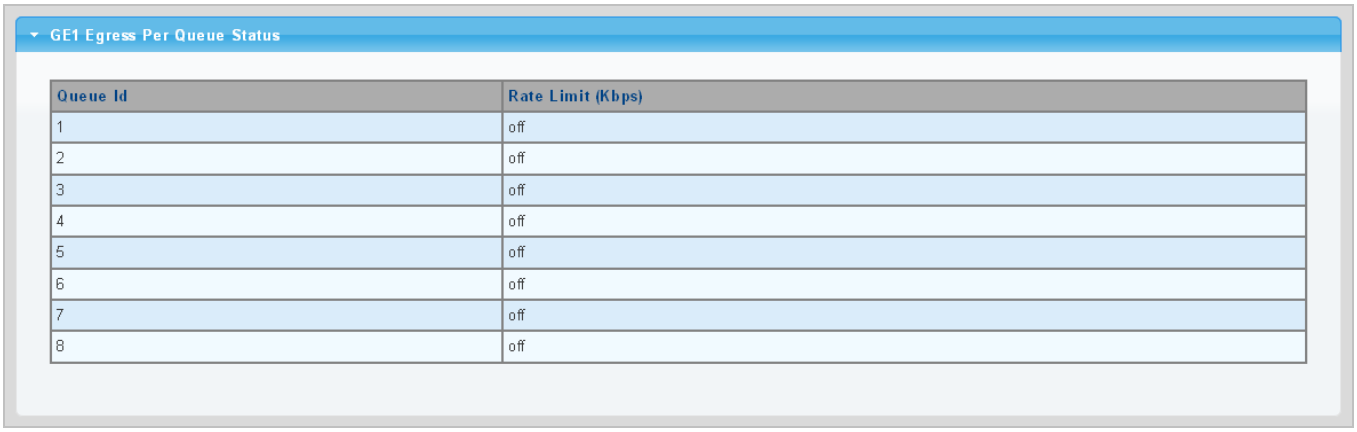


Figure 4-8-21 Egress Queue Status Screenshot

The page includes the following fields:

Object	Description
• **Queue ID**	Display the current queue ID
• **Rate Limit (Kbps)**	Display the current rate limit

4.8.5 Voice VLAN

4.5.8.1 Introduction to Voice VLAN

Configure the switch port rate limit for the switch port on this page.

Voice VLAN is specially configured for the user voice data traffic. By setting a Voice VLAN and adding the ports of the connected voice equipments to Voice VLAN, the user will be able to configure QoS (Quality of service) service for voice data, and improve voice data traffic transmission priority to ensure the calling quality.

The switch can judge if the data traffic is the voice data traffic from specified equipment according to the source MAC address field of the data packet entering the port. The packet with the source MAC address complying with the system defined voice equipment **OUI (Organizationally Unique Identifier)** will be considered the voice data traffic and transmitted to the Voice VLAN.

The configuration is based on MAC address, acquiring a mechanism in which every voice equipment transmitting information through the network has got its unique MAC address. VLAN will trace the address belongs to specified MAC. By This means, VLAN allows the voice equipment always belong to Voice VLAN when relocated physically. The greatest advantage of the VLAN is the equipment can be automatically placed into Voice VLAN according to its voice traffic which will be transmitted at specified priority. Meanwhile, when voice equipment is physically relocated, it still belongs to the Voice VLAN without any further configuration modification, which is because it is based on voice equipment other than switch port.

Note

The Voice VLAN feature enables the voice traffic to forward on the Voice VLAN, and then the switch can be classified and scheduled to network traffic. **It is recommended there are two VLANs on a port** -- one for voice, one for data.

Note

Before connecting the IP device to the switch, **the IP phone should configure the voice VLAN ID correctly**. It should be configured through its own GUI.

4.8.5.2 Properties

The Voice VLAN feature enables voice traffic to forward on the Voice VLAN, and then the switch can be classified and scheduled to network traffic. It is recommended that there are two VLANs on a port -- one for voice, one for data.

Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI. This page provides to select the ingress bandwidth preamble. The Ingress Bandwidth Control Setting/Status screen in Figure 4-8-22 and Figure 4-8-23 appears.

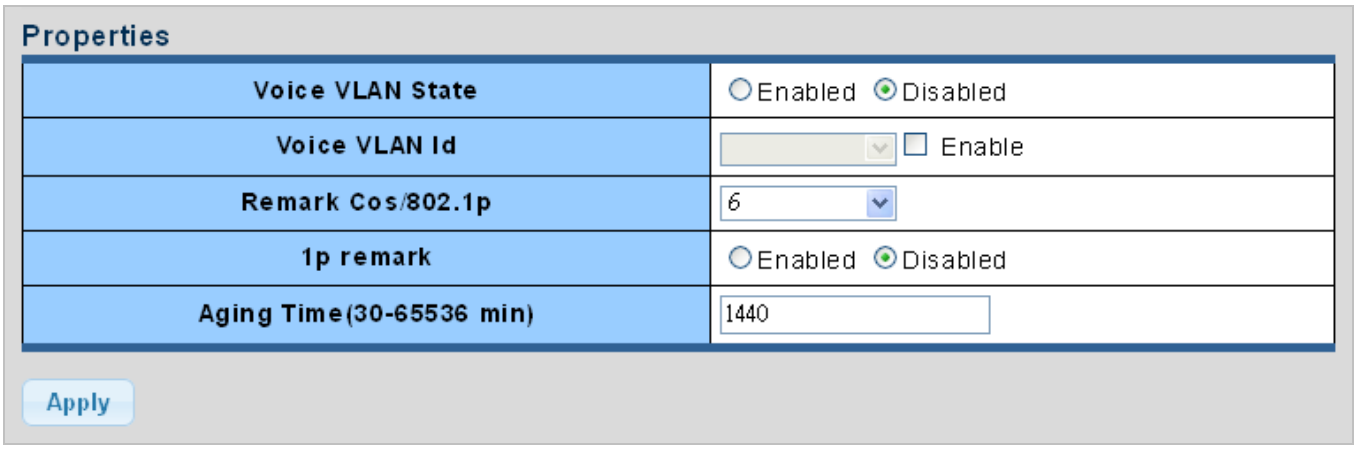


Figure 4-8-22 Properites Screenshot

The page includes the following fields:

Object	Description
• **Voice VLAN State**	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible modes are: ■ **Enabled**: Enable Voice VLAN mode operation. ■ **Disabled**: Disable Voice VLAN mode operation
• **Voice VLAN ID**	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is conflict configuration if the value equal management VID, MVR VID, PVID, etc. The allowed range is from 1 to 4095.
• **Remark CoS/802.1p**	Select 802.1p value from this drop-down list
• **1p remark**	Enable or disable 802.1p remark
• **Aging Time (30-65536 min)**	The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (\Default: **1440** minutes).

Buttons

Apply: Click to apply changes.

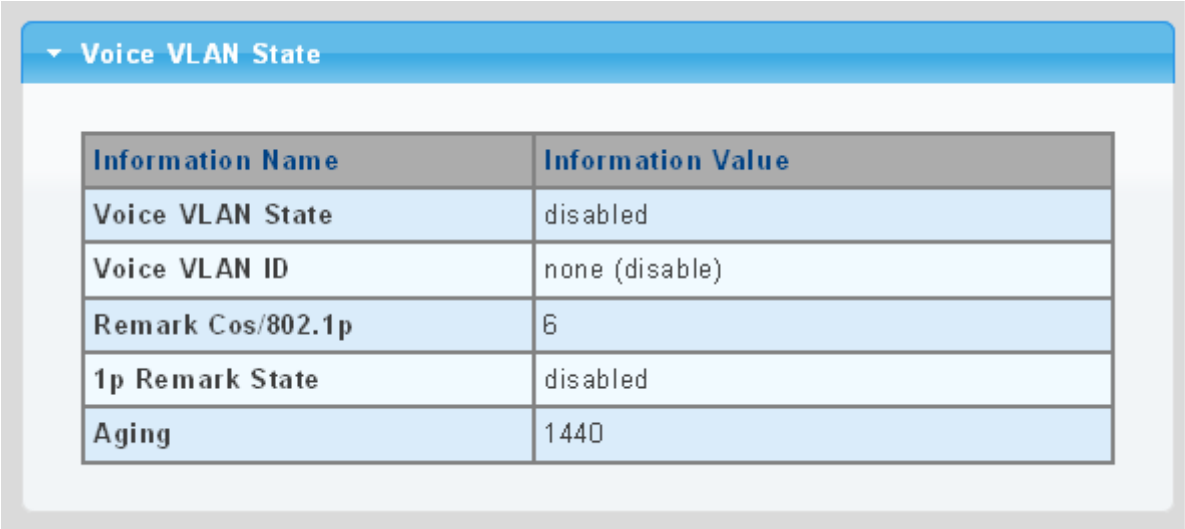


Figure 4-8-23 Properites Screenshot

The page includes the following fields:

Object	Description
• **Voice VLAN State**	Display the current voice VLAN state.
• **Voice VLAN ID**	Display the current voice VLAN ID.
• **Remark CoS/802.1p**	Display the current remark CoS/802.1p.
• **1p remark**	Display the current 1p remark.
• **Aging**	Display the current aging time.

4.8.5.3 Telephony OUI MAC Setting

Configure VOICE VLAN OUI table on this page. The Telephony OUI MAC Setting screens in Figure 4-8-24 and Figure 4-8-25 appear.

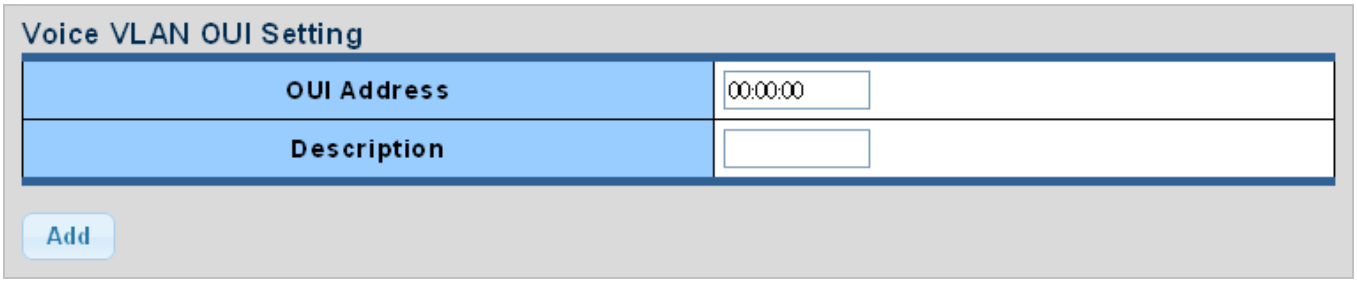


Figure 4-8-24 Voice VLAN OUI Settings Screenshot

The page includes the following fields:

Object	Description
• **OUI Address**	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx:xx:xx" (x is a hexadecimal digit).
• **Description**	User-defined text that identifies the VoIP devices

Buttons

Add: Click to add voice VLAN OUI setting.

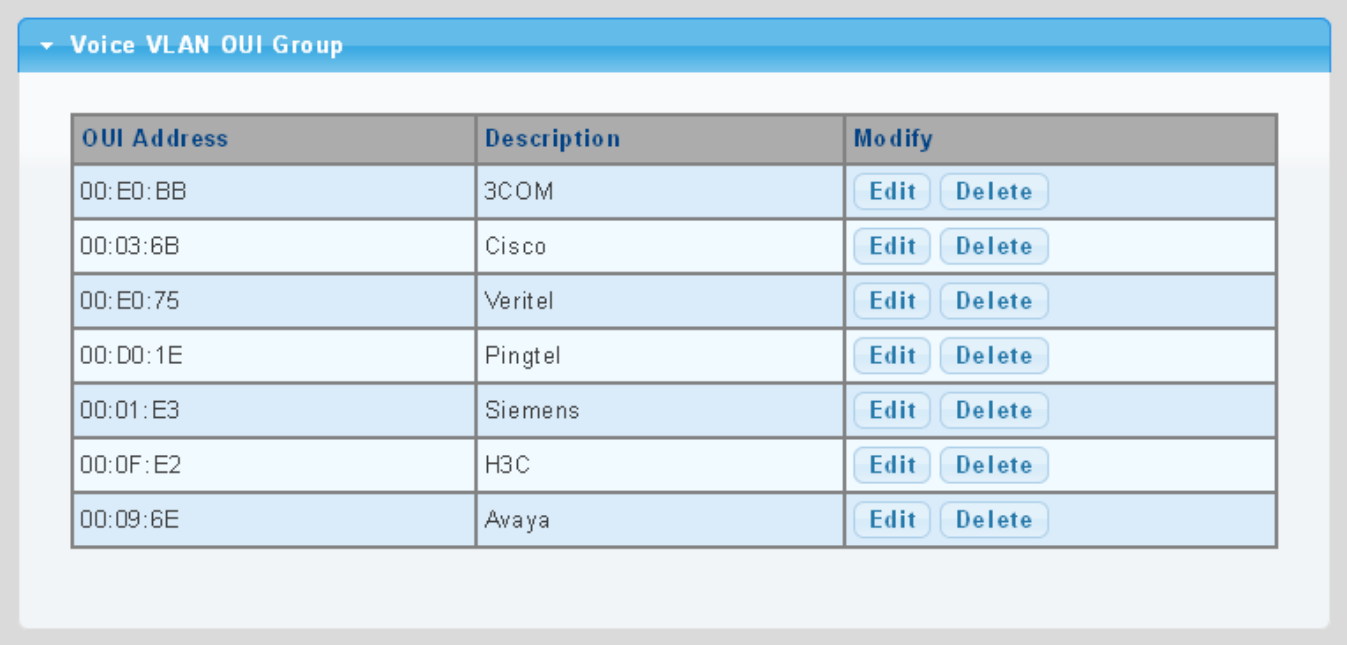


Figure 4-8-25 Voice VLAN OUI Group Screenshot

The page includes the following fields:

Object	Description
• **OUI Address**	Display the current OUI address
• **Description**	Display the current description
• **Modify**	Click Edit to edit voice VLAN OUI group parameter Click Delete to delete voice VLAN OUI group parameter

4.8.5.4 Telephony OUI Port Setting

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI. The Telephony OUI MAC Setting screens in Figure 4-8-26 and Figure 4-8-27 appear.

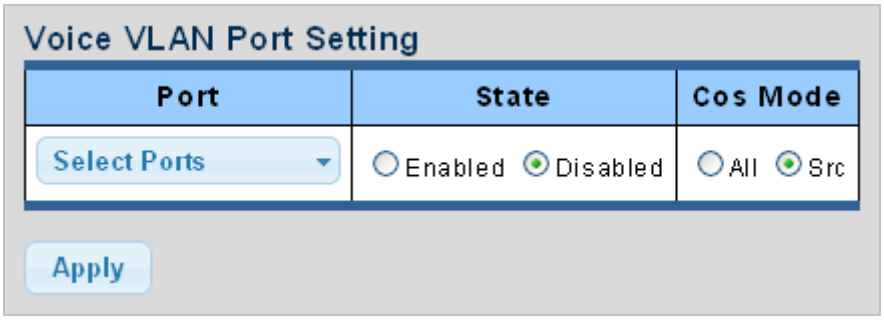


Figure 4-8-26 Voice VLAN Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number from this drop-down list
• **State**	Enable or disable the voice VLAN port setting. The default value is "Disabled".
• **CoS Mode**	Select the current CoS mode

Buttons

Apply: Click to apply changes.

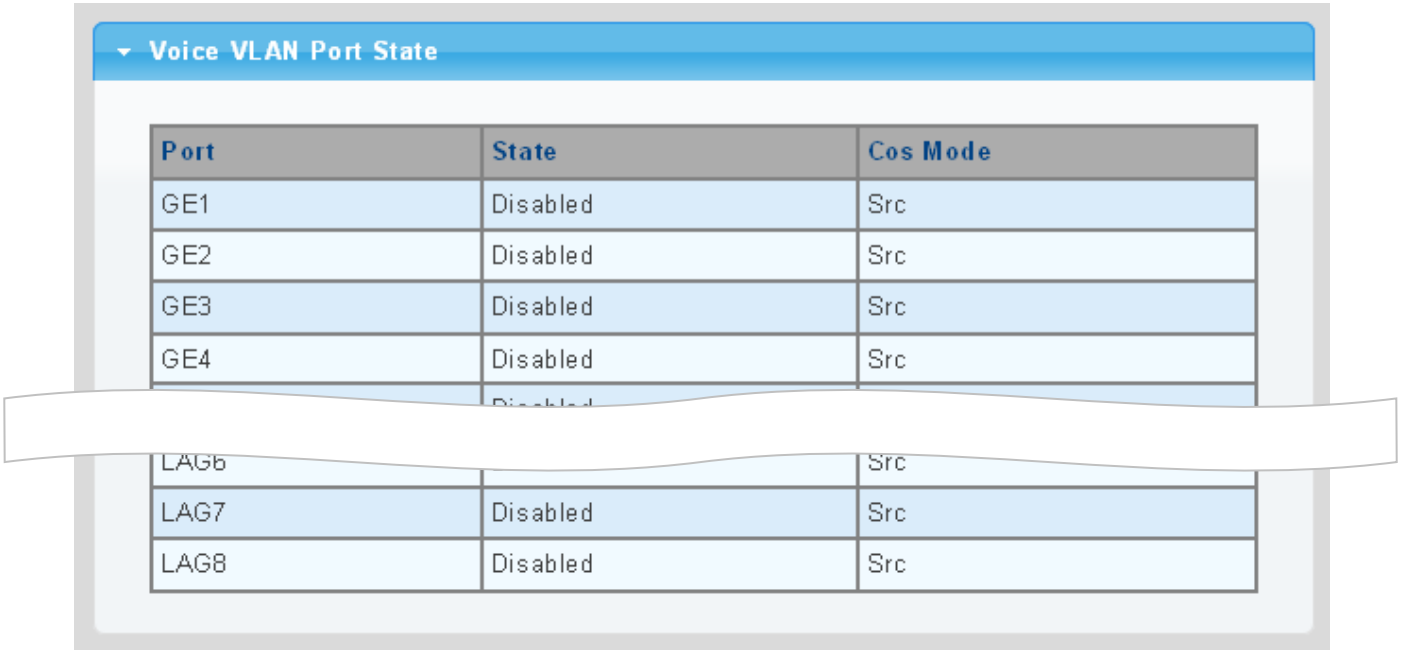


Figure 4-8-27 Voice VLAN Port State Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **State**	Display the current state
• **CoS Mode**	Display the current CoS mode

4.9 Security

This section is to control the access of the Managed Switch, including the user access and management control.

The Security page contains links to the following main topics:

- **802.1x**
- **Radius Server**
- **TACACS+ Server**
- **AAA**
- **Access**
- **Management Access Method**
- **DHCP Snooping**
- **Dynamic ARP Inspection**
- **IP Source Guard**
- **Port Security**
- **DoS**
- **Strom Control**

4.9.1 802.1X

Overview of 802.1X (Port-based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as **EAPOL (EAP over LANs)** frames. EAPOL frames encapsulate **EAP PDU**s (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like **MD5-Challenge**, **PEAP**, and **TLS**. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Overview of User Authentication

It is allowed to configure the Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This Managed Switch provides secure network management access using the following options:

- **Remote Authentication Dial-in User Service (RADIUS)**
- **Terminal Access Controller Access Control System Plus (TACACS+)**
- **Local user name and Privilege Level control**

4.9.1.1 Understanding IEEE 802.1X Port-based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only **Extensible Authentication Protocol over LAN (EAPOL)** traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ **Device Roles**

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.

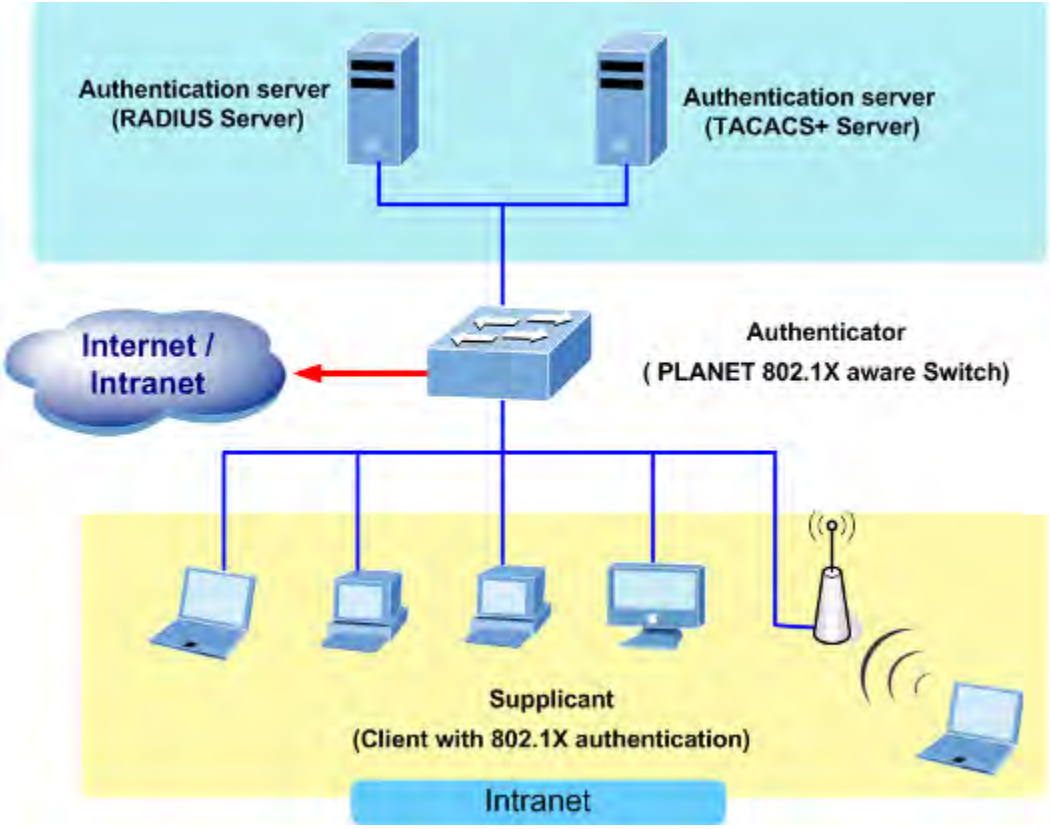


Figure 4-9-1

- ***Client***—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1X specification.)

- ***Authentication server***—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible Authentication Protocol (EAP)** extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- ***Switch* (802.1X device)**—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ **Authentication Initiation and Message Exchange**

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if, during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

Note

If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. "Figure 4-9-2" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

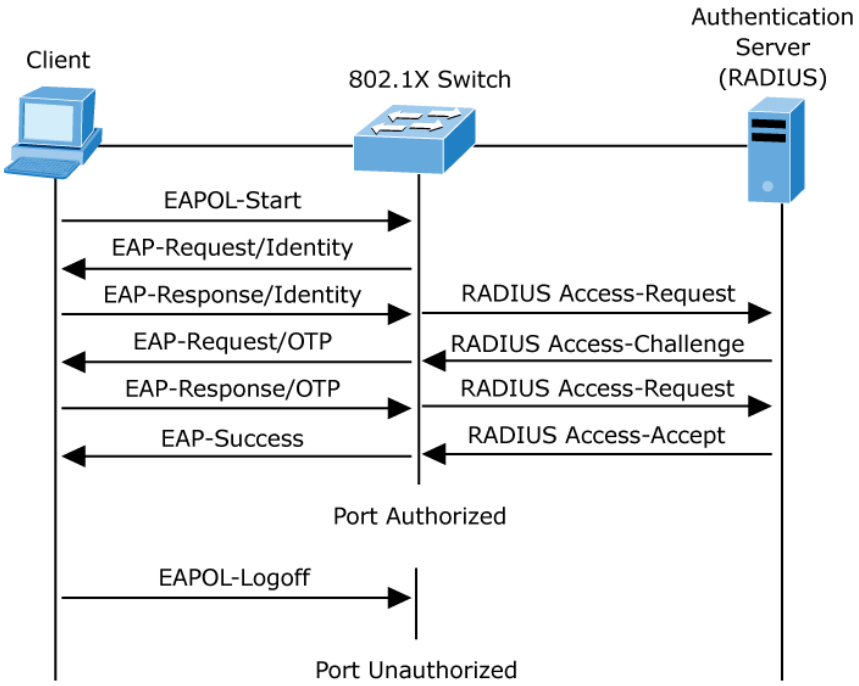


Figure 4-9-2 EAP Message Exchange

■ **Ports in Authorized and Unauthorized States**

The switch port state determines whether or not the client is granted access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

4.9.1.2 802.1X Setting

This page allows you to configure the IEEE 802.1X authentication system.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "**Security→802.1X Access Control→802.1X Setting**" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

The 802.1X Setting and Information screens in Figure 4-9-3 and Figure 4-9-4 appear.

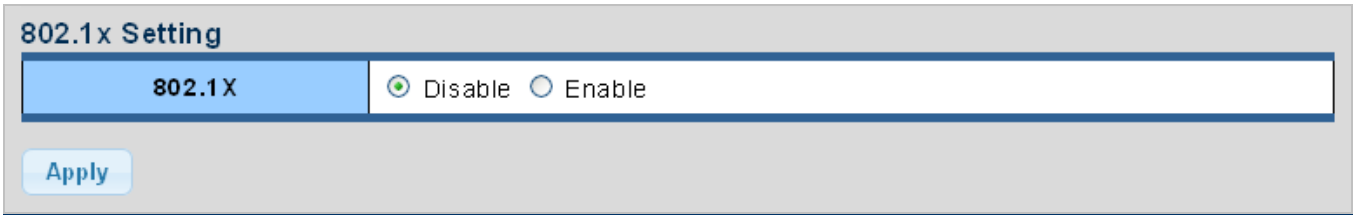


Figure 4-9-3 802.1X Setting Screenshot

The page includes the following fields:

Object	Description
• **802.1X**	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Buttons

Apply: Click to apply changes.

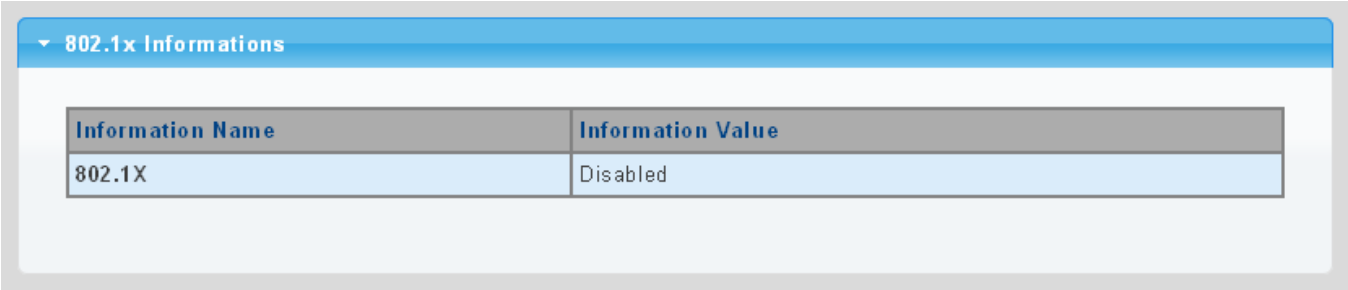


Figure 4-9-4 802.1X Information Screenshot

The page includes the following fields:

Object	Description
• **802.1X**	Display the current 802.1X state

4.9.1.3 802.1X Port Setting

This page allows you to configure the IEEE 802.1X Port Setting. The 802.1X Port Setting screens in Figure 4-9-5 and Figure 4-9-6 appear.

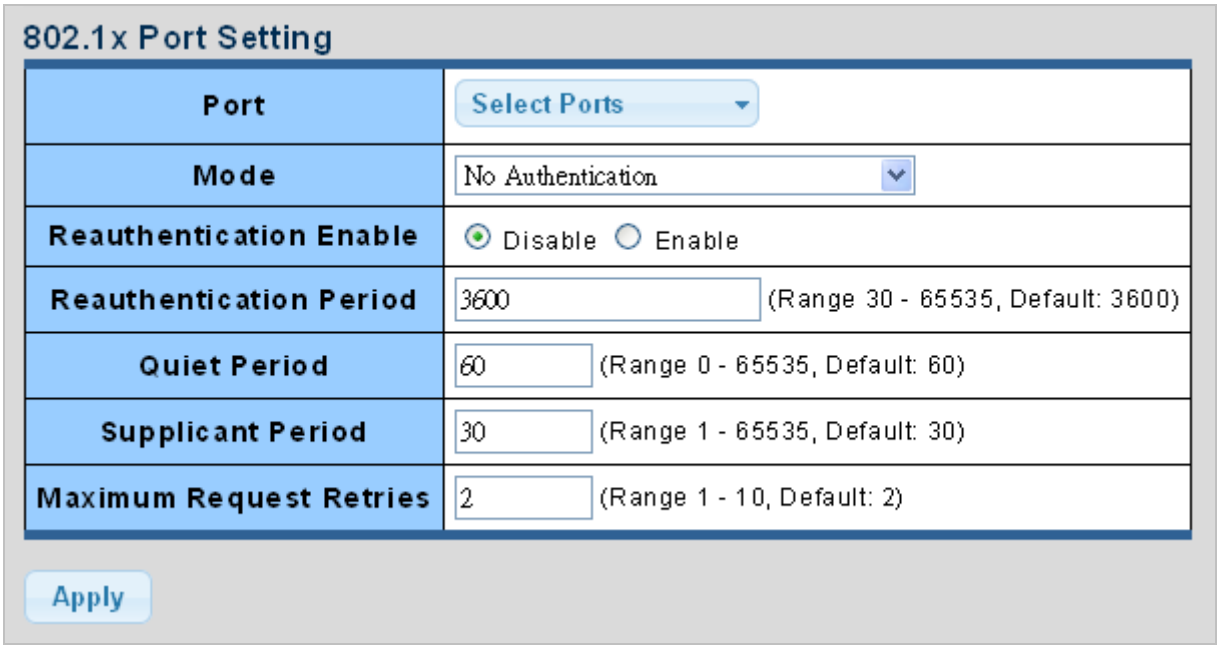


Figure 4-9-5 802.1X Port Setting Screenshot

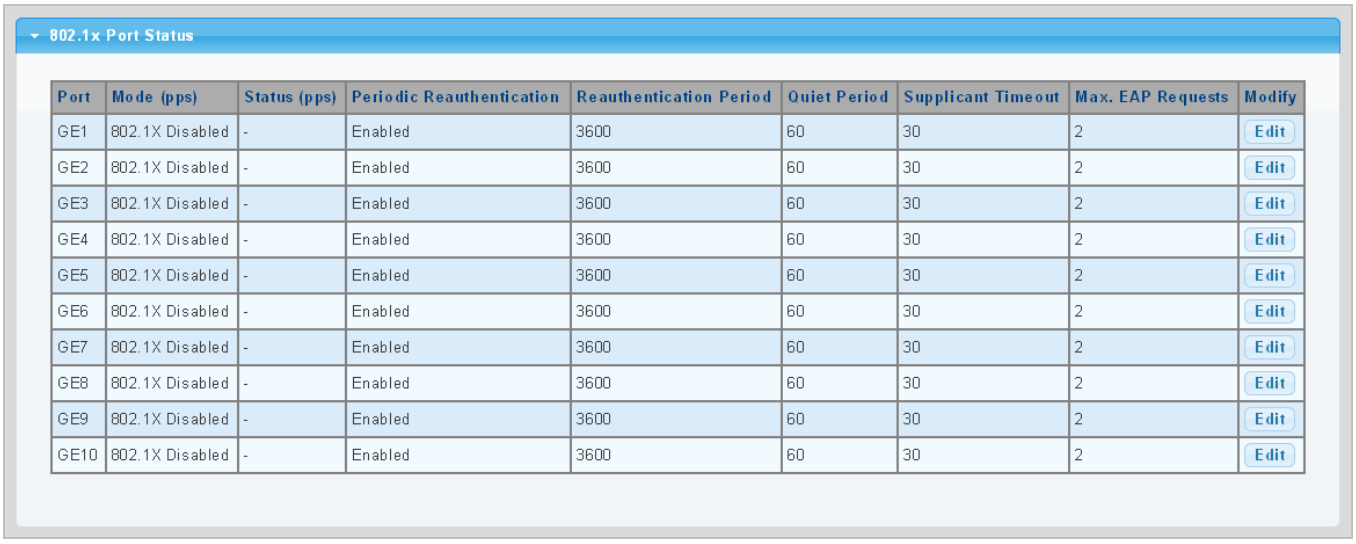
The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **Mode**	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: ■ **No Authentication** ■ **Authentication** ■ **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication. ■ **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
• **Reauthentication Enable**	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a

	switch port or if a supplicant is no longer attached.
• **Reauthentication Period**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range from 30 to 65535 seconds.
• **Quiet Period**	Sets time to keep silent on supplicant authentication failure.
• **Supplicant Period**	Sets the interval for the supplicant to re-transmit EAP request/identify frame.
• **Maximum Request Retries**	The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

Buttons

Apply: Click to apply changes.



802.1x Port Status

Port	Mode (pps)	Status (pps)	Periodic Reauthentication	Reauthentication Period	Quiet Period	Supplicant Timeout	Max. EAP Requests	Modify
GE1	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE2	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE3	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE4	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE5	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE6	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE7	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE8	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE9	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE10	802.1X Disabled	-	Enabled	3600	60	30	2	Edit

Figure 4-9-6 802.1X Port Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Mode (pps)**	Display the current mode.
• **Status (pps)**	Display the current status.
• **Periodic Reauthentication**	Display the current periodic reauthentication.

• **Reauthentication Period**	Display the current reauthentication period.
• **Quiet Period**	Display the current quiet period.
• **Supplicant Timeout**	Display the current supplicant timeout.
• **Max. EAP Requests**	Display the current Max. EAP requests.
• **Modify**	Click Edit to edit 802.1X port setting parameter.

4.9.1.4 Guest VLAN Setting

Overview

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meantime, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

The 802.1X Guest VLAN setting screens in Figure 4-9-7 and Figure 4-9-8 appear.

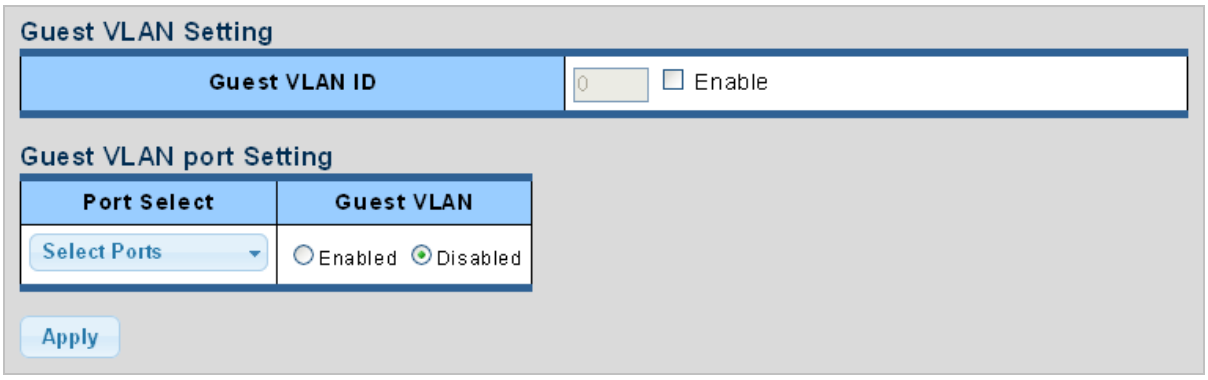


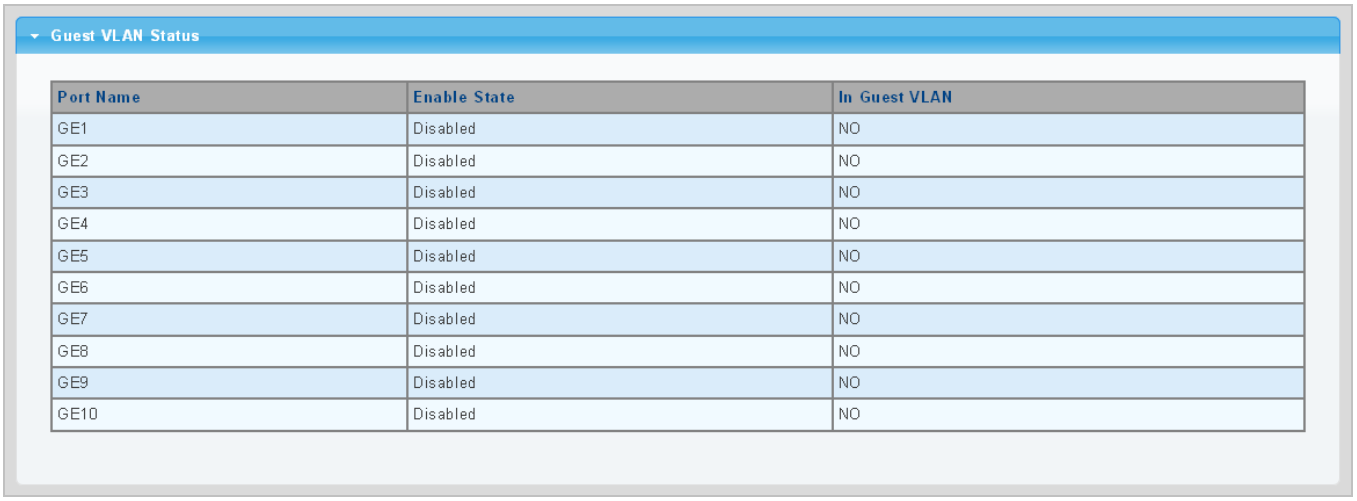
Figure 4-9-7 Guest VLAN Setting Screenshot

The page includes the following fields:

Object	Description
• **Guest VLAN ID**	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1~4094].
• **Guest VLAN Enabled**	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. ■ When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. ■ When unchecked, the ability to move to the Guest VLAN is disabled for all ports.
• **Guest VLAN Port Setting**	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.: • **Port-based 802.1X**

Buttons

Apply: Click to apply changes.



Guest VLAN Status

Port Name	Enable State	In Guest VLAN
GE1	Disabled	NO
GE2	Disabled	NO
GE3	Disabled	NO
GE4	Disabled	NO
GE5	Disabled	NO
GE6	Disabled	NO
GE7	Disabled	NO
GE8	Disabled	NO
GE9	Disabled	NO
GE10	Disabled	NO

Figure 4-9-8 Guest VLAN Status Screenshot

The page includes the following fields:

Object	Description
• **Port Name**	The switch port number of the logical port
• **Enable State**	Display the current state
• **In Guest VLAN**	Display the current guest VLAN

4.9.1.5 Authenticated Host

The Authenticated Host Table screen in Figure 4-9-9 appears.

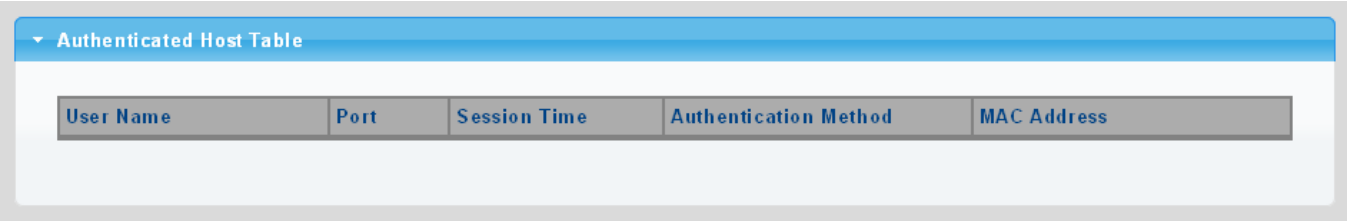


Figure 4-9-9 Authenticated Host Table Screenshot

The page includes the following fields:

Object	Description
• **User Name**	Display the current user name
• **Port**	Display the current port number
• **Session Time**	Display the current session time
• **Authentication Method**	Display the current authentication method
• **MAC Address**	Display the current MAC address

4.9.2 RADIUS Server

This page is to configure the RADIUS server connection session parameters. The RADIUS Settings screens in Figure 4-9-10, Figure 4-9-11 and Figure 4-9-12 appears.

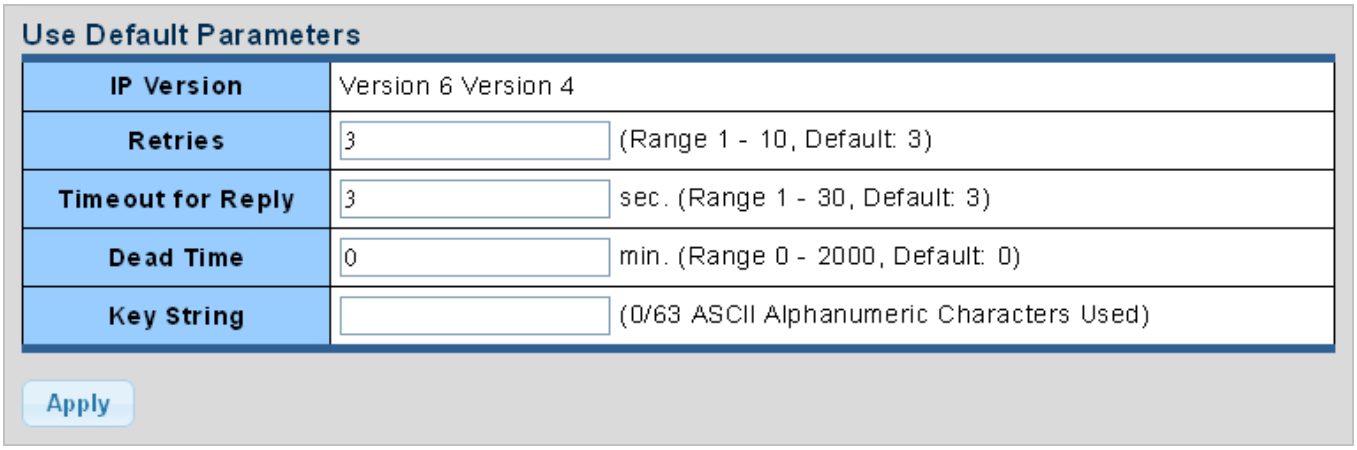


Figure 4-9-10 Use Default Parameters Screenshot

The page includes the following fields:

Object	Description
• **Retries**	Timeout is the number of seconds, in the range from 1 to 10, to wait for a reply from a RADIUS server before retransmitting the request.
• **Timeout for Reply**	Retransmit is the number of times, in the range from 1 to 30, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
• **Key String**	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

Buttons

Apply: Click to apply changes.

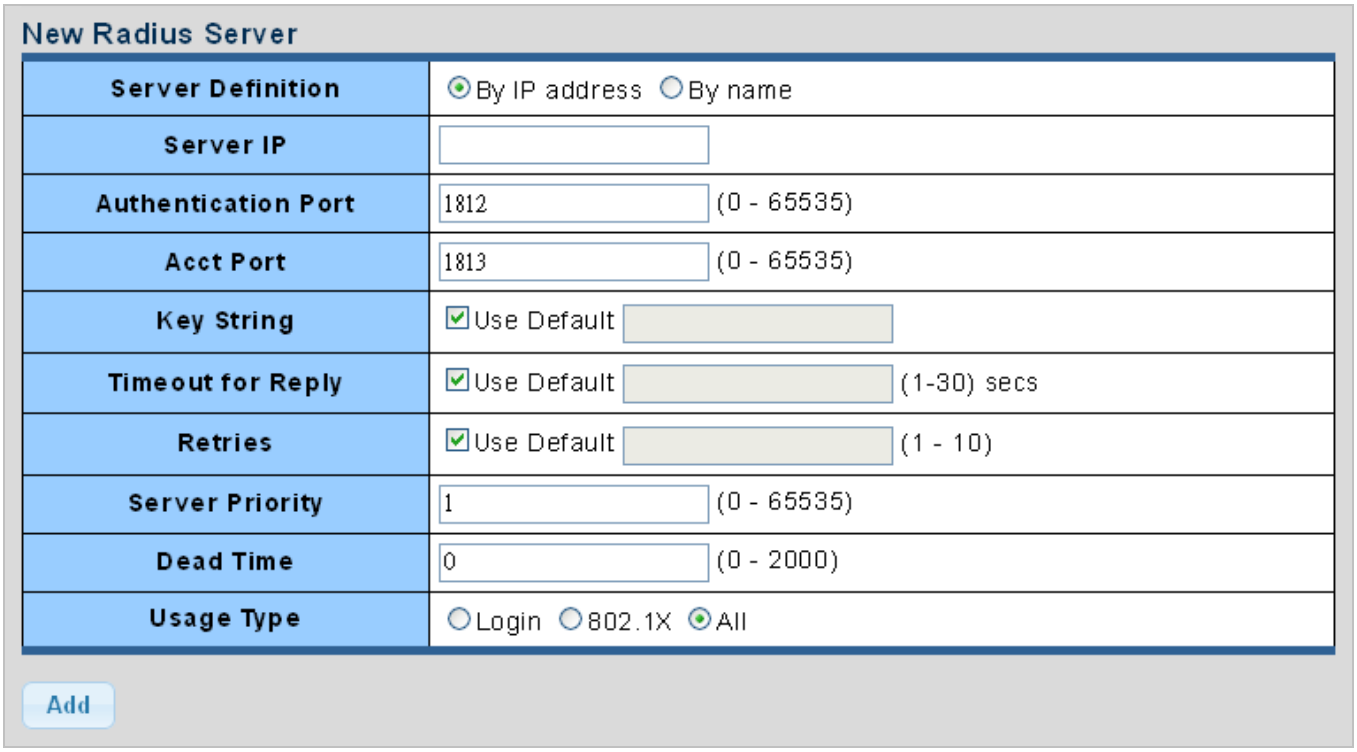


Figure 4-9-11 New Radius Server Screenshot

The page includes the following fields:

Object	Description
• **Server Definition**	Set the server definition
• **Server IP**	Address of the Radius server IP/name
• **Authentication Port**	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
• **Acct Port**	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
• **Key String**	The shared key - shared between the RADIUS Authentication Server and the switch.
• **Timeout for Reply**	The Timeout, which can be set to a number between 1 and 30 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
• **Retries**	Timeout is the number of seconds, in the range from 1 to 10, to wait for a reply from a RADIUS server before retransmitting the request.

• **Server Priority**	Set the server priority
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
• **Usage Type**	Set the usage type. The following modes are available: ■ **Login** ■ **802.1X** ■ **All**

Buttons

Add: Click to add Radius server setting.

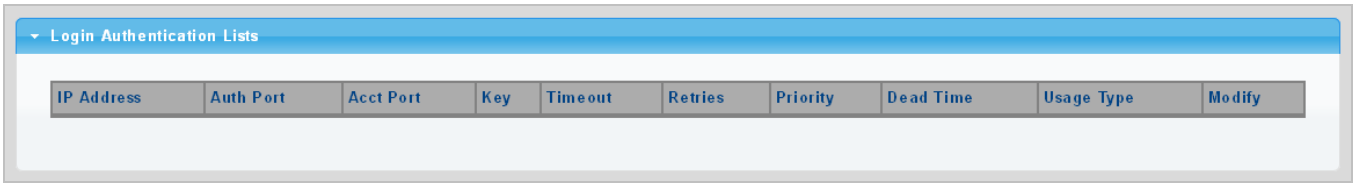


Figure 4-9-12 Login Authentication List Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	Display the current IP address
• **Auth Port**	Display the current auth port
• **Acct Port**	Display the current acct port
• **Key**	Display the current key
• **Timeout**	Display the current timeout
• **Retries**	Display the current retry times
• **Priority**	Display the current priority
• **Dead Time**	Display the current dead time
• **Usage Type**	Display the current usage type
• **Modify**	Click Edit to edit login authentication list parameter. Click Delete to delete login authentication list entry.

4.9.3 TACACS+ Server

This page is to configure the RADIUS server connection session parameters. The RADIUS Settings screens in Figure 4-9-13, Figure 4-9-14 and Figure 4-9-15 appear.

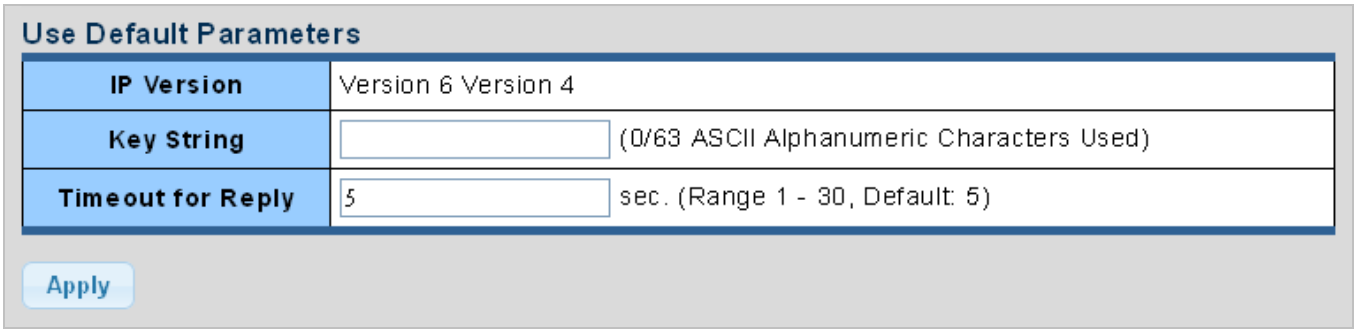


Figure 4-9-13 Guest VLAN Setting Screenshot

The page includes the following fields:

Object	Description
• **Key String**	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.
• **Timeout for Reply**	Retransmit is the number of times, in the range from 1 to 30, a TACACS+ request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Buttons

Apply: Click to apply changes.

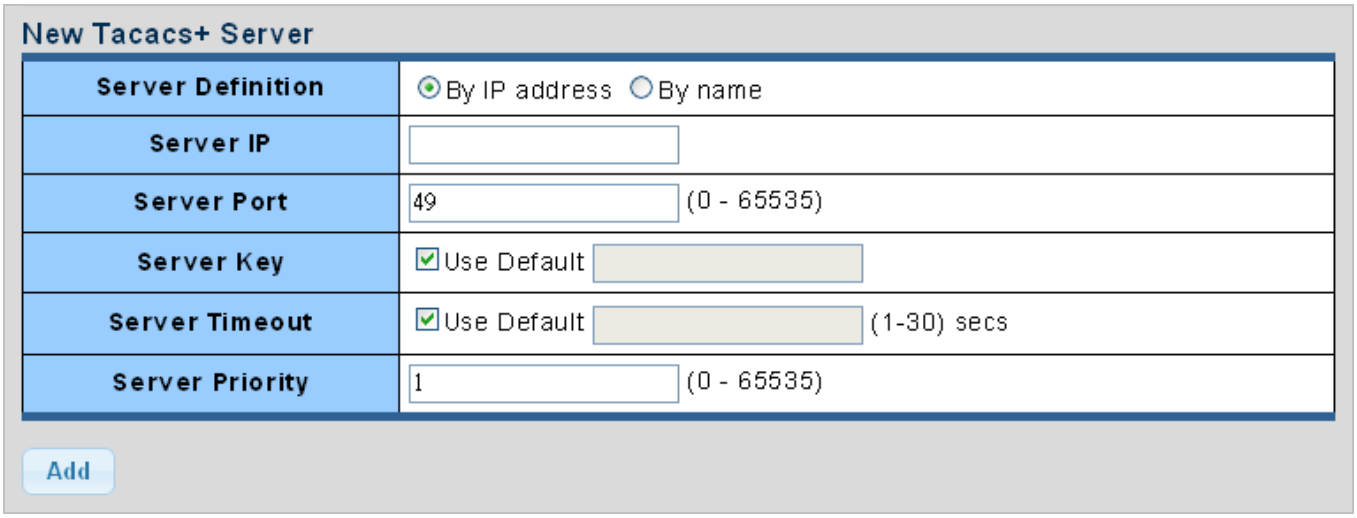


Figure 4-9-14 New Radius Server Screenshot

The page includes the following fields:

Object	Description
• **Server Definition**	Set the server definition
• **Server IP**	Address of the TACACS+ server IP/name
• **Server Port**	Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: **49**)
• **Server Key**	The key- shared between the TACACS+ Authentication Server and the switch.
• **Server Timeout**	The number of seconds the switch waits for a reply from the server before it resends the request.
• **Server Priority**	Set the server priority

Buttons

Add: Click to add Radius server setting.

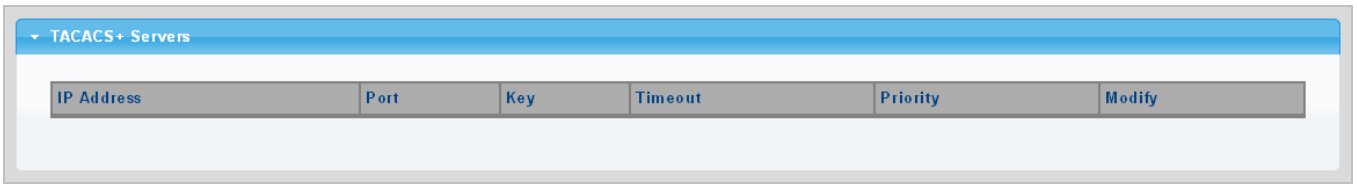


Figure 4-9-15 Login Authentication List Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	Display the current IP address
• **Port**	Display the current port
• **Key**	Display the current key
• **Timeout**	Display the current timeout
• **Retries**	Display the current retry times
• **Priority**	Display the current priority
• **Modify**	Click Edit to edit login authentication list parameter Click Delete to delete login authentication list entry

4.9.4 AAA

Authentication, authorization, and accounting (AAA) provides a framework for configuring access control on the Managed Switch. The three security functions can be summarized as follows:

- **Authentication** — Identifies users that request access to the network.
- **Authorization** — Determines if users can access specific services.
- **Accounting** — Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are then applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The Managed Switch supports the following AAA features:

- Accounting for **IEEE 802.1X authenticated users** that access the network through the Managed Switch.
- Accounting for users that access **management interfaces** on the Managed Switch through the console and Telnet.
- Accounting for **commands** that users enter at specific CLI privilege levels. Authorization of users that access management interfaces on the Managed Switch through the console and Telnet.

To configure AAA on the Managed Switch, you need to follow this general process:

1. Configure RADIUS and TACACS+ server access parameters. See "**Configuring Local/Remote Logon Authentication**".

2. Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.

3. Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use. Apply the method names to port or line interfaces.

Note

This guide assumes that RADIUS and TACACS+ servers have already been configured to support AAA. The configuration of RADIUS and TACACS+ server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS or TACACS+ server software.

4.9.4.1 Login List

This page is to login list parameters. The authentication list screen in Figure 4-9-17 and Figure 4-9-18 appears.

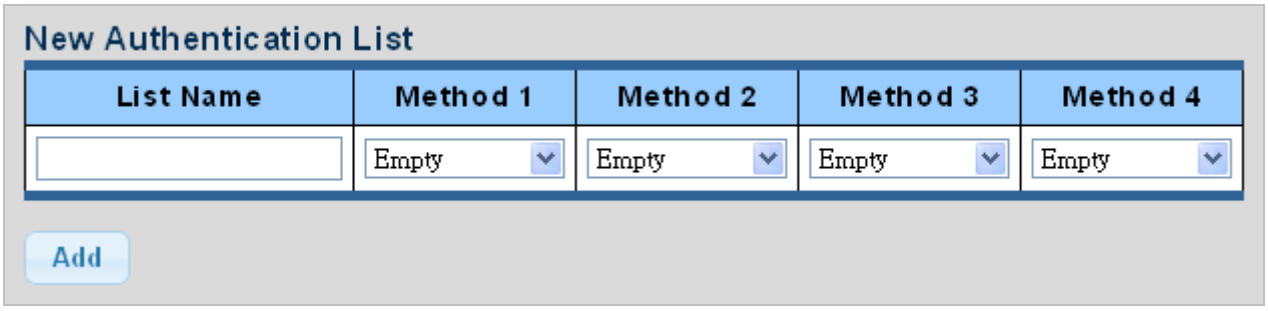


Figure 4-9-17 New Authentication List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Defines a name for the authentication list
• **Method 1-4**	Set the login authentication method: Empty / None / Local / TACACS+ / RADIUS / Enable

Buttons

Add: Click to add authentication list.

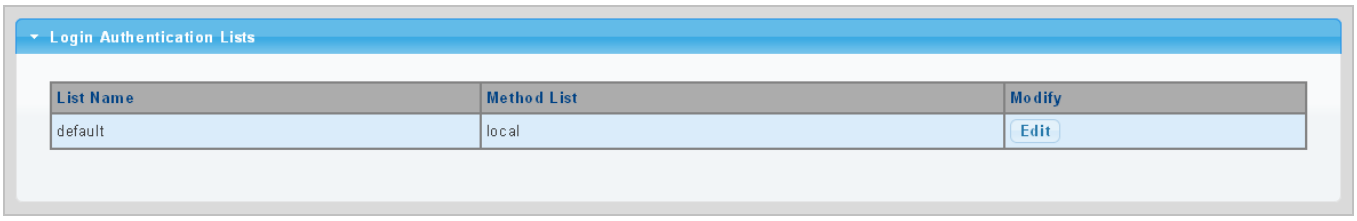


Figure 4-9-18 Login Authentication List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Display the current list name
• **Method List**	Display the current method list
• **Modify**	Click Edit to edit login authentication list parameter Click Delete to delete login authentication list entry

4.9.4.2 Enable List

This page is to login list parameters. The authentication list screens in Figure 4-9-19 and Figure 4-9-20 appear.

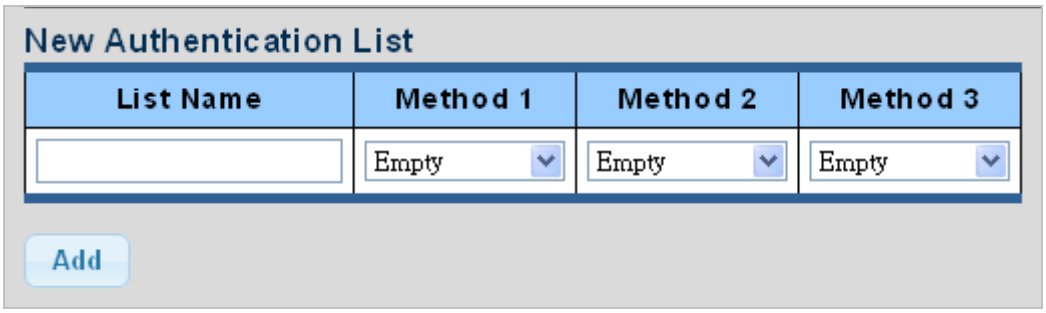


Figure 4-9-19 New Authentication List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Defines a name for the authentication list
• **Method 1-3**	Set the login authentication method: Empty / None / Enable / TACACS+ / RADIUS

Buttons

Add: Click to add authentication list.

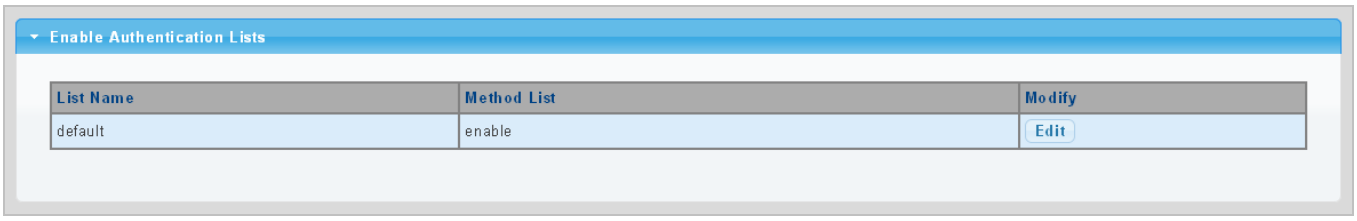


Figure 4-9-20 Login Authentication List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Display the current list name
• **Method List**	Display the current method list
• **Modify**	Click Edit to edit login authentication list parameter Click Delete to delete login authentication list entry

4.9.5 Access

This section is to control the access of the Managed Switch, including the different access methods – Telnet, SSH, HTTP and HTTPs.

4.9.5.1 Telnet

The Telnet Settings and Information screen in Figure 4-9-21 and Figure 4-9-22 appear.

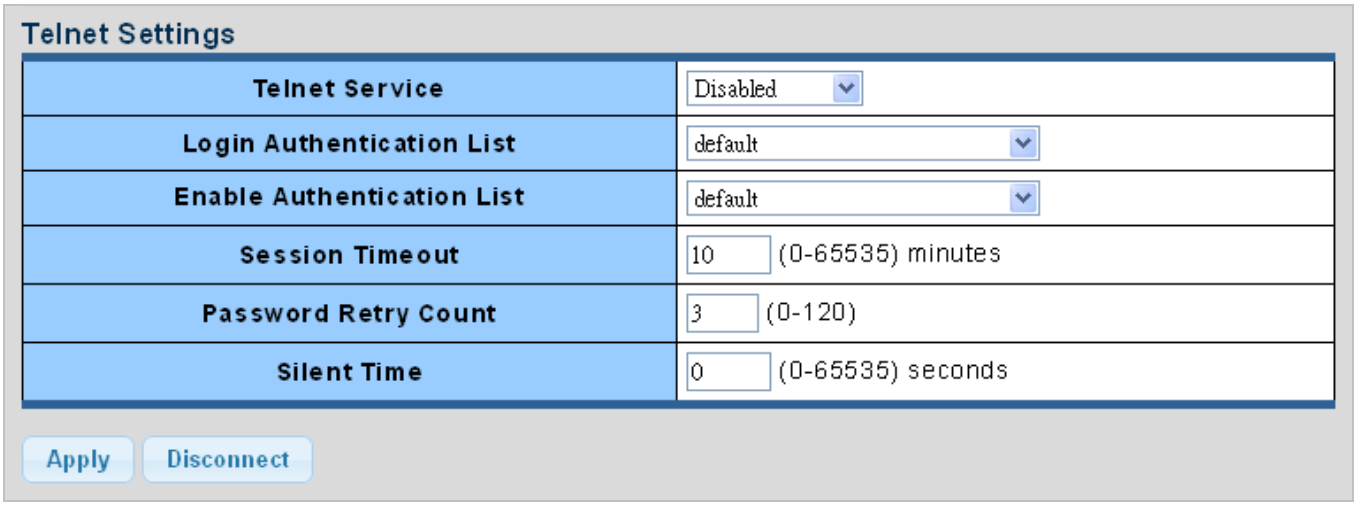


Figure 4-9-21 Telnet Settings Screenshot

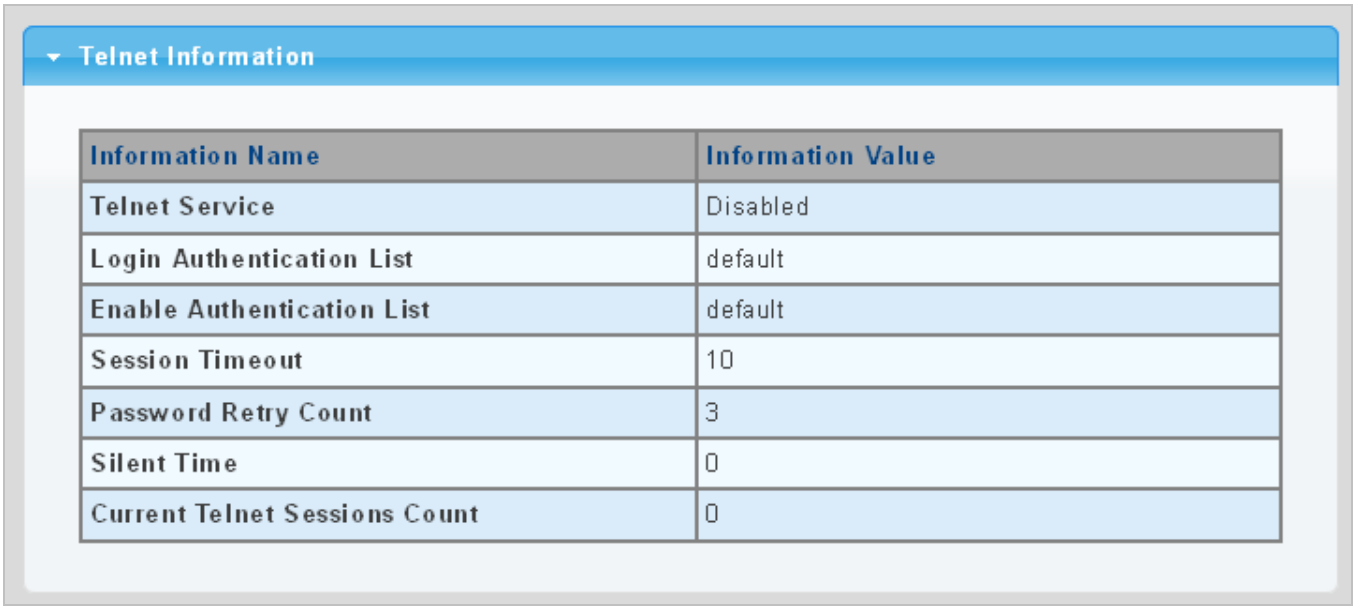
The page includes the following fields:

Object	Description
• **Telnet Service**	Disable or enable telnet service
• **Login Authentication List**	Select login authentication list from this drop-down list
• **Enable Authentication List**	Select enable authentication list from this drop-down list
• **Session Timeout**	Set the session timeout value
• **Password Retry Count**	Set the password retry count value
• **Silent Time**	Set the silent time value

Buttons

Apply: Click to apply changes

Disconnect: Click to disconnect telnet communication



Telnet Information

Information Name	Information Value
Telnet Service	Disabled
Login Authentication List	default
Enable Authentication List	default
Session Timeout	10
Password Retry Count	3
Silent Time	0
Current Telnet Sessions Count	0

Figure 4-9-21 Telnet Information Screenshot

The page includes the following fields:

Object	Description
• **Telnet Service**	Display the current Telnet service
• **Login Authentication List**	Display the current login authentication list
• **Enable Authentication List**	Display the current enable authentication list
• **Session Timeout**	Display the current session timeout
• **Password Retry Count**	Display the current password retry count
• **Silent Time**	Display the current silent time
• **Current Telnet Session Count**	Display the current telnet session count

4.9.5.2 SSH

Configure SSH on this page. This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The SSH Settings and Information screens in Figure 4-9-23 and Figure 4-9-24 appear.

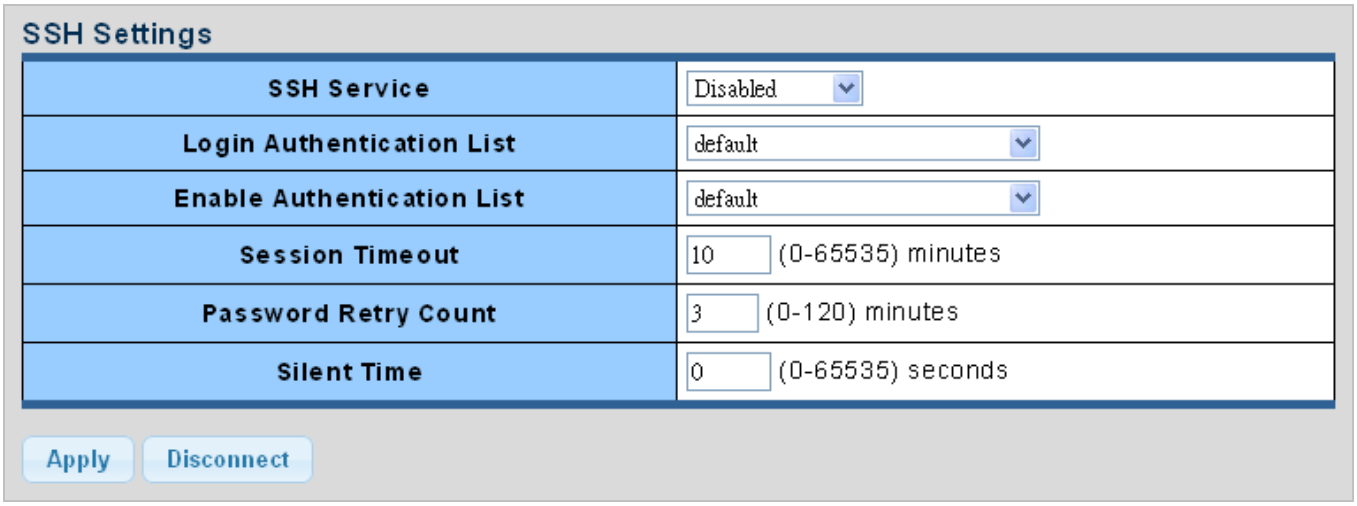


Figure 4-9-23 SSH Settings Screenshot

The page includes the following fields:

Object	Description
• **SSH Service**	Disable or enable SSH service
• **Login Authentication List**	Select login authentication list from this drop-down list
• **Enable Authentication List**	Select enable authentication list from this drop-down list
• **Session Timeout**	Set the session timeout value
• **Password Retry Count**	Set the password retry count value
• **Silent Time**	Set the silent time value

Buttons

Apply: Click to apply changes.

Disconnect: Click to disconnect telnet communication.

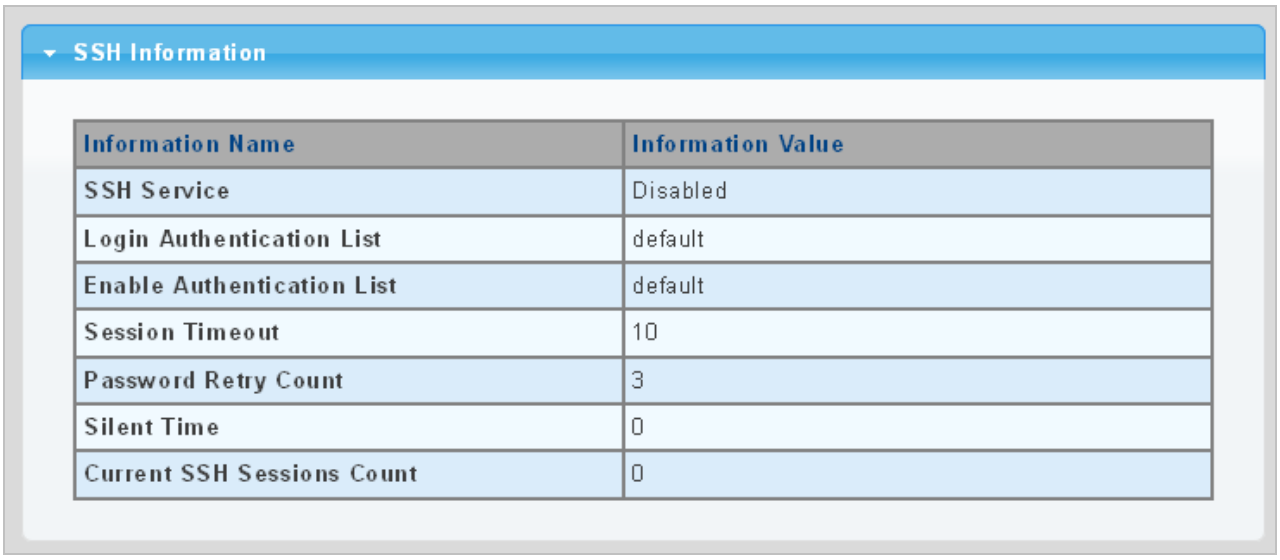


Figure 4-9-24 SSH Information Screenshot

The page includes the following fields:

Object	Description
• **SSH Service**	Display the current SSH service
• **Login Authentication List**	Display the current login authentication list
• **Enable Authentication List**	Display the current enable authentication list
• **Session Timeout**	Display the current session timeout
• **Password Retry Count**	Display the current password retry count
• **Silent Time**	Display the current silent time
• **Current SSH Session Count**	Display the current SSH session count

4.9.5.3 HTTP

The HTTP Settings and Information screens in Figure 4-9-25 and Figure 4-9-26 appear.

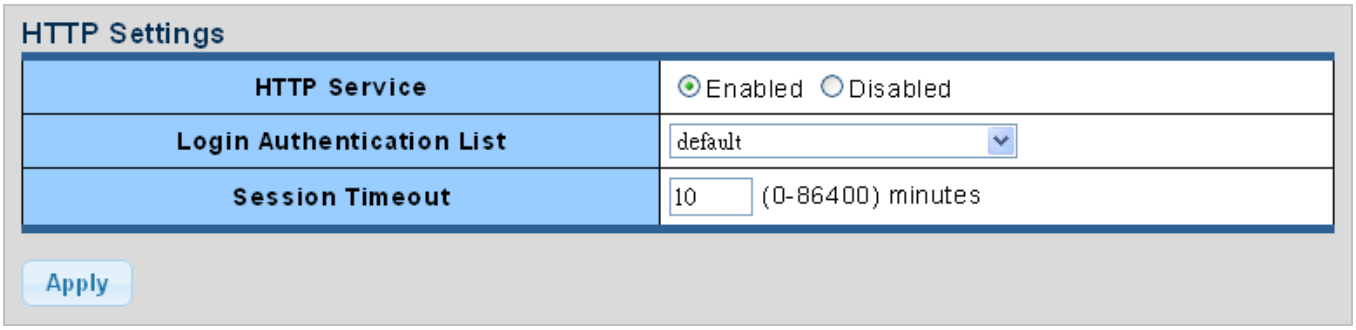


Figure 4-9-25 HTTP Settings Screenshot

The page includes the following fields:

Object	Description
• **HTTP Service**	Disable or enable HTTP service
• **Login Authentication List**	Select login authentication list from this drop-down list
• **Session Timeout**	Set the session timeout value

Buttons

Apply: Click to apply changes.

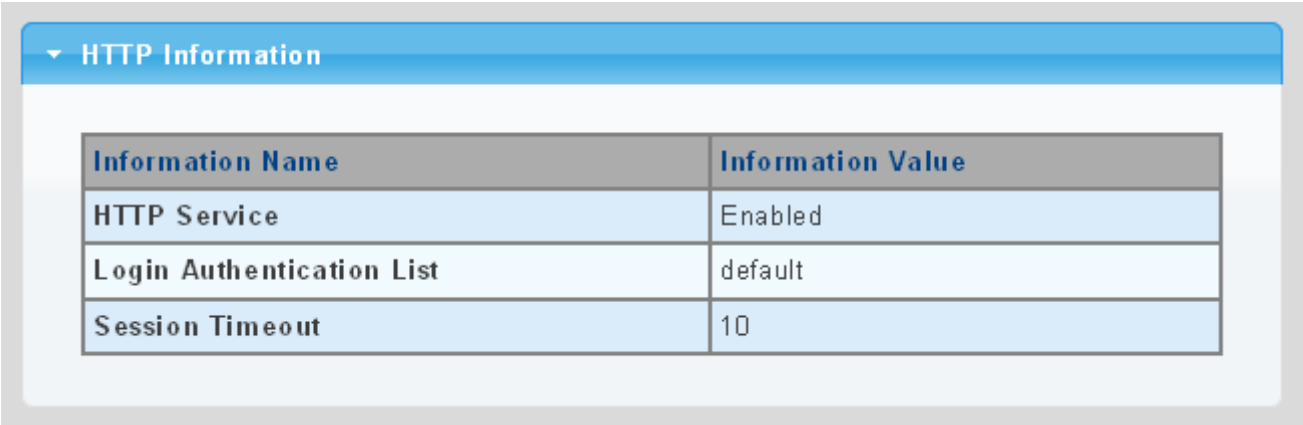


Figure 4-9-26 HTTP Information Screenshot

The page includes the following fields:

Object	Description
• **HTTP Service**	Display the current HTTP service
• **Login Authentication List**	Display the current login authentication list
• **Session Timeout**	Display the current session timeout

4.9.5.4 HTTPs

The HTTPs Settings and Information screen in Figure 4-9-27 and Figure 4-9-28 appear.

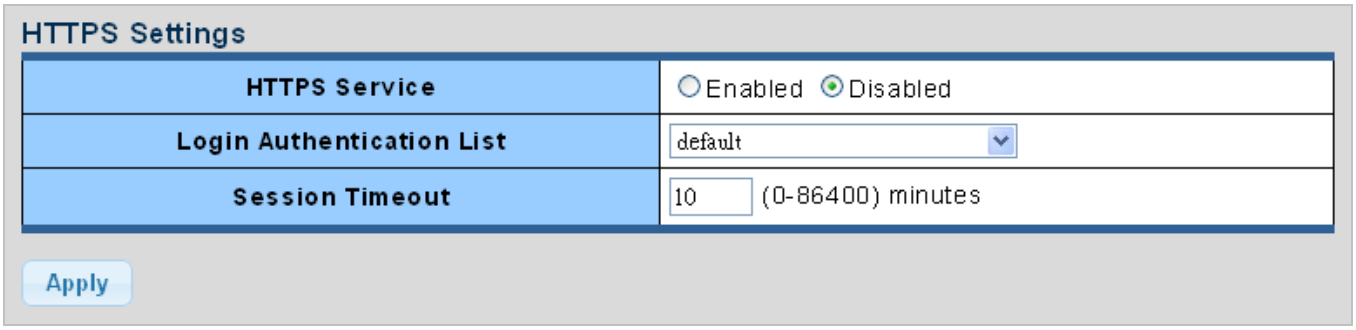


Figure 4-9-27 HTTPs Settings Screenshot

The page includes the following fields:

Object	Description
• **HTTPs Service**	Disable or enable HTTPs service
• **Login Authentication List**	Select login authentication list from this drop-down list
• **Session Timeout**	Set the session timeout value

Buttons

Apply: Click to apply changes.

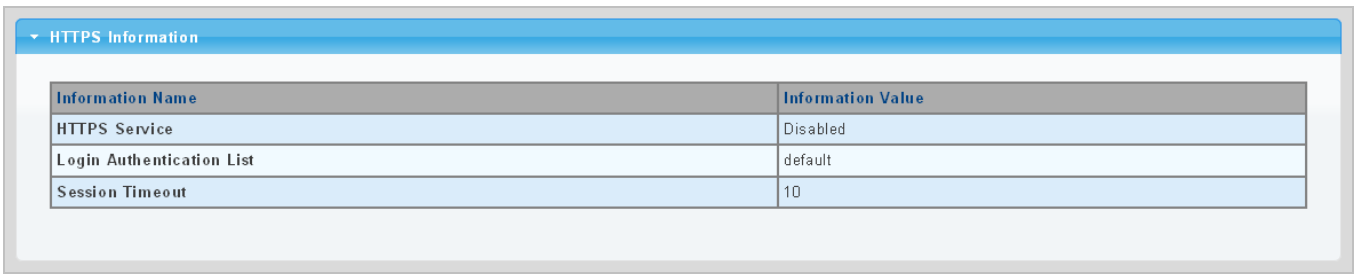


Figure 4-9-28 HTTPs Information Screenshot

The page includes the following fields:

Object	Description
• **HTTPs Service**	Display the current HTTPs service
• **Login Authentication List**	Display the current login authentication list
• **Session Timeout**	Display the current session timeout

4.9.6 Management Access Method

4.9.6.1 Profile Rules

The Profile Rule Table Setting and Table screens in Figure 4-9-29 and Figure 4-9-30 appear.

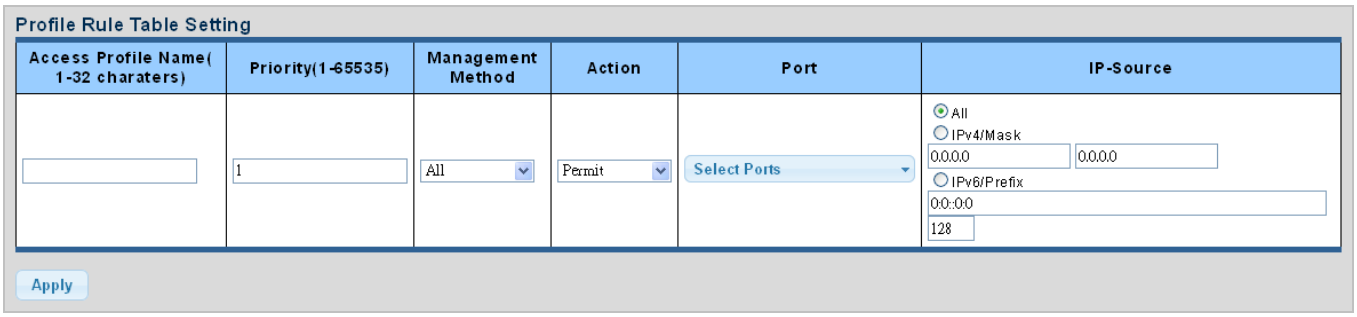


Figure 4-9-29 Profile Rule Table Setting Screenshot

The page includes the following fields:

Object	Description
• **Access Profile Name (1-32 characters)**	Indicates the access profile name
• **Priority (1-65535)**	Set priority The allowed value is from 1 to 65535

• **Management Method**	Indicates the host can access the switch from HTTP/HTTPs/telnet/SSH/SNMP/All interface that the host IP address matched the entry.
• **Action**	An IP address can contain any combination of permit or deny rules. (Default: **Permit** rules)Sets the access mode of the profile; either **permit** or **deny**.
• **Port**	Select port from this drop-down list
• **IP-Source**	Indicates the IP address for the access management entry

Buttons

Apply: Click to apply changes.

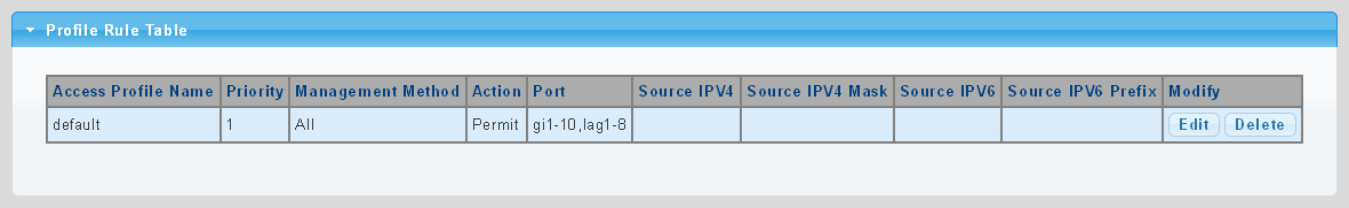


Figure 4-9-30 Profile Rule Table Screenshot

The page includes the following fields:

Object	Description
• **Access Profile Name**	Display the current access profile name
• **Priority**	Display the current priority
• **Management Method**	Display the current management method
• **Action**	Display the current action
• **Port**	Display the current port list
• **Source IPv4**	Display the current source IPv4 address
• **Source IPv4 Mask**	Display the current source IPv4 mask
• **Source IPv6**	Display the current source IPv6 address
• **Source IPv6 Prefix**	Display the current source IPv6 prefix
• **Modify**	Click Edit to edit profile rule parameter Click Delete to delete profile rule entry

4.9.6.2 Access Rules

The access profile screens in Figure 4-9-31 and Figure 4-9-32 appear.

Figure 4-9-31 Access Profile Screenshot

The page includes the following fields:

Object	Description
• **Access Profile**	Select access profile from this drop-down list

Buttons

Apply: Click to apply changes.

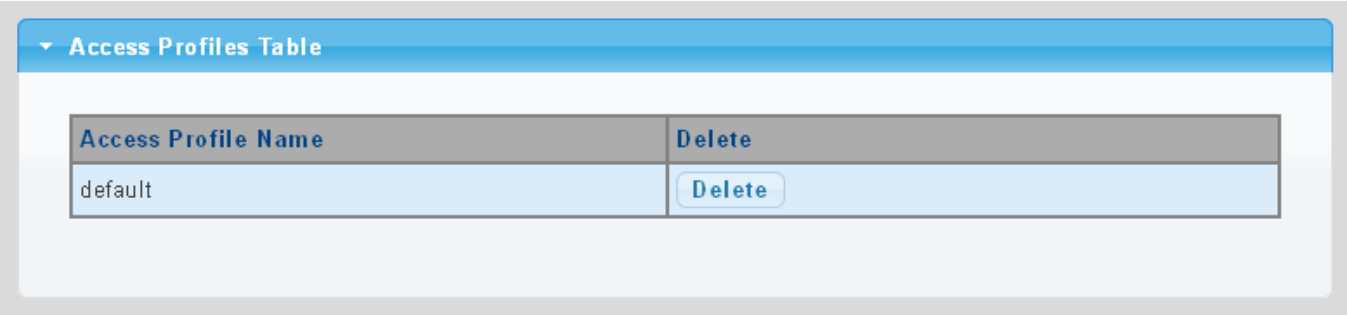


Figure 4-9-32 Access Profile Table Screenshot

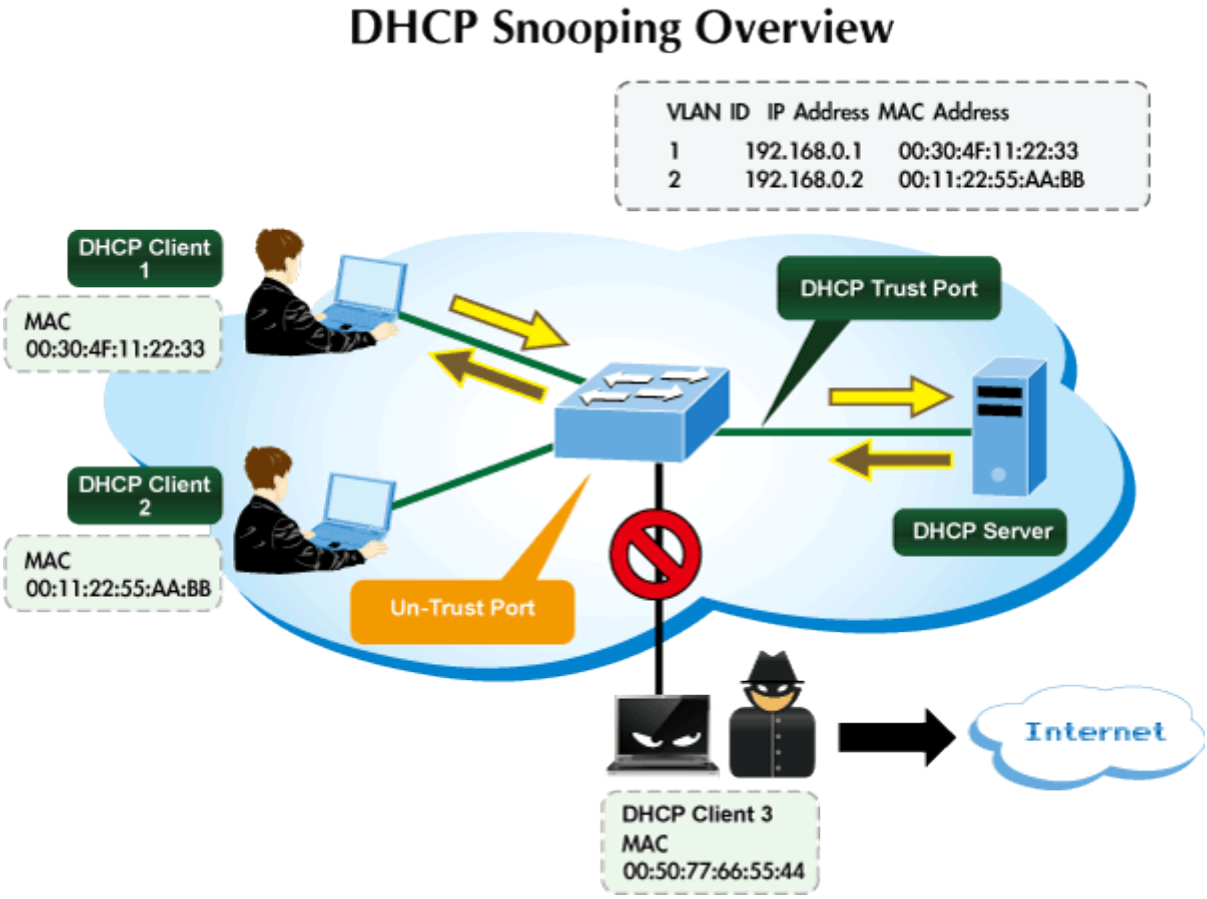
The page includes the following fields:

Object	Description
• **Access Profile**	Display the current access profile
• **Delete**	Click Delete to delete access profile entry

4.9.7 DHCP Snooping

4.9.7.1 DHCP Snooping Overview

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.



Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. **DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall**. When DHCP snooping is enabled globally and enabled on a VLAN interface, **DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped**.
- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- Filtering rules are implemented as follows:

- If the global DHCP snooping is disabled, all DHCP packets are forwarded.
- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:
  - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
  - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
  - If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
  - If the DHCP packet is not a recognizable type, it is dropped.

- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

- Additional considerations when the switch itself is a DHCP client – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

4.9.7.2 Global Setting

DHCP Snooping is used to block intruder on the untrusted ports of switch when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server. Configure DHCP Snooping on this page. The DHCP Snooping Setting and Information screens in Figure 4-9-33 and Figure 4-9-34 appear.

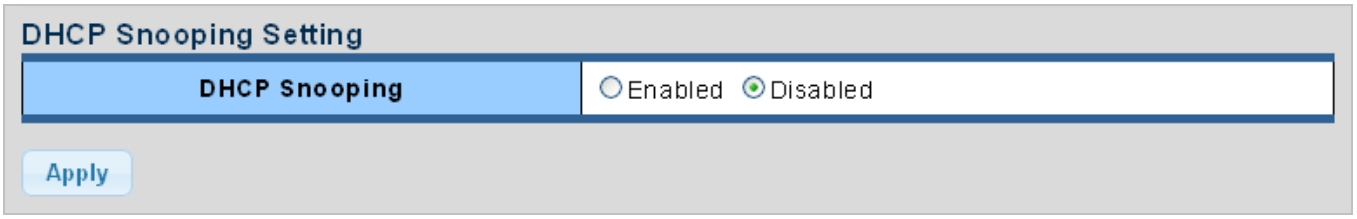


Figure 4-9-33 DHCP Snooping Setting Screenshot

The page includes the following fields:

Object	Description
• **DHCP Snooping**	Indicates the DHCP snooping mode operation. Possible modes are: ■ **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ■ **Disabled**: Disable DHCP snooping mode operation.

Buttons

Apply: Click to apply changes.

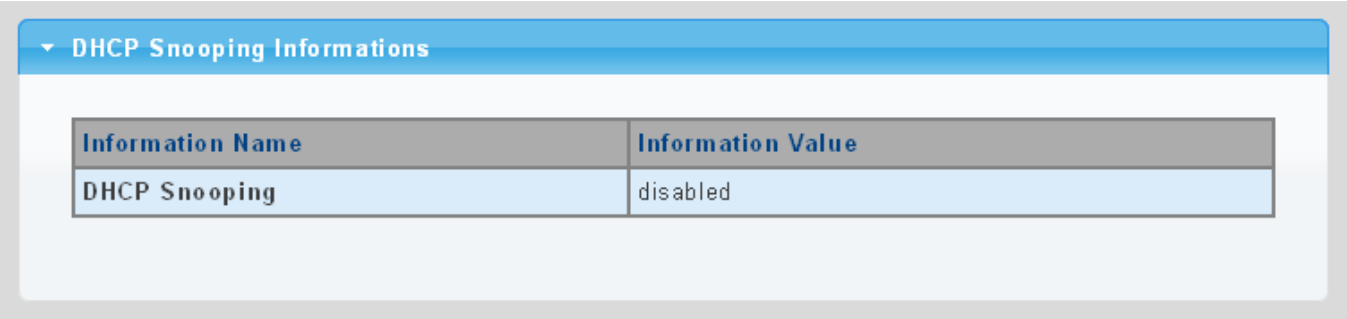


Figure 4-9-34 DHCP Snooping Information Screenshot

The page includes the following fields:

Object	Description
• **DHCP Snooping**	Display the current DHCP snooping status

4.9.7.3 DHCP Snooping VLAN Setting

Command Usage

- 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.
- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
- When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

The DHCP Snooping VLAN Setting screens in Figure 4-9-35 and Figure 4-9-36 appear.

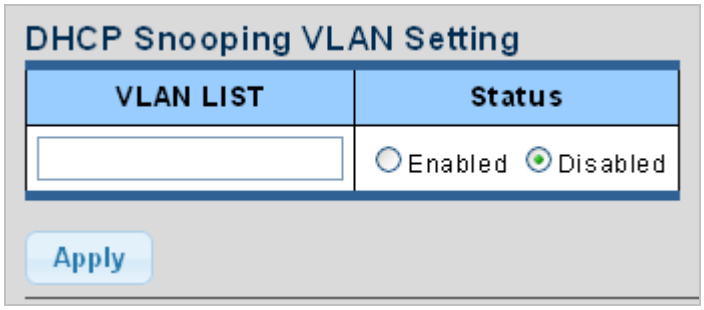


Figure 4-9-35 DHCP Snooping VLAN Setting Screenshot

The page includes the following fields:

Object	Description
• **VLAN List**	Indicates the ID of this particular VLAN.
• **Status**	Indicates the DHCP snooping mode operation. Possible modes are: ■ **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ■ **Disabled**: Disable DHCP snooping mode operation.

Buttons

Apply: Click to apply changes.

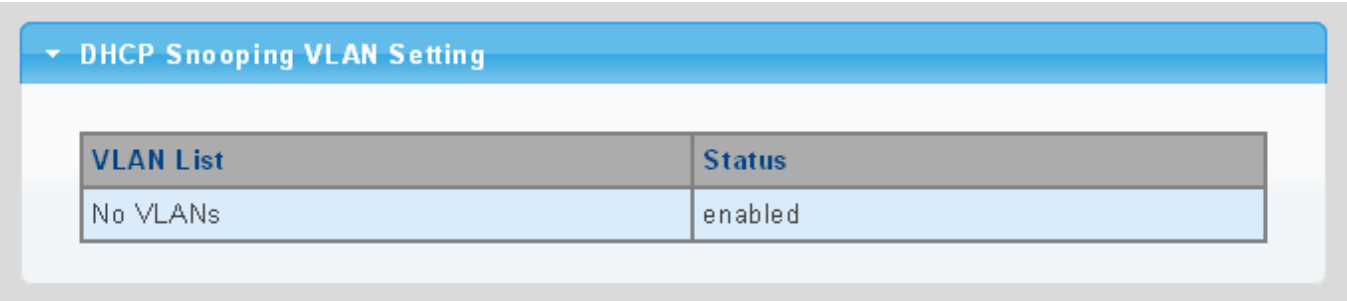


Figure 4-9-36 DHCP Snooping VLAN Setting Screenshot

The page includes the following fields:

Object	Description
• **VLAN List**	Display the current VLAN list
• **Status**	Display the current DHCP snooping status

4.9.7.4 Port Setting

Configures switch ports as trusted or untrusted.

Command Usage

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.
- When DHCP snooping enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- Set all ports connected to DHCP servers within the local network or firewall to trusted state. Set all other ports outside the local network or firewall to untrusted state.

The DHCP Snooping Port Setting screen in Figure 4-9-37 and Figure 4-9-38 appears.

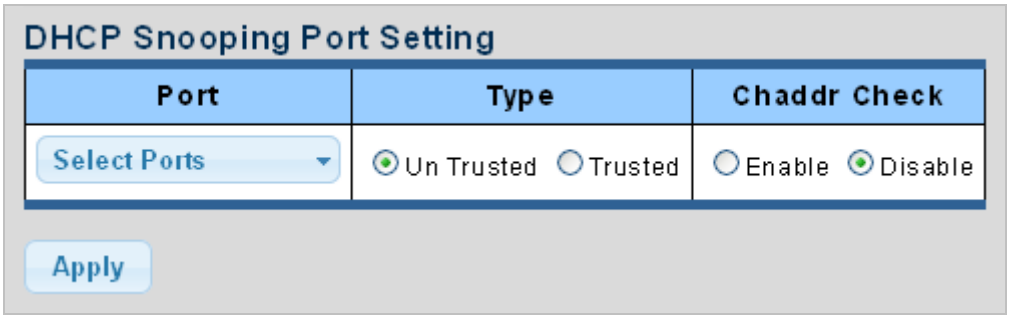


Figure 4-9-37 DHCP Snooping Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **Type**	Indicates the DHCP snooping port mode. Possible port modes are: ■ **Trusted**: Configures the port as trusted sources of the DHCP message. ■ **Untrusted**: Configures the port as untrusted sources of the DHCP message.
• **Chaddr Check**	Indicates that the Chaddr check function is enabled on selected port. Chaddr: Client hardware address.

Buttons

Apply: Click to apply changes.

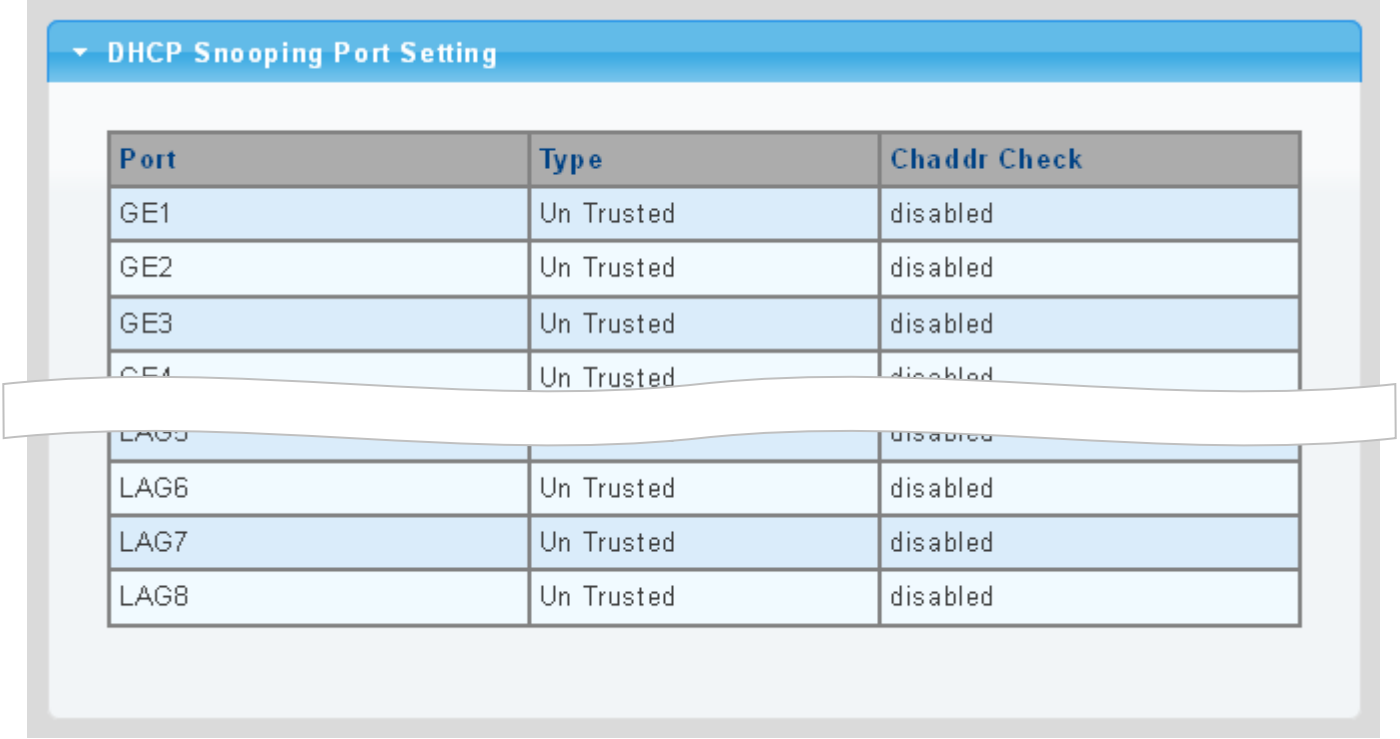


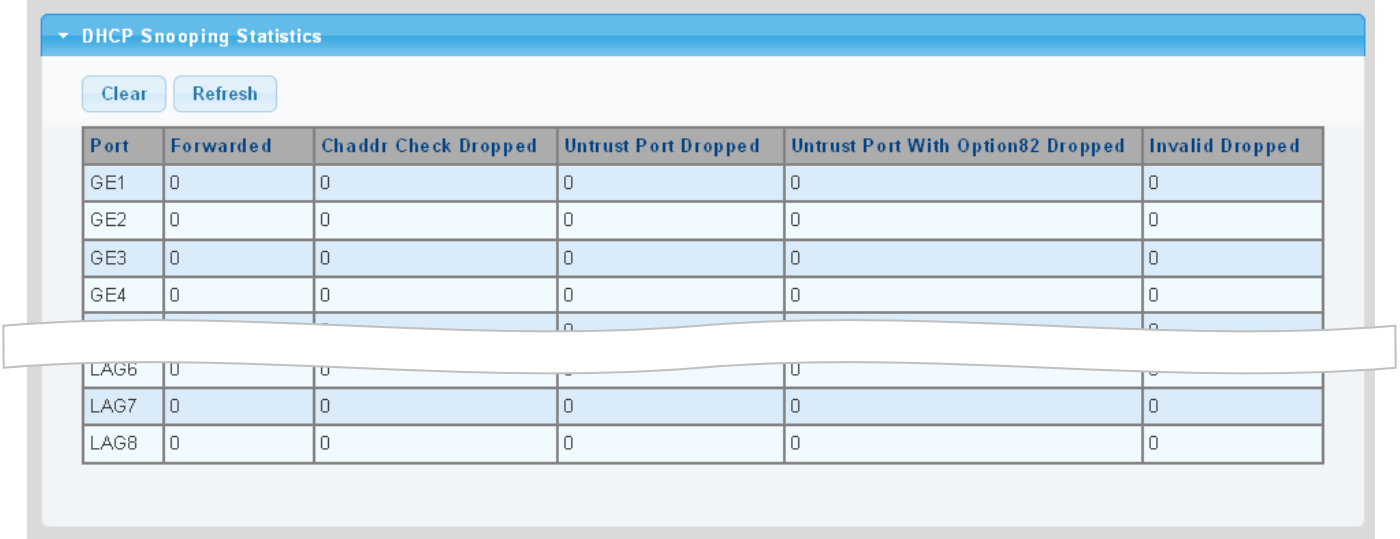
Figure 4-9-38 DHCP Snooping Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Type**	Display the current type
• **Chaddr Check**	Display the current chaddr check

4.9.7.5 Statistics

The DHCP Snooping Statistics screen in Figure 4-9-39 appears.



Port	Forwarded	Chaddr Check Dropped	Untrust Port Dropped	Untrust Port With Option82 Dropped	Invalid Dropped
GE1	0	0	0	0	0
GE2	0	0	0	0	0
GE3	0	0	0	0	0
GE4	0	0	0	0	0
LAG6	0	0	[illegible]	0	[illegible]
LAG7	0	0	0	0	0
LAG8	0	0	0	0	0

Figure 4-9-39 DHCP Snooping Statistics Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Forwarded**	Display the current forwarded
• **Chaddr Check Dropped**	Display the chaddr check dropped
• **Untrust Port Dropped**	Display untrust port dropped
• **Untrust Port with Option82 Dropped**	Display untrust port with option82 dropped
• **Invalid Dropped**	Display invalid dropped

Buttons

Clear: Click to clear the statistics.

Refresh: Click to refresh the statistics.

4.9.7.6 Database Agent

Overview of the DHCP Snooping Database Agent

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 8192 bindings.

Each database entry (*binding*) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. A *checksum* value, the end of each entry, is the number of bytes from the start of the file to end of the entry. Each entry is 72 bytes, followed by a space and then the checksum value.

To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DCHP spoofing attacks.

The database agent stores the bindings in a file at a configured location. When reloading, the switch reads the binding file to build the DHCP snooping binding database. The switch keeps the file current by updating it when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

The DHCP Snooping Database and Information screens in Figure 4-9-40 and Figure 4-9-41 appear.

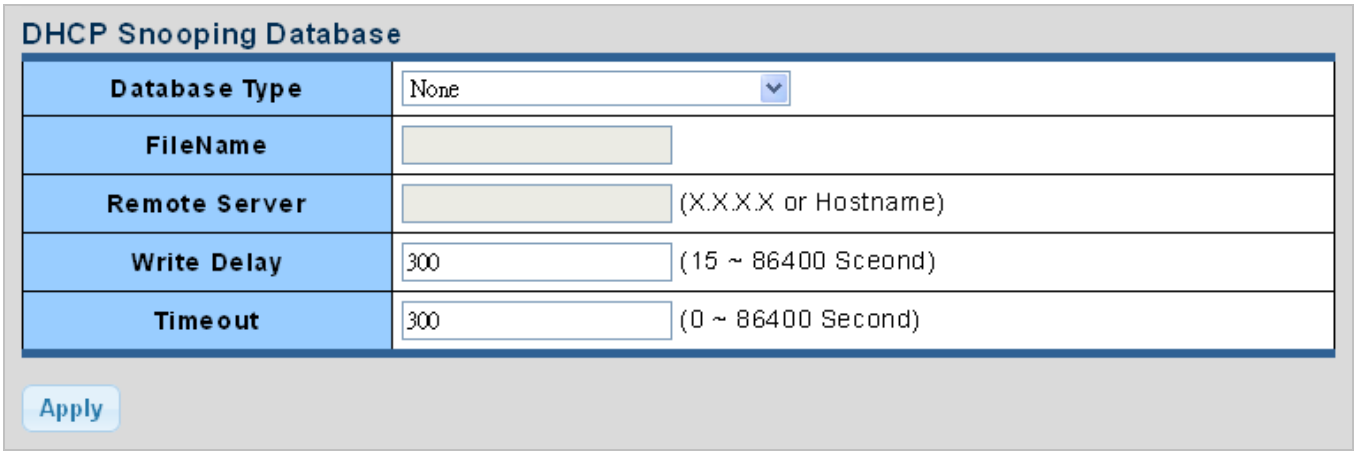


Figure 4-9-40 DHCP Snooping Database Setting Screenshot

The page includes the following fields:

Object	Description
• **Database Type**	Select database type
• **File Name**	The name of file image

• **Remote Server**	Fill in your remote server IP address
• **Write Delay**	Specify the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes).
• **Timeout**	Specify when to stop the database transfer process after the binding database changes. The range is from 0 to 86400. Use 0 for an infinite duration. The default is 300 seconds (5 minutes).

Buttons

Apply: Click to apply changes.

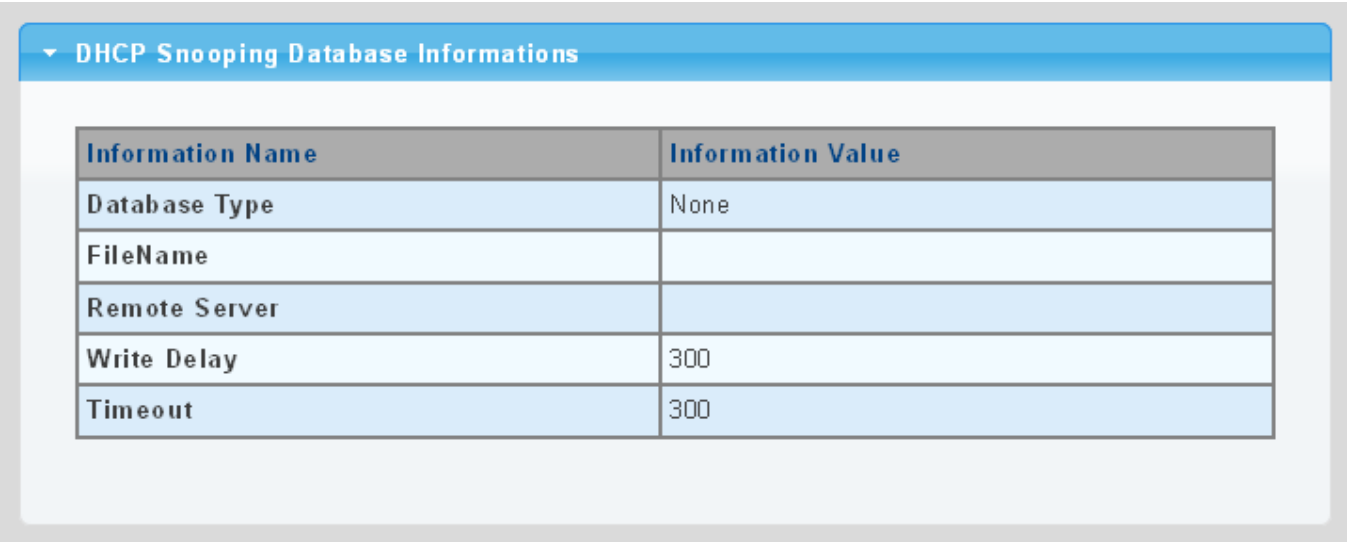


Figure 4-9-41 DHCP Snooping Database Information Screenshot

The page includes the following fields:

Object	Description
• **Database Type**	Display the current database type
• **File Name**	Display the current file name
• **Remote Server**	Display the current remote server
• **Write Delay**	Display the current write delay
• **Timeout**	Display the current timeout

4.9.7.7 Rate Limit

After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The DHCP Rate Limit Setting and Config screens in Figure 4-9-42 and Figure 4-9-43 appear.

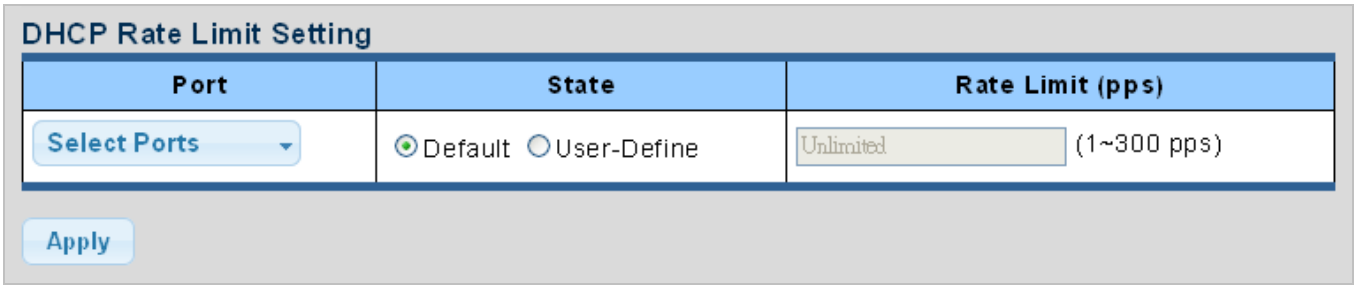


Figure 4-9-42 DHCP Rate Limit Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **State**	Set default or user-define
• **Rate Limit (pps)**	Configure the rate limit for the port policer. The default value is "unlimited". Valid values are in the range from 1 to 300.

Buttons

Apply: Click to apply changes

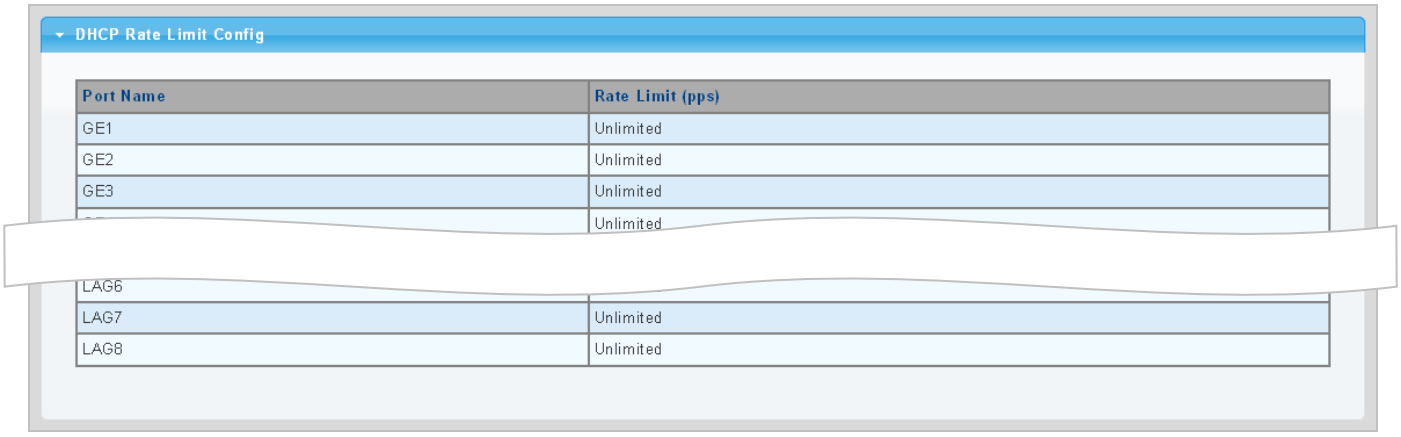


Figure 4-9-43 DHCP Rate Limit Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Rate Limit (pps)**	Display the current rate limit

4.9.7.8 Option82 Global Setting

DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to DHCP servers. Known as **DHCP Option 82**, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.

The **DHCP option 82** enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options:

- Circuit ID (option 1)
- Remote ID (option2).

The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on.
The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The DHCP Rate Limit Setting and Config screens in Figure 4-9-44 and Figure 4-9-45 appear.

Figure 4-9-44 Option82 Global Setting Screenshot

The page includes the following fields:

Object	Description
• **State**	Set the option2 (remote ID option) content of option 82 added by DHCP request packets. ■ **Default** means the default VLAN MAC format. ■ **User-Define** means the remote-id content of option 82 specified by users

Buttons

Apply: Click to apply changes.

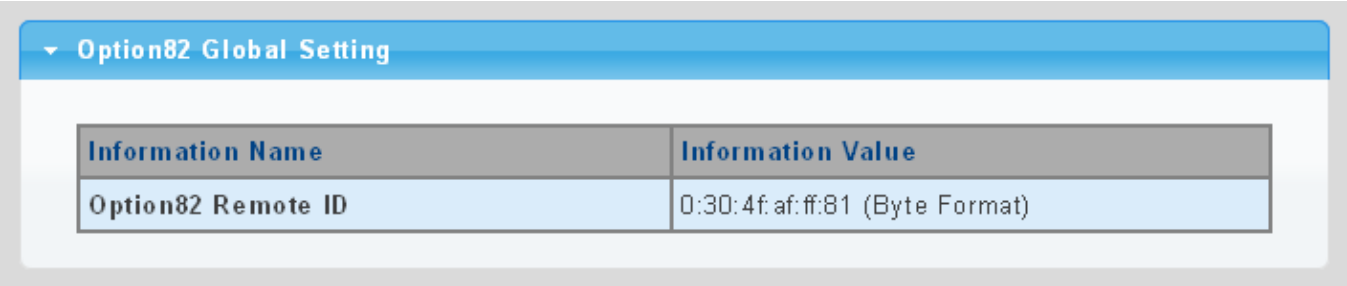


Figure 4-9-45 Option82 Global Setting Screenshot

The page includes the following fields:

Object	Description
• **Option82 Remote ID**	Display the current option82 remote ID

4.9.7.9 Option82 Port Setting

This function is used to set the retransmitting policy of the system for the received DHCP request message which contains option82.

- The **drop** mode means that if the message has option82, then the system will drop it without processing.
- The **keep** mode means that the system will keep the original option82 segment in the message, and forward it to the server to process
- The **replace** mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process.

Option82 Port Setting screens in Figure 4-9-46 and Figure 4-9-47 appear.

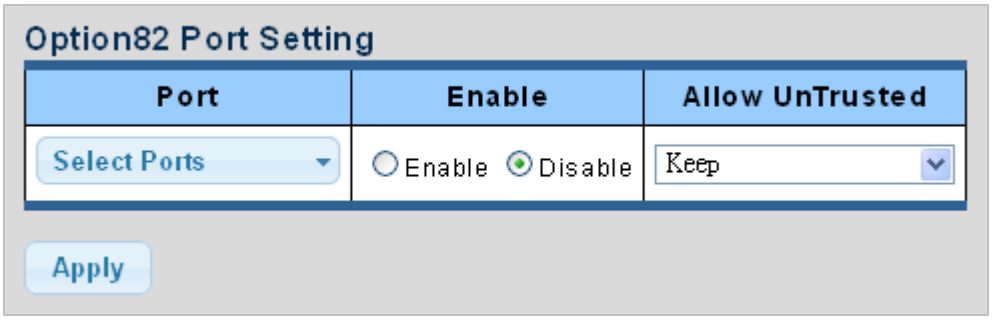


Figure 4-9-46 Option82 Global Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **Enable**	Enable or disable option82 function on port
• **Allow Untrusted**	Select modes from this drop-down list. The following modes are available: ■ **Drop** ■ **Keep** ■ **Replace**

Buttons

Apply: Click to apply changes.

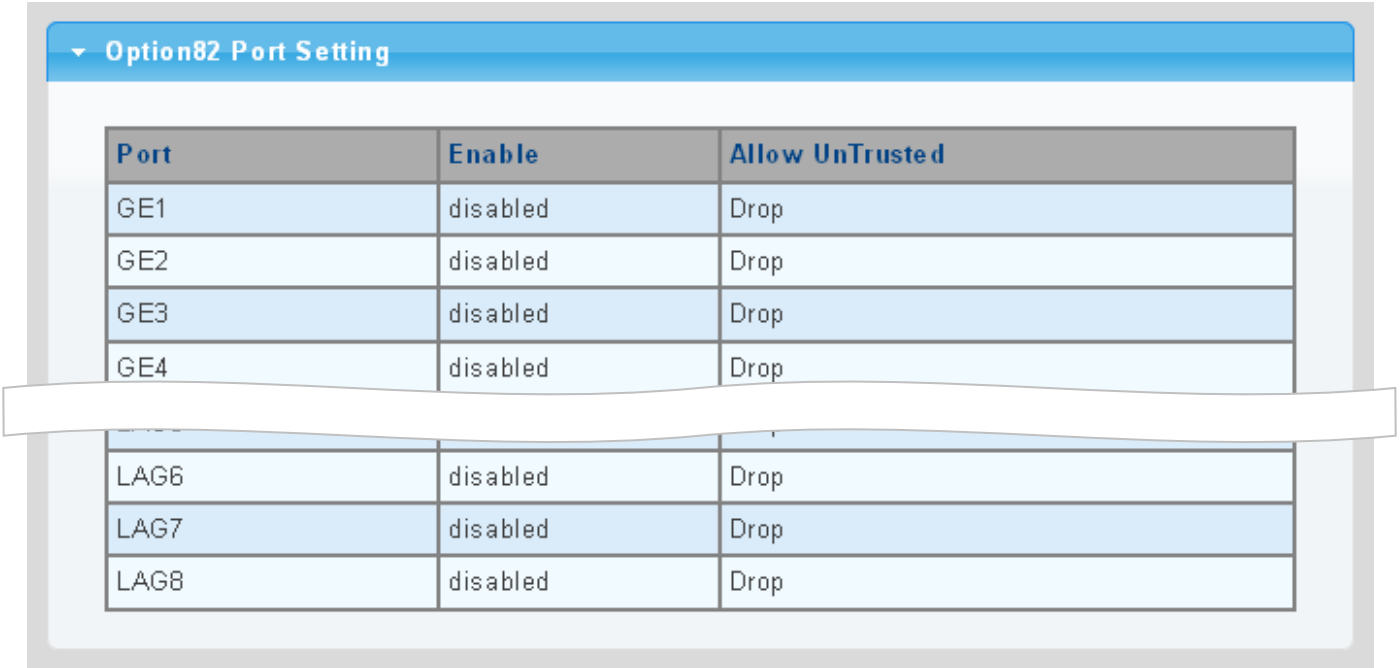


Figure 4-9-47 Option82 Global Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Enable**	Display the current status
• **Allow Untrusted**	Display the current untrusted mode

4.9.7.10 Option82 Circuit-ID Setting

Set creation method for option82, users can define the parameters of circuit-id suboption by themselves. Option82 Circuit-ID Setting screens in Figure 4-9-48 and Figure 4-9-49 appear.

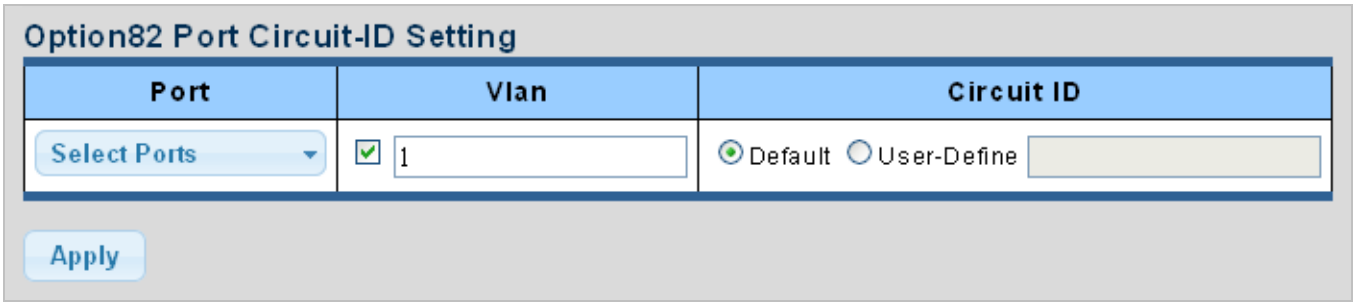


Figure 4-9-48 Option82 Port Circuit-ID Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **VLAN**	Indicates the ID of this particular VLAN
• **Circuit ID**	Set the option1 (Circuit ID) content of option 82 added by DHCP request packets

Buttons

Apply: Click to apply changes.

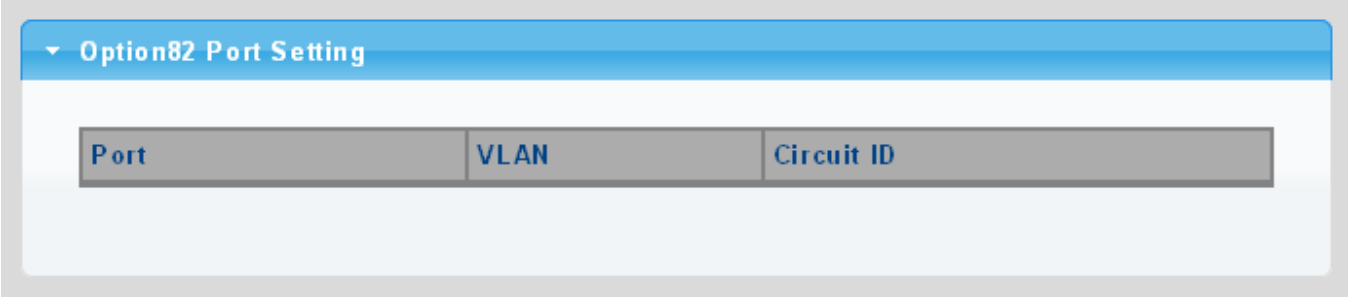


Figure 4-9-49 Option82 Port Circuit-ID Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Display the current port
• **VLAN**	Display the current VLAN
• **Circuit ID**	Display the current circuit ID

4.9.8 Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT. This page provides ARP Inspection related configuration.

Note

A Dynamic ARP prevents the untrust ARP packets based on the DHCP Snooping Database.

4.9.8.1 Global Setting

DAI Setting and Information screens in Figure 4-9-50 and Figure 4-9-51 appear.

Figure 4-9-50 DAI Setting Screenshot

The page includes the following fields:

Object	Description
• **DAI**	Enable the Global Dynamic ARP Inspection or disable the Global ARP Inspection

Buttons

Apply: Click to apply changes.

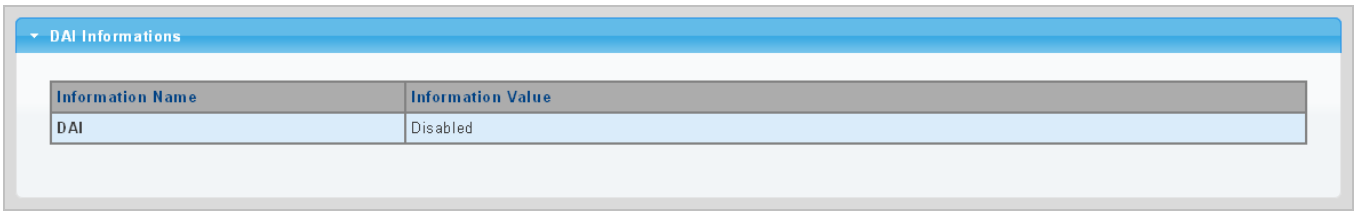


Figure 4-9-51 DAI Information Screenshot

The page includes the following fields:

Object	Description
• **DAI**	Display the current DAI status

4.9.8.2 VLAN Setting

DAI VLAN Setting screens in Figure 4-9-52 and Figure 4-9-53 appear.

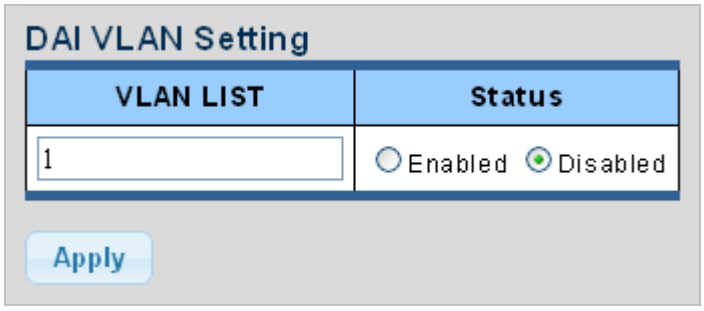


Figure 4-9-52 DAI VLAN Setting Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Indicates the ID of this particular VLAN
Status	Enables Dynamic ARP Inspection on the specified VLAN Options: ■ **Enable** ■ **Disable**

Buttons

Apply: Click to apply changes.

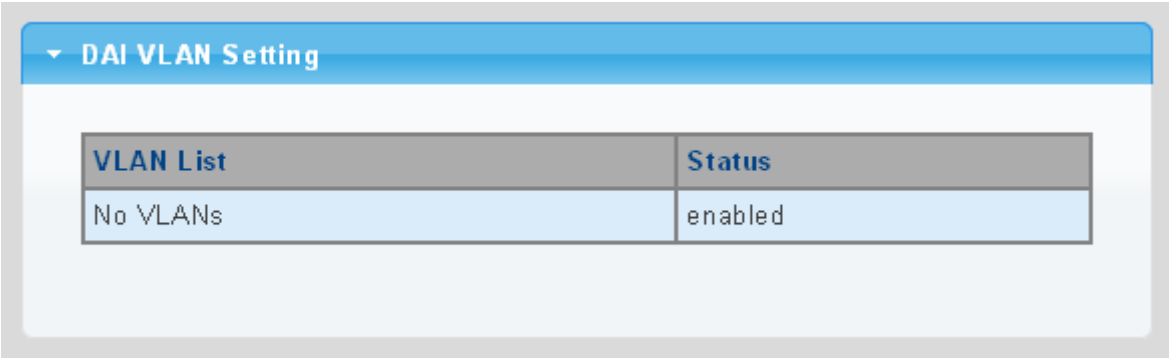


Figure 4-9-53 DAI VLAN Setting Screenshot

The page includes the following fields:

Object	Description
• **VLAN List**	Display the current VLAN list
• **Status**	Display the current status

4.9.8.3 Port Setting

Configures switch ports as DAI trusted or untrusted and check mode. DAI Port Setting screens in Figure 4-9-54 and Figure 4-9-55 appear.

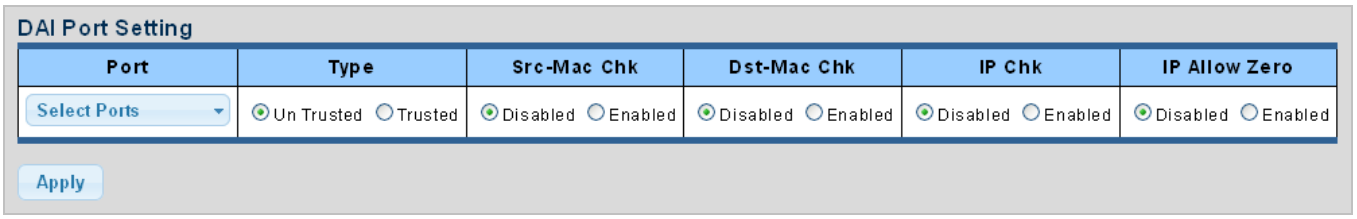


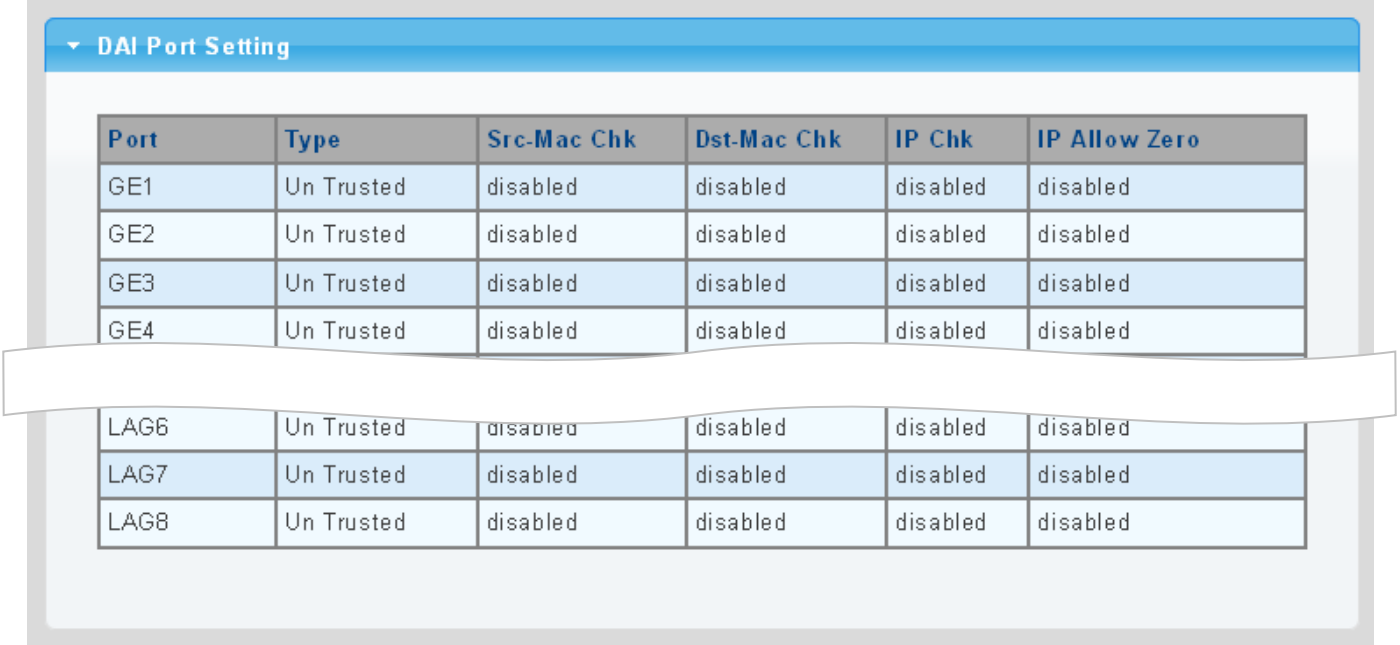
Figure 4-9-54 DAI Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **Type**	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Default: All interfaces are untrusted.
• **Src-Mac Chk**	Enable or disable to checks 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. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
• **Dst-Mac Chk**	Enable or disable to checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
• **IP Chk**	Enable or disable to checks the source and destination IP addresses of ARP packets. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.
• **IP Allow Zero**	Enable or disable to checks all-zero IP addresses.

Buttons

Apply: Click to apply changes.



DAI Port Setting

Port	Type	Src-Mac Chk	Dst-Mac Chk	IP Chk	IP Allow Zero
GE1	Un Trusted	disabled	disabled	disabled	disabled
GE2	Un Trusted	disabled	disabled	disabled	disabled
GE3	Un Trusted	disabled	disabled	disabled	disabled
GE4	Un Trusted	disabled	disabled	disabled	disabled
LAG6	Un Trusted	disabled	disabled	disabled	disabled
LAG7	Un Trusted	disabled	disabled	disabled	disabled
LAG8	Un Trusted	disabled	disabled	disabled	disabled

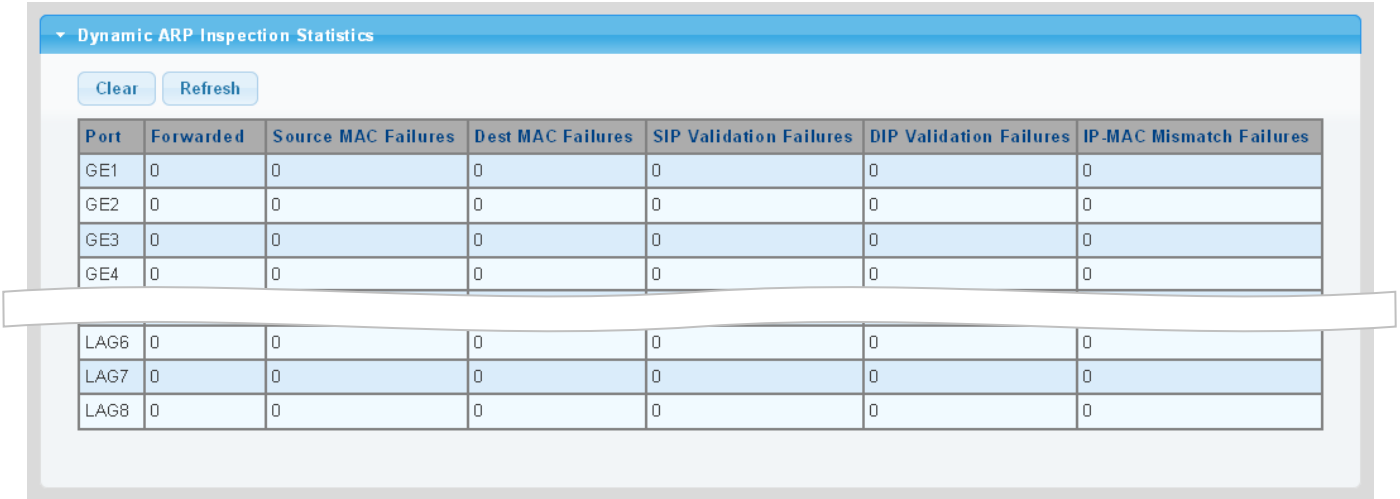
Figure 4-9-55 DAI Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Type**	Display the current port type
• **Src-Mac Chk**	Display the current Src-Mac Chk status
• **Dst-Mac Chk**	Display the current Dst-Mac Chk status
• **IP Chk**	Display the current IP Chk status
• **IP Allow Zero**	Display the current IP allow zero status

4.9.8.4 Statistics

Configures switch ports as DAI trusted or untrusted and check mode. DAI Port Setting screen in Figure 4-9-56 appears.



Port	Forwarded	Source MAC Failures	Dest MAC Failures	SIP Validation Failures	DIP Validation Failures	IP-MAC Mismatch Failures
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
GE4	0	0	0	0	0	0
LAG6	0	0	0	0	0	0
LAG7	0	0	0	0	0	0
LAG8	0	0	0	0	0	0

Figure 4-9-56 DAI Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Forwarded**	Display the current forwarded
Source MAC Failures	Display the current source MAC failures
• **Dest MAC Failures**	Display the current source MAC failures
• **SIP Validation Failures**	Display the current SIP Validation failures
• **DIP Validation Failures**	Display the current DIP Validation failures
• **IP-MAC Mismatch Failures**	Display the current IP-MAC mismatch failures

Buttons

Clear: Click to clear the statistics.

Refresh: Click to refresh the statistics.

4.9.8.5 Rate Limit

The ARP Rate Limit Setting and Config screens in Figure 4-9-57 and Figure 4-9-58 appear.

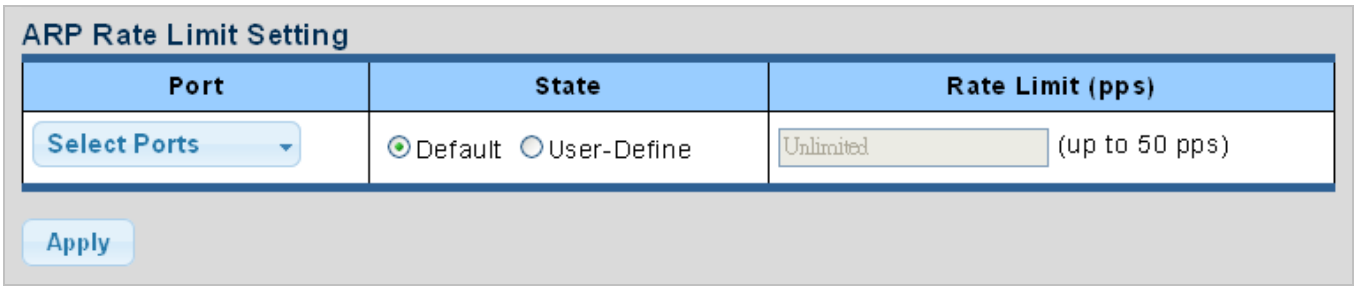


Figure 4-9-57 ARP Rate Limit Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **State**	Set default or user-define
• **Rate Limit (pps)**	Configure the rate limit for the port policer. The default value is "unlimited".

Buttons

Apply: Click to apply changes.

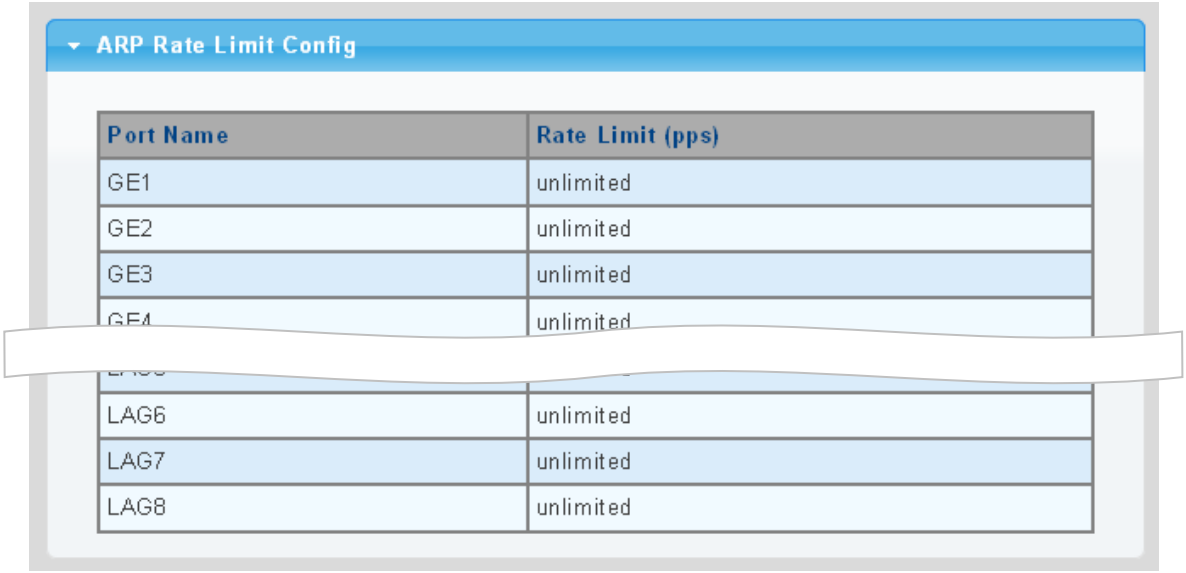


Figure 4-9-58 ARP Rate Limit Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Rate Limit (pps)**	Display the current rate limit

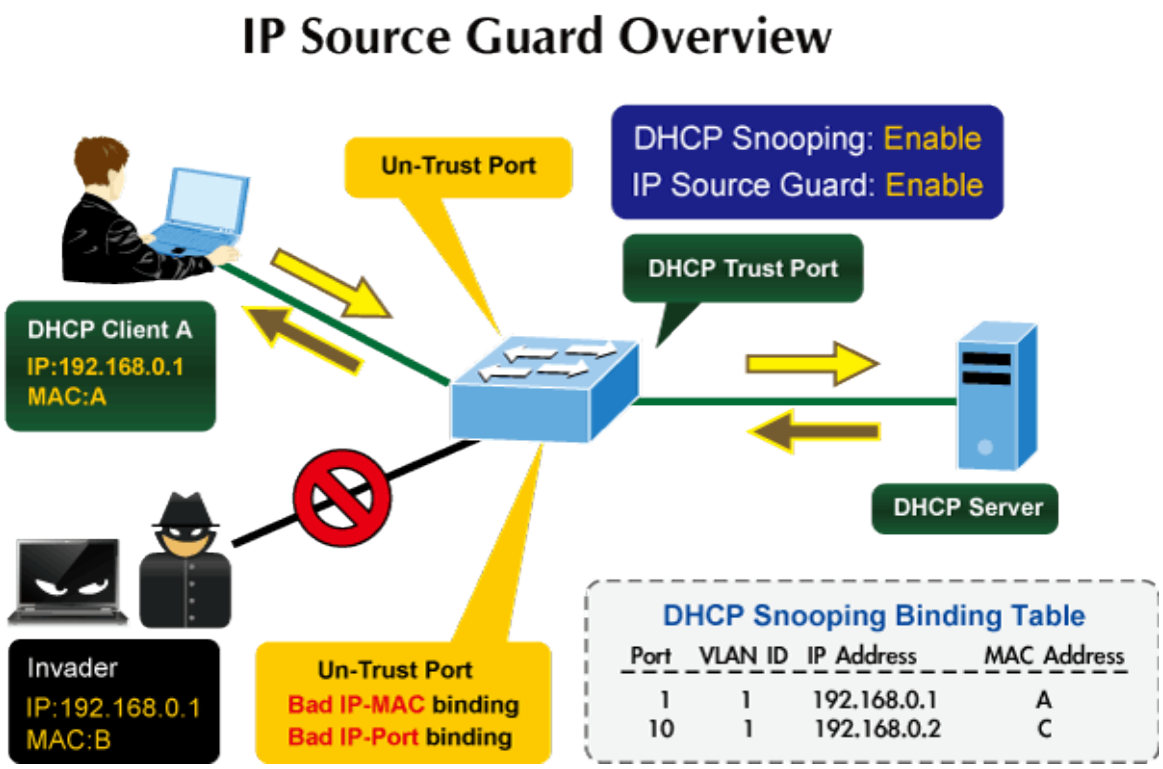
4.9.9 IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

After receiving a packet, the port looks up the key attributes (including IP address, MAC address and VLAN tag) of the packet in the binding entries of the IP source guard. If there is a matching entry, the port will forward the packet. Otherwise, the port will abandon the packet.

IP source guard filters packets based on the following types of binding entries:

- IP-port binding entry
- MAC-port binding entry
- IP-MAC-port binding entry



4.9.9.1 Port Settings

IP Source Guard is a secure feature used to restrict IP traffic on **DHCP snooping untrusted ports** by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

The IP Source Guard Port Setting and Information screens in Figure 4-9-60 and Figure 4-9-61 appear.

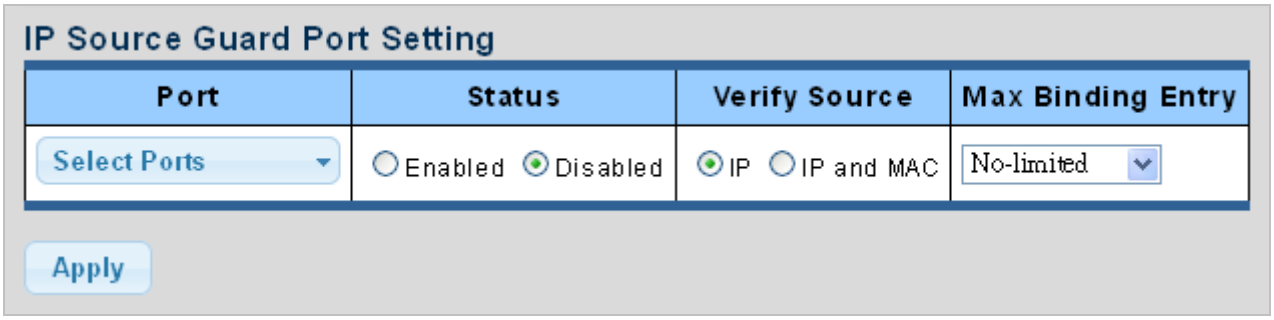


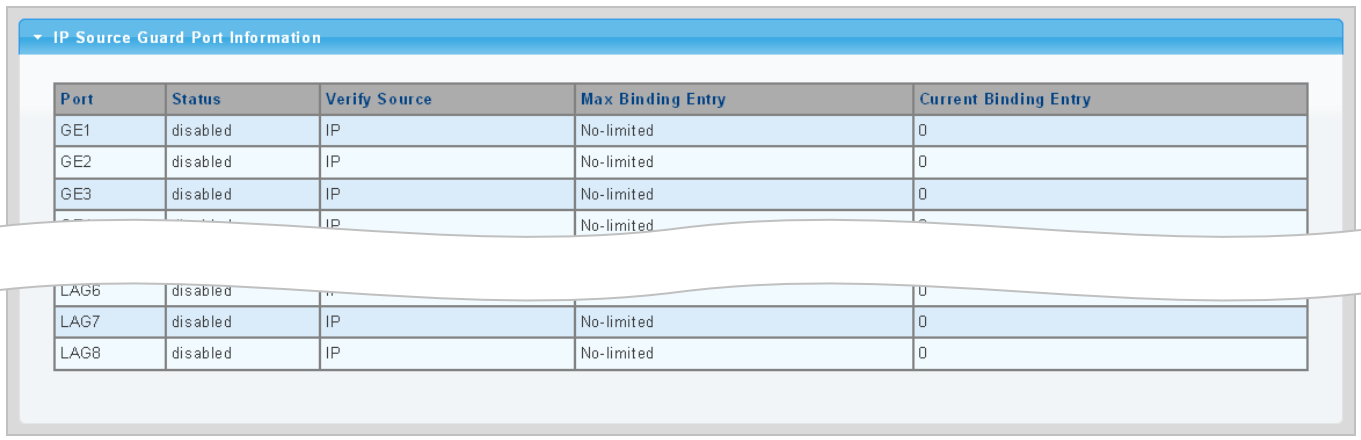
Figure 4-9-60 IP Source Guard Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **Status**	Enable or disable the IP source guard
• **Verify Source**	Configures the switch to filter inbound traffic based IP address, or IP address and MAC address. ■ **None** Disables IP source guard filtering on the Managed Switch. ■ **IP** Enables traffic filtering based on IP addresses stored in the binding table. ■ **IP and MAC** Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.
• **Max Binding Entry**	The maximum number of IP source guard that can be secured on this port

Buttons

Apply: Click to apply changes.



IP Source Guard Port Information

Port	Status	Verify Source	Max Binding Entry	Current Binding Entry
GE1	disabled	IP	No-limited	0
GE2	disabled	IP	No-limited	0
GE3	disabled	IP	No-limited	0
[illegible]	[illegible]	IP	No-limited	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
LAG6	disabled	[illegible]	[illegible]	0
LAG7	disabled	IP	No-limited	0
LAG8	disabled	IP	No-limited	0

Figure 4-9-61 IP Source Guard Port Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Status**	Display the current status
• **Verify Source**	Display the current verify source
• **Max Binding Entry**	Display the current max binding entry
• **Current Binding Entry**	Display the current binding entry

4.9.9.2 Binding Table

The IP Source Guard Static Binding Entry and Table Status screens in Figure 4-9-62 and Figure 4-9-63 appear.

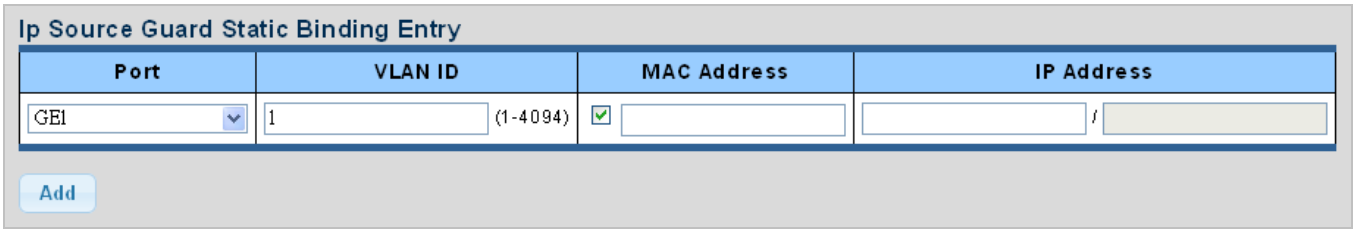


Figure 4-9-62 IP Source Guard Static Binding Entry Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **VLAN ID**	Indicates the ID of this particular VLAN
• **MAC Address**	Sourcing MAC address is allowed
• **IP Address**	Sourcing IP address is allowed

Buttons

Add: Click to add authentication list

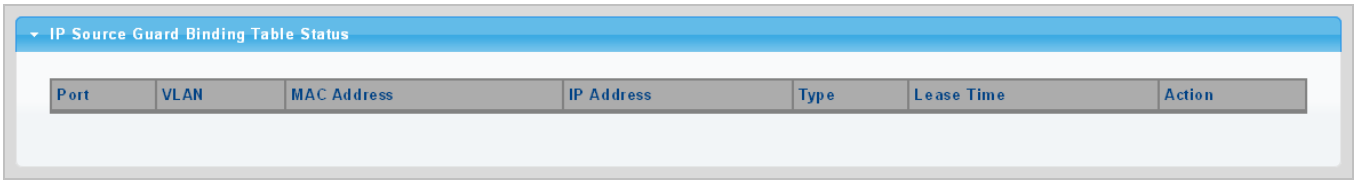


Figure 4-9-63 IP Source Guard Binding Table Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	Display the current port
• **VLAN ID**	Display the current VLAN
• **MAC Address**	Display the current MAC address
• **IP Address**	Display the current IP Address
• **Type**	Display the current entry type
• **Lease Time**	Display the current lease time
• **Action**	Click Delete to delete IP source guard binding table status entry

4.9.10 Port Security

This page allows you to configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of four different as described below.

The Limit Control module is one of the modules that utilize a lower-layer module while the Port Security module manages MAC addresses learned on the port.

The Limit Control configuration consists of two sections, a system- and a port-wid. The IP Source Guard Static Binding Entry and Table Status screens in Figure 4-9-64 and Figure 4-9-65 appear.

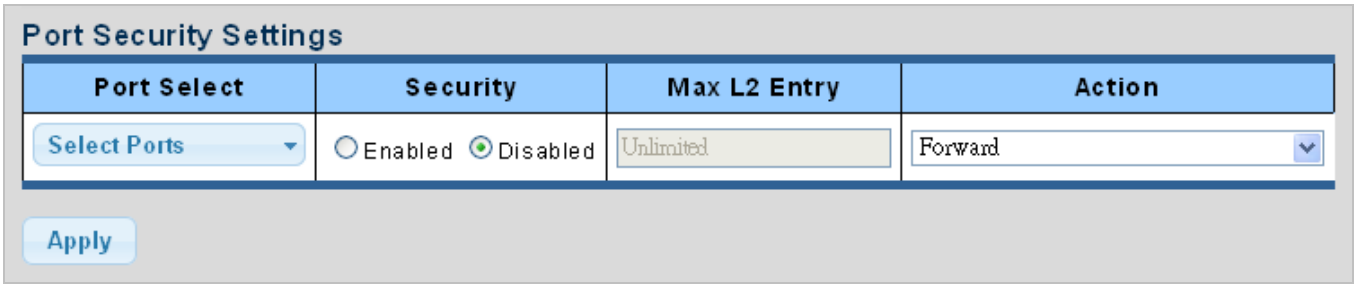


Figure 4-9-64 Port Security Setting Screenshot

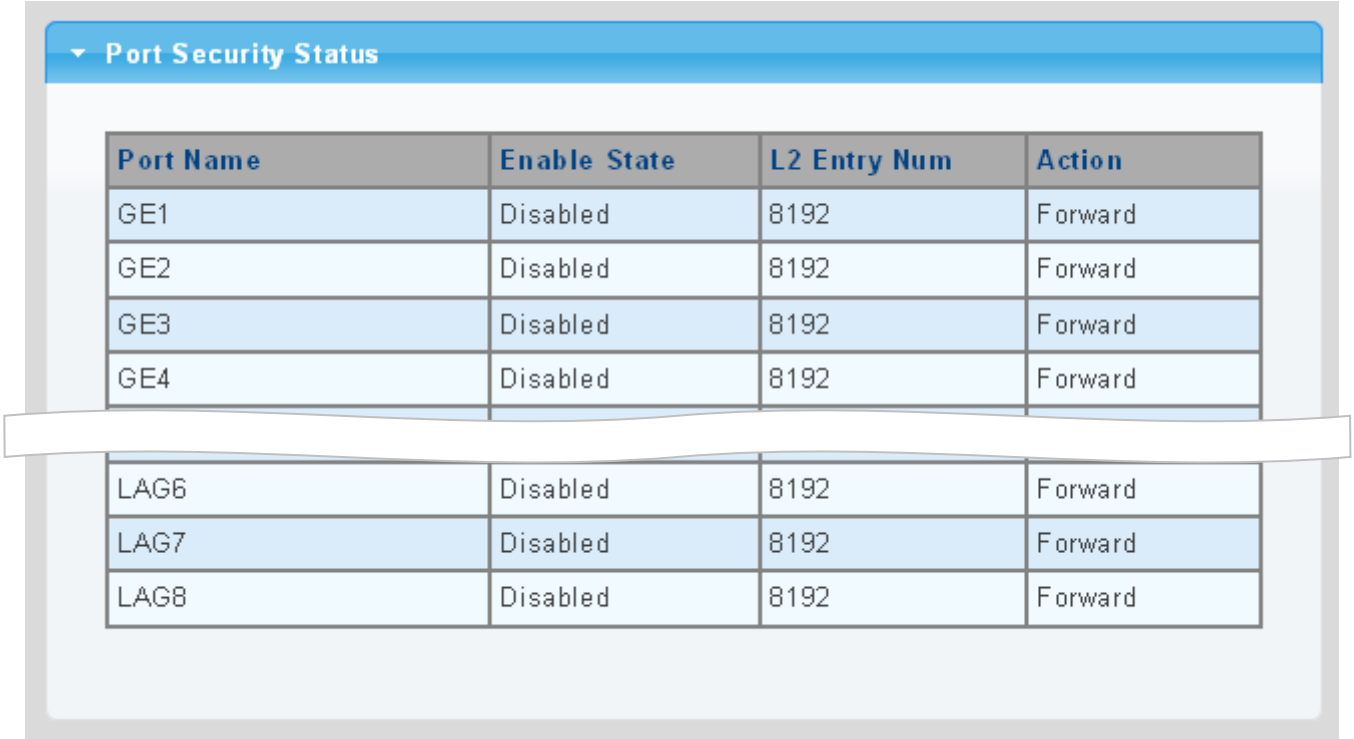
The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **Security**	Enable or disable the port security
• **Mac L2 Entry**	The maximum number of MAC addresses that can be secured on this port. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
• **Action**	If Limit is reached, the switch can take one of the following actions: ■ **Forward**: Do not allow more than Limit MAC addresses on the port, but take no further action. ■ **Shutdown**: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new will be learned. Even if the link is physically disconnected

	and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Disable and re-enable Limit Control on the port or the switch, 2) Click the Reopen button. ■ **Discard**: If Limit + 1 MAC addresses is seen on the port, it will trigger the action that do not learn the new MAC and drop the package.

Buttons

Apply: Click to apply changes.



Port Name	Enable State	L2 Entry Num	Action
GE1	Disabled	8192	Forward
GE2	Disabled	8192	Forward
GE3	Disabled	8192	Forward
GE4	Disabled	8192	Forward
LAG6	Disabled	8192	Forward
LAG7	Disabled	8192	Forward
LAG8	Disabled	8192	Forward

Figure 4-9-65 Port Security Status Screenshot

The page includes the following fields:

Object	Description
• **Port Name**	The switch port number of the logical port
• **Enable State**	Display the current per port security status
• **L2 Entry Num**	Display the current L2 entry number
• **Action**	Display the current action

4.9.11 DoS

The DoS is short for **Denial of Service**, which is a simple but effective destructive attack on the internet. The server under DoS attack will drop normal user data packet due to non-stop processing the attacker's data packet, leading to the denial of the service and worse can lead to leak of sensitive data of the server.

Security feature refers to applications such as protocol check which is for protecting the server from attacks such as DoS. The protocol check allows the user to drop matched packets based on specified conditions. The security features provide several simple and effective protections against Dos attacks while acting no influence on the linear forwarding performance of the switch.

4.9.11.1 Global DoS Setting

The Global DoS Setting and Information screens in Figure 4-9-66 and Figure 4-9-67 appear.

Global DoS Setting

DMAC = SMAC	⦿ Enabled ○ Disabled
Land	⦿ Enabled ○ Disabled
UDP Blat	⦿ Enabled ○ Disabled
TCP Blat	⦿ Enabled ○ Disabled
POD	⦿ Enabled ○ Disabled
IPv6 Min Fragment	⦿ Enabled ○ Disabled Byte: 1240 (0-65535)
ICMP Fragments	⦿ Enabled ○ Disabled
IPv4 Ping Max Size	⦿ Enabled ○ Disabled
IPv6 Ping Max Size	⦿ Enabled ○ Disabled
Ping Max Size Setting	Byte: 512 (0-65535)
Smurf Attack	⦿ Enabled ○ Disabled Netmask Length: 0 (0-32)
TCP Min Hdr Size	⦿ Enabled ○ Disabled Bytes: 20 (0-31)
TCP-SYN(SPORT<1024)	⦿ Enabled ○ Disabled
Null Scan Attack	⦿ Enabled ○ Disabled
X-Mas Scan Attack	⦿ Enabled ○ Disabled
TCP SYN-FIN Attack	⦿ Enabled ○ Disabled
TCP SYN-RST Attack	⦿ Enabled ○ Disabled
TCP Fragment (Offset = 1)	⦿ Enabled ○ Disabled

Apply

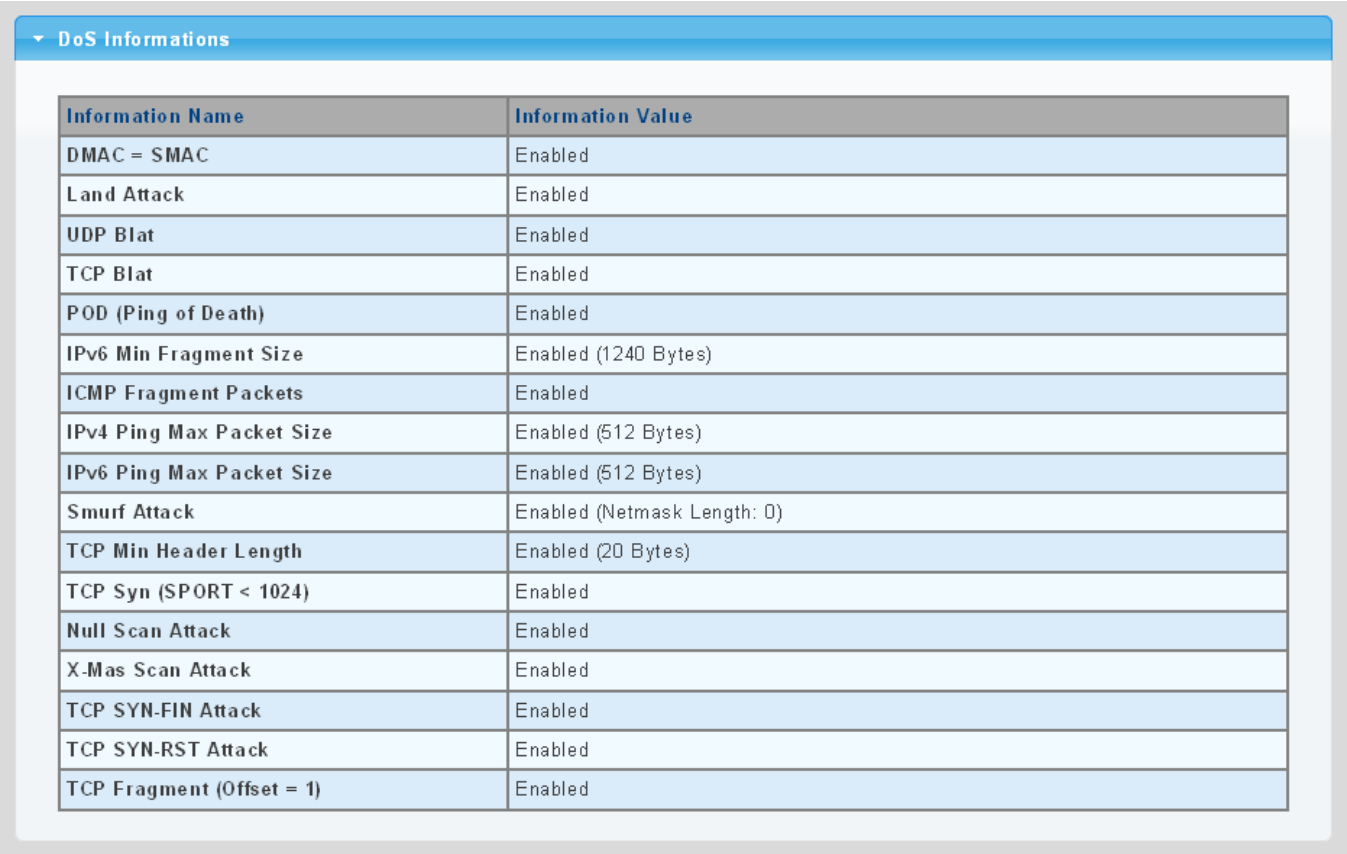
Figure 4-9-66 Global DoS Setting Screenshot

The page includes the following fields:

Object	Description
• **DMAC = SMAC**	Enable or disable DoS check mode by DMAC = SMAC
• **Land**	Enable or disable DoS check mode by land
• **UDP Blat**	Enable or disable DoS check mode by UDP blat
• **TCP Blat**	Enable or disable DoS check mode by TCP blat
• **POD**	Enable or disable DoS check mode by POD
• **IPv6 Min Fragment**	Enable or disable DoS check mode by IPv6 min fragment
• **ICMP Fragments**	Enable or disable DoS check mode by ICMP fragment
• **IPv4 Ping Max Size**	Enable or disable DoS check mode by IPv4 ping max size
• **IPv6 Ping Max Size**	Enable or disable DoS check mode by IPv6 ping max size
• **Ping Max Size Setting**	Set the max size for ping
• **Smurf Attack**	Enable or disable DoS check mode by smurf attack
• **TCP Min Hdr Size**	Enable or disable DoS check mode by TCP min hdr size
• **TCP-SYN (SPORT < 1024)**	Enable or disable DoS check mode by TCP-syn (sport < 1024)
• **Null Scan Attack**	Enable or disable DoS check mode by null scan attack
• **X-Mas Scan Attack**	Enable or disable DoS check mode by x-mas scan attack
• **TCP SYN-FIN Attack**	Enable or disable DoS check mode by TCP syn-fin attack
• **TCP SYN-RST Attack**	Enable or disable DoS check mode by TCP syn-rst attack
• **TCP Fragment (Offset = 1)**	Enable or disable DoS check mode by TCP fragment (offset = 1)

Buttons

Apply: Click to apply changes.



DoS Informations

Information Name	Information Value
DMAC = SMAC	Enabled
Land Attack	Enabled
UDP Blat	Enabled
TCP Blat	Enabled
POD (Ping of Death)	Enabled
IPv6 Min Fragment Size	Enabled (1240 Bytes)
ICMP Fragment Packets	Enabled
IPv4 Ping Max Packet Size	Enabled (512 Bytes)
IPv6 Ping Max Packet Size	Enabled (512 Bytes)
Smurf Attack	Enabled (Netmask Length: 0)
TCP Min Header Length	Enabled (20 Bytes)
TCP Syn (SPORT < 1024)	Enabled
Null Scan Attack	Enabled
X-Mas Scan Attack	Enabled
TCP SYN-FIN Attack	Enabled
TCP SYN-RST Attack	Enabled
TCP Fragment (Offset = 1)	Enabled

Figure 4-9-67 DoS Information Screenshot

The page includes the following fields:

Object	Description
• **DMAC = SMAC**	Display the current DMAC = SMAC status
• **Land Attach**	Display the current land attach status
• **UDP Blat**	Display the current UDP blat status
• **TCP Blat**	Display the current TCP blat status
• **POD**	Display the current POD status
• **IPv6 Min Fragment**	Display the current IPv6 min fragment status
• **ICMP Fragments**	Display the current ICMP fragment status
• **IPv4 Ping Max Size**	Display the current IPv4 ping max size status
• **IPv6 Ping Max Size**	Display the current IPv6 ping max size status
• **Smurf Attack**	Display the current smurf attack status
• **TCP Min Header Length**	Display the current TCP min header length
• **TCP-SYN (SPORT < 1024)**	Display the current TCP syn status
• **Null Scan Attack**	Display the current null scan attack status
• **X-Mas Scan Attack**	Display the current x-mas scan attack status
• **TCP SYN-FIN Attack**	Display the current TCP syn-fin attack status
• **TCP SYN-RST Attack**	Display the current TCP syn-rst attack status
• **TCP Fragment (Offset = 1)**	Display the TCP fragment (offset = 1) status

4.9.11.2 DoS Port Setting

The DoS Port Setting and Status screens in Figure 4-9-68 and Figure 4-9-69 appear.

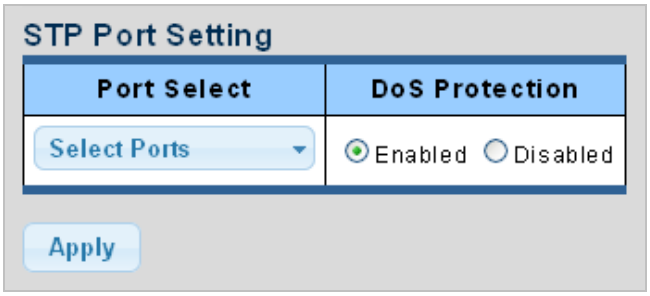


Figure 4-9-68 Port Security Setting Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port from this drop-down list.
• **DoS Protection**	Enable or disable per port DoS protection.

Buttons

Apply: Click to apply changes.

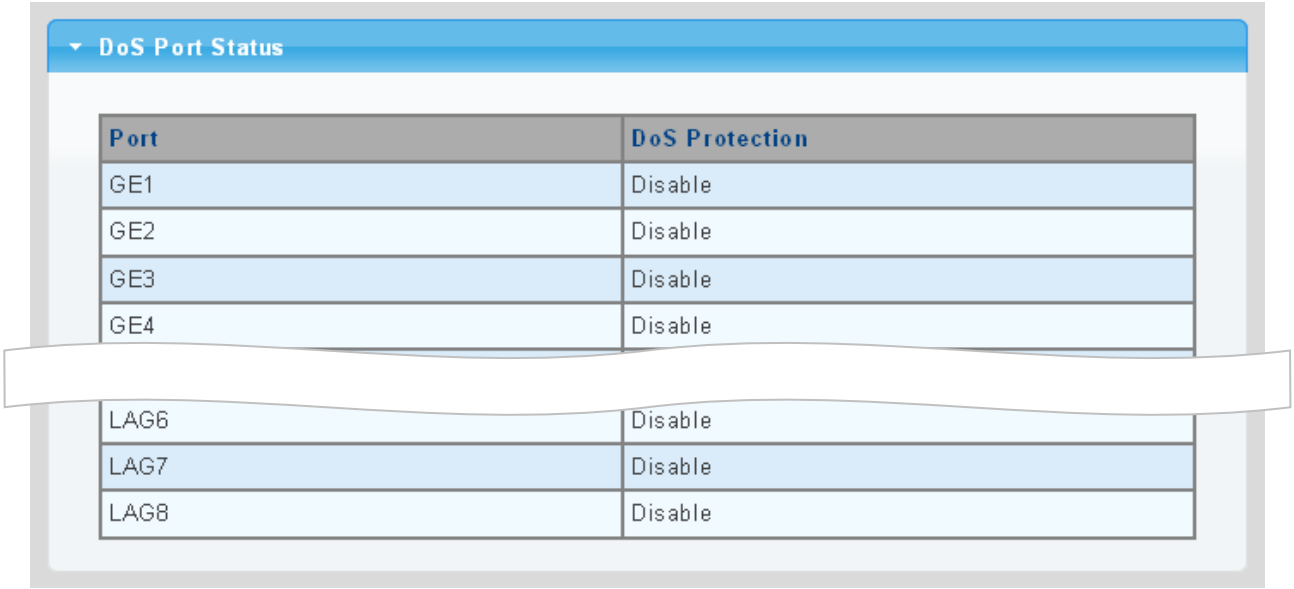


Figure 4-9-68 Port Security Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **DoS Protection**	Display the current DoS protection

4.9.12 Storm Control

Storm control for the switch is configured on this page.

There is an unknown unicast storm rate control, unknown multicast storm rate control, and a broadcast storm rate control.

These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

4.9.12.1 Global Setting

The Storm Control Global Setting and Information screens in Figure 4-9-69 and Figure 4-9-70 appear.

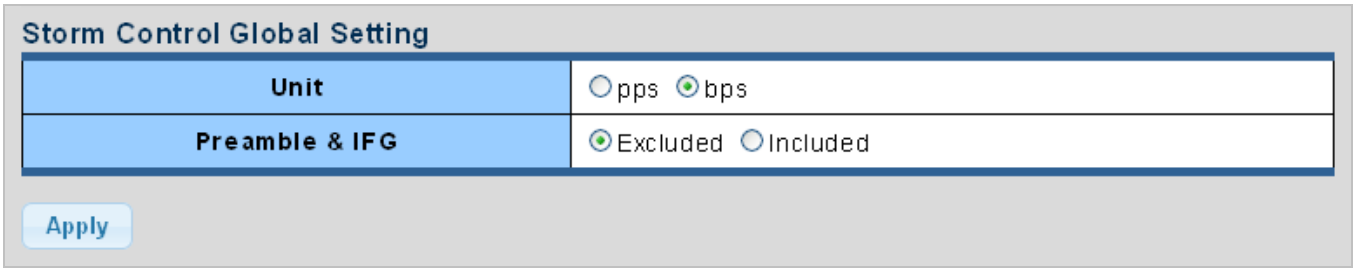


Figure 4-9-69 Storm Control Global Setting Screenshot

The page includes the following fields:

Object	Description
• **Unit**	Controls the unit of measure for the storm control rate as "pps" or "bps". The default value is "bps".
• **Preamble and IFG**	Set the excluded or included interframe gap

Buttons

Apply: Click to apply changes.

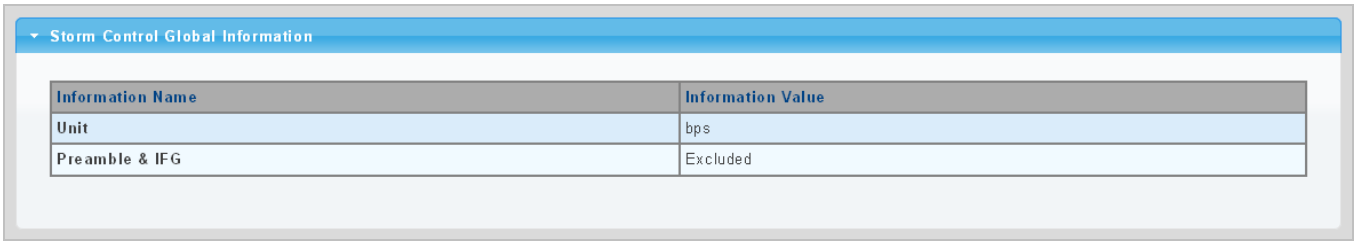


Figure 4-9-70 Storm Control Global Information Screenshot

The page includes the following fields:

Object	Description
• **Unit**	Display the current unit
• **Preamble and IFG**	Display the current preamble and IFG

4.9.12.2 Port Setting

Storm control for the switch is configured on this page. There are three types of storm rate control:

- **Broadcast** storm rate control
- **Unknown Unicast** storm rate control
- **Unknown Multicast** storm rate control

The configuration indicates the permitted packet rate for unknown unicast, unknown multicast, or broadcast traffic across the switch. The Storm Control Configuration screens in Figure 4-9-71 and Figure 4-9-72 appear.

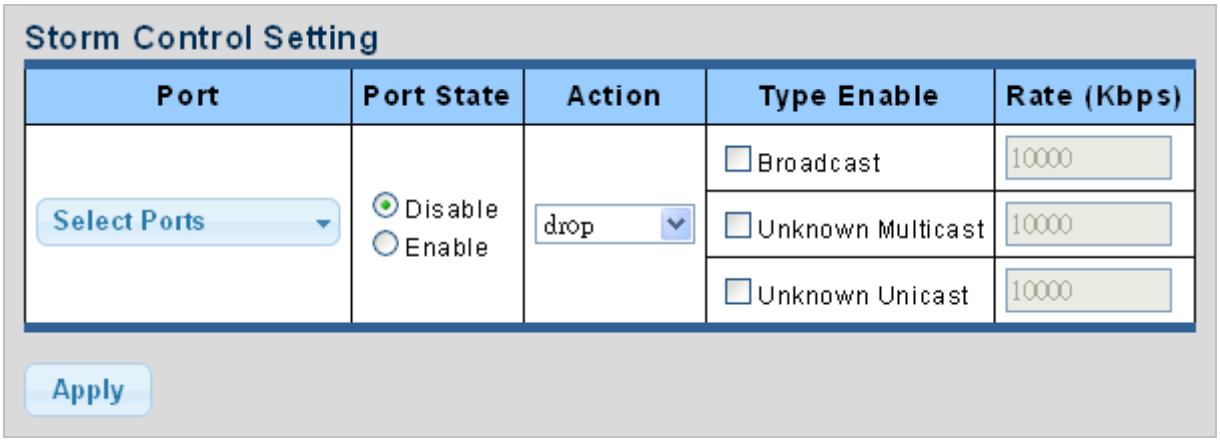


Figure 4-9-71 Storm Control Setting Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list.
• **Port State**	Enable or disable the storm control status for the given storm type.
• **Action**	Configures the action performed when storm control is over rate on a port. Valid values are **Shutdown** or **Drop**.
• **Type Enable**	The settings in a particular row apply to the frame type listed here: ■ **broadcast** ■ **unknown unicast** ■ **unknown multicast**
• **Rate (kbps/pps)**	Configure the rate for the storm control. The default value is "10,000".

Buttons

Apply: Click to apply changes

Storm Control Information

Port	Port State	Broadcast (Kbps)	Unknown Multicast (Kbps)	Unknown Unicast (Kbps)	Action
GE1	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE2	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE3	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE4	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE5	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE6	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE7	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE8	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE9	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE10	disabled	Off (10000)	Off (10000)	Off (10000)	Drop

Figure 4-9-72 Storm Control Information Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Port State**	Display the current port state
• **Broadcast (Kbps/pps)**	Display the current broadcast storm control rate
• **Unknown Multicast (Kbps/pps)**	Display the current unknown multicast storm control rate
• **Unknown Unicast (Kbps/pps)**	Display the current unknown unicast storm control rate
• **Action**	Display the current action

4.10 ACL

ACL is an acronym for **Access Control List**. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

ACE is an acronym for **Access Control Entry**. It describes access permission associated with a particular ACE ID.
There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.
The ACL page contains links to the following main topics:

- **MAC-based ACL** Configuration MAC-based ACL setting
- **MAC-based ACE** Add / Edit / Delete the MAC-based ACE (Access Control Entry) setting
- **IPv4-based ACL** Configuration IPv4-based ACL setting
- **IPv4-based ACE** Add / Edit / Delete the IPv4-based ACE (Access Control Entry) setting
- **IPv6-based ACL** Configuration IPv6-based ACL setting
- **IPv6-based ACE** Add / Edit / Delete the IPv6-based ACE (Access Control Entry) setting
- **ACL Binding** Configure the ACL parameters (ACE) of each switch port.

4.10.1 MAC-based ACL

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. MAC-based ACL screens in Figure 4-10-1 and Figure 4-10-2 appear.

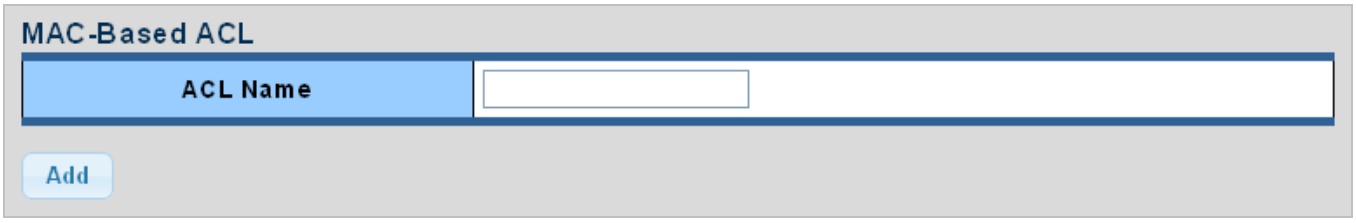


Figure 4-10-1 MAC-based ACL Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Create a named MAC-based ACL list

■ **ACL Table**

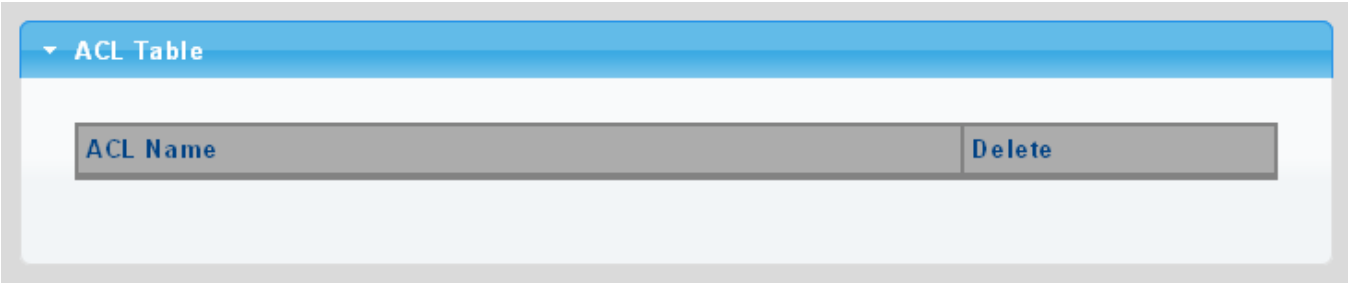


Figure 4-10-2 ACL Table Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Click Delete to delete ACL name entry

4.10.2 MAC-based ACE

An ACE consists of several parameters. Different parameter options are displayed depending on the frame type that you selected. The MAC-based ACE screen in Figure 4-10-3 and Figure 4-10-4 appears.

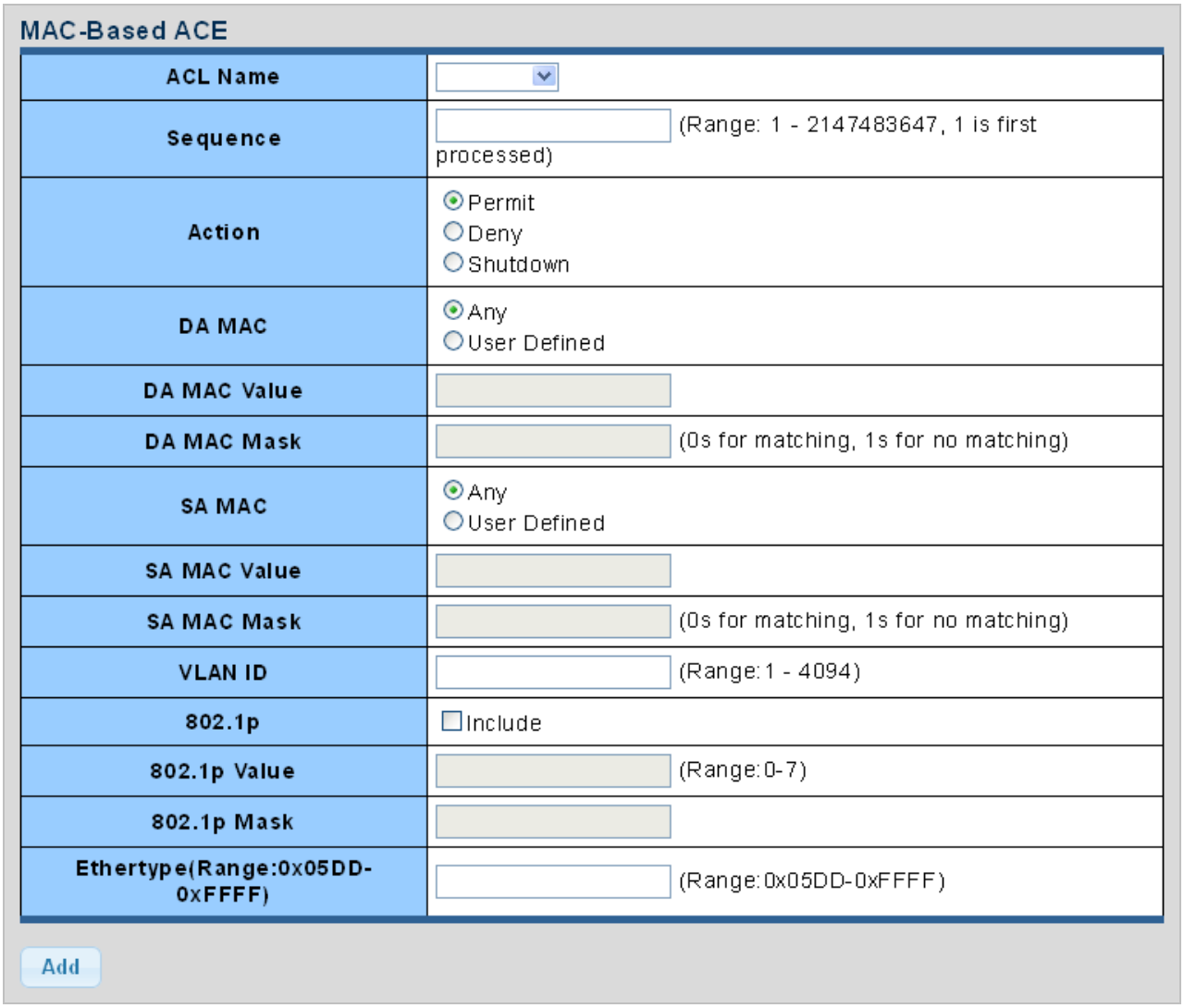


Figure 4-10-3 MAC-based ACE Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Select ACL name from this drop-down list
• **Sequence**	Set the ACL sequence
• **Action**	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped. ■ **Shutdown**: Port shutdown is disabled for the ACE.
• **DA MAC**	Specify the destination MAC filter for this ACE. ■ **Any**: No DA MAC filter is specified.

	■ **User Defined**: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DA MAC value appears.
• **DA MAC Value**	When "User Defined" is selected for the DA MAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DA MAC value.
• **DA MAC Mask**	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. ■ **0**: ARP frames where SHA is not equal to the DA MAC address. ■ **1**: ARP frames where SHA is equal to the DA MAC address.
• **SA MAC**	Specify the source MAC filter for this ACE. ■ **Any**: No SA MAC filter is specified. ■ **User Defined**: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering a SA MAC value appears.
• **SA MAC Value**	When "User Defined" is selected for the SA MAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SA MAC value.
• **SA MAC Mask**	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. ■ **0**: ARP frames where SHA is not equal to the SA MAC address. ■ **1**: ARP frames where SHA is equal to the SA MAC address.
• **VLAN ID**	Indicates the ID of this particular VLAN
• **802.1p**	Include or exclude the 802.1p value
• **802.1p Value**	Set the 802.1p value
• **802.1p Mask**	■ **0**: where frame is not equal to the 802.1p value. ■ **1**: where frame is equal to the 802.1p value.
• **Ethertype (Range: 0x05DD – 0xFFFF)**	You can enter a specific EtherType value. The allowed range is from **0x05DD** to **0xFFFF**. A frame that hits this ACE matches this EtherType value.

Buttons

Add: Click to add ACE list.

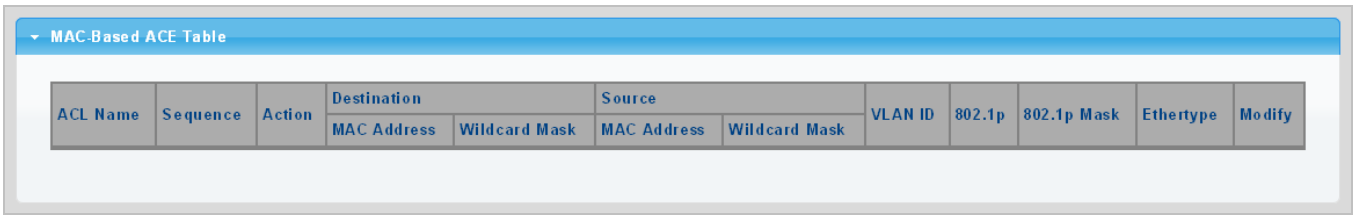


Figure 4-10-4 MAC-based ACE Table Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Display the current ACL name
• **Sequence**	Display the current sequence
• **Action**	Display the current action
• **Destination MAC Address**	Display the current destination MAC address
• **Destination MAC Address Mask**	Display the current destination MAC address mask
• **Source MAC Address**	Display the current source MAC address
• **Source MAC Address Mask**	Display the current source MAC address mask
• **VLAN ID**	Display the current VLAN ID
• **802.1p**	Display the current 802.1p value
• **802.1p Mask**	Display the current 802.1p mask
• **Ethertype**	Display the current Ethernet type
• **Modify**	Click Edit to edit MAC-based ACL parameter Click Delete to delete MAC-based ACL entry

4.10.3 IPv4-based ACL

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. IPv4-based ACL screens in Figure 4-10-5 and Figure 4-10-6 appear.

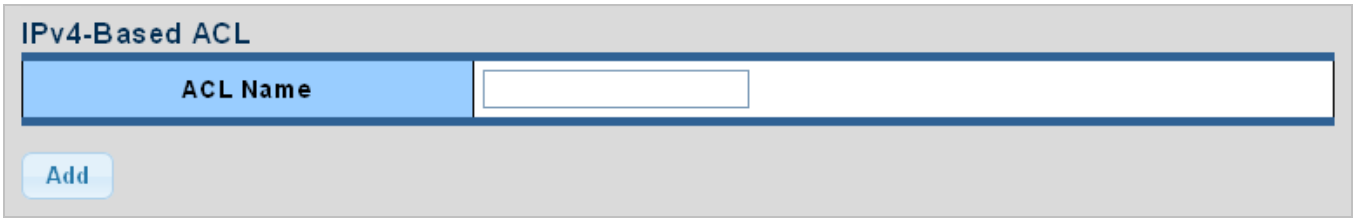


Figure 4-10-5 IPv4-based ACL Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Create a named IPv4-based ACL list

Buttons

Add: Click to add ACL name list.

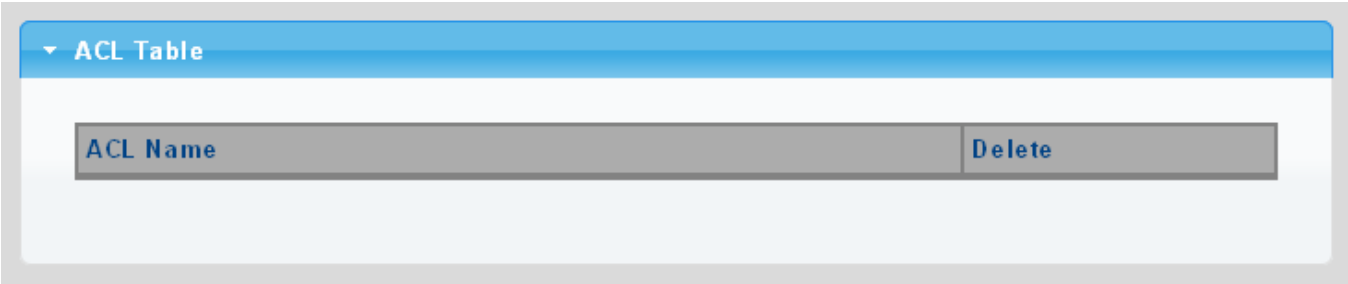


Figure 4-10-6 ACL Table Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Click Delete to delete ACL name entry.

4.10.4 IPv4-based ACE

An ACE consists of several parameters. Different parameter options are displayed depending on the frame type that you selected. The IPv4-based ACE screens in Figure 4-10-7 and Figure 4-10-8 appear.

IPv4-Based ACE

ACL Name	
Sequence	(Range: 1 - 2147483647, 1 is first processed)
Action	Permit Deny Shutdown
Protocol	Any(IP) Select from list icmp Protocol ID to match 1
Source IP Address	Any User Defined
Source IP Address Value	
Source IP Wildcard Mask	(0s for matching, 1s for no matching)
Destination IP Address	Any User Defined
Destination IP Address Value	
Destination IP Wildcard Mask	(0s for matching, 1s for no matching)
Source Port	Any Single 0 (Range: 0 - 65535) Range 0 - 65535 (Range: 0 - 65535)
Destination Port	Any Single(Range: 0 - 65535) 0 (Range: 0 - 65535) Range(Range: 0 - 65535) 0 - 65535 (Range: 0 - 65535)
TCP Flags	Urg Set Unset Don't Care Ack Set Unset Don't Care Psh Set Unset Don't Care Rst Set Unset Don't Care Syn Set Unset Don't Care Fin Set Unset Don't Care
Type of Service	Any DSCP to match 0 (Range: 0 - 63) IP Precedence to match 0 (Range: 0 - 7)
ICMP	Any Select from list Echo Repl Protocol ID to match 0 (Range: 0 - 255)
ICMP Code	Any User Defined 0 (Range: 0 - 255)

Figure 4-10-7 IP-based ACE Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Select ACL name from this drop-down list.
• **Sequence**	Set the ACL sequence.
• **Action**	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped. ■ **Shutdown**: Port shutdown is disabled for the ACE..
• **Protocol**	Specify the protocol filter for this ACE. ■ **Any(IP)**: No protocol filter is specified. ■ **Select from list**: If you want to filter a specific protocol with this ACE, choose this value and select protocol from this drop-down list. ■ **Protocol ID to match**: I If you want to filter a specific protocol with this ACE, choose this value and set current protocol ID.
• **Source IP Address**	Specify the Source IP address filter for this ACE. ■ **Any**: No source IP address filter is specified. ■ **User Defined**: If you want to filter a specific source IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• **Source IP Address Value**	When "User Defined" is selected for the source IP address filter, you can enter a specific source IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this source IP address value.
• **Source IP Wildcard Mask**	When "User Defined" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
• **Destination IP Address**	Specify the Destination IP address filter for this ACE. ■ **Any**: No destination IP address filter is specified. ■ **User Defined**: If you want to filter a specific destination IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• **Destination IP Address Value**	When "User Defined" is selected for the destination IP address filter, you can enter a specific destination IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this destination IP address value.
• **Destination IP Wildcard Mask**	When "User Defined" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.
• **Source Port**	Specify the source port for this ACE. ■ **Any**: No specifc source port is specified (source port status is "don't-care"). ■ **Single**: If you want to filter a specific source port with this ACE, you can enter a specific source port value. A field for entering a source port value appears. The allowed range is from **0** to **65535**. A frame that hits this ACE

		matches this source port value. ■ **Range**: If you want to filter a specific source port range with this ACE, you can enter a specific source port range value. A field for entering a source port value appears. The allowed range is from **0** to **65535**. A frame that hits this ACE matches this source port value.
• **Destination Port**	Specify the destination port for this ACE. ■ **Any**: No specifc destination port is specified (destination port status is "don't-care"). ■ **Single**: If you want to filter a specific destination port with this ACE, you can enter a specific destination port value. A field for entering a destination port value appears. The allowed range is from **0** to **65535**. A frame that hits this ACE matches this destination port value. ■ **Range**: If you want to filter a specific destination port range with this ACE, you can enter a specific destination port range value. A field for entering a destination port value appears.	
• **TCP Flags**	UGR	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. ■ **Set**: TCP frames where the URG field is set must be able to match this entry. ■ **Unset**: TCP frames where the URG field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. ■ **Set**: TCP frames where the ACK field is set must be able to match this entry. ■ **Unset**: TCP frames where the ACK field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	PSH	Specify the TCP "Push Function" (PSH) value for this ACE. ■ **Set**: TCP frames where the PSH field is set must be able to match this entry. ■ **Unset**: TCP frames where the PSH field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	RST	■ Specify the TCP "Reset the connection" (RST) value for this ACE. **Set**: TCP frames where the RST field is set must be able to match this entry. ■ **Unset**: TCP frames where the RST field is set must not be able to match this entry.

		■ **Don't Care**: Any value is allowed ("don't-care").
	SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. ■ **Set**: TCP frames where the SYN field is set must be able to match this entry. ■ **Unset**: TCP frames where the SYN field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. ■ **Set**: TCP frames where the FIN field is set must be able to match this entry. ■ **Unset**: TCP frames where the FIN field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
• **Type of Service**	Specify the type of service for this ACE. ■ **Any**: No specifc type of service is specified (destination port status is "don't-care"). ■ **DSCP**: If you want to filter a specific DSCP with this ACE, you can enter a specific DSCP value. A field for entering a DSCP value appears. The allowed range is from **0** to **63**. A frame that hits this ACE matches this DSCP value. ■ **IP Recedence**: If you want to filter a specific IP recedence with this ACE, you can enter a specific IP recedence value. A field for entering an IP recedence value appears. The allowed range is from **0** to **7**. A frame that hits this ACE matches this IP recedence value.	
• **ICMP**	Specify the ICMP for this ACE. ■ **Any**: No specifc ICMP is specified (destination port status is "don't-care"). ■ **List**: If you want to filter a specific list with this ACE, you can select a specific list value. ■ **Protocol ID**: If you want to filter a specific protocol ID filter with this ACE, you can enter a specific protocol ID value. A field for entering a protocol ID value appears. The allowed range is from **0** to **255**. A frame that hits this ACE matches this protocol ID value.	
• **ICMP Code**	Specify the ICMP code filter for this ACE. ■ **Any**: No ICMP code filter is specified (ICMP code filter status is "don't-care"). ■ **User Defined**: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. The allowed range is from **0** to **255**. A frame that hits this ACE matches this ICMP code value.	

Buttons

Add: Click to add ACE list.

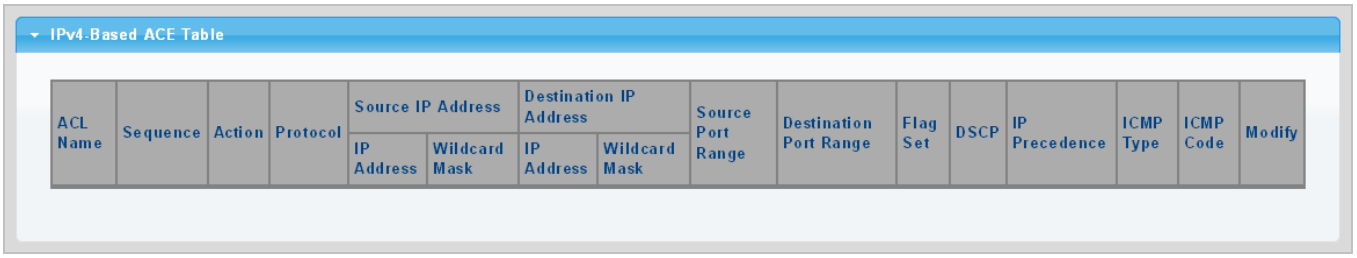


Figure 4-10-8 IPv4-based ACE Table Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Display the current ACL name
• **Sequence**	Display the current sequence
• **Action**	Display the current action
• **Protocol**	Display the current protocol
• **Source IP Address**	Display the current source IP address
• **Source IP Address Wildcard Mask**	Display the current source IP address wildcard mask
• **Destination IP Address**	Display the current destination IP address
• **Destination IP Address Wildcard Mask**	Display the current destination IP address wildcard mask
• **Source Port Range**	Display the current source port range
• **Destination Port Range**	Display the current destination port range
• **Flag Set**	Display the current flag set
• **DSCP**	Display the current DSCP
• **IP Precedence**	Display the current IP precedence
• **ICMP Type**	Display the current ICMP Type
• **ICMP Code**	Display the current ICMP code
• **Modify**	Click Edit to edit IPv4-based ACL parameter Click Delete to delete IPv4-based ACL entry

4.10.5 IPv6-based ACL

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. IPv6-based ACL screens in Figure 4-10-9 and Figure 4-10-10 appear.

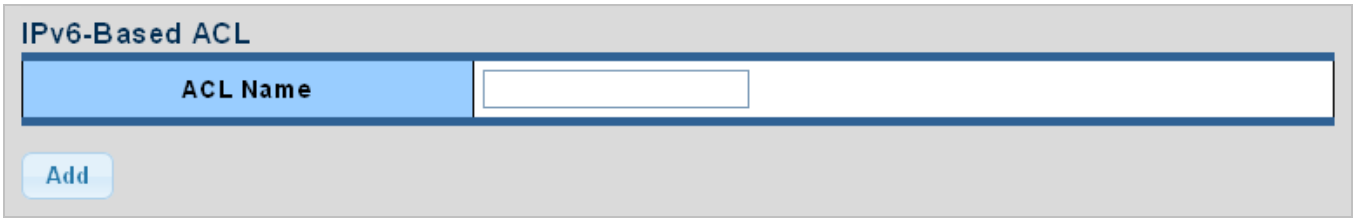


Figure 4-10-9 IPv6-based ACL Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Create a named IPv6-based ACL list

Buttons

Add: Click to add ACL name list.

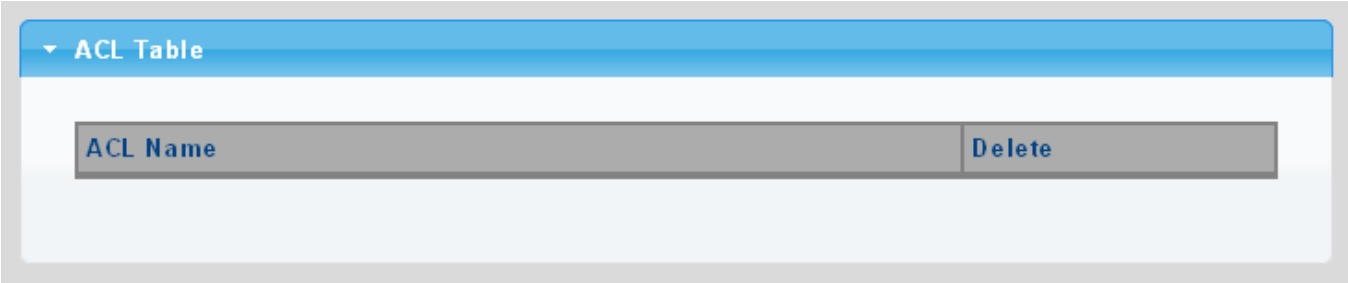


Figure 4-10-10 ACL Table Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Click Delete to delete ACL name entry

4.10.6 IPv6-based ACE

An ACE consists of several parameters. Different parameter options are displayed depending on the frame type that you selected. The IPv6-based ACE screens in Figure 4-10-11 and Figure 4-10-12 appear.

IPv6-Based ACE

ACL Name	
Sequence	(Range: 1 - 2147483647, 1 is first processed)
Action	Permit Deny Shutdown
Protocol	Any(IP) Select from list tcp
Source IP Address	Any User Defined
Source IP Address Value	
Source IP Prefix Length	0 (Range: 0 - 128)
Destination IP Address	Any User Defined
Destination IP Address Value	
Destination IP refix Length	0 (0s for matching, 1s for no matching)
Source Port	Any Single 0 (Range: 0 - 65535) Range 0 - 65535 (Range: 0 - 65535)
Destination Port	Any Single(Range: 0 - 65535) 0 (Range: 0 - 65535) Range(Range: 0 - 65535) 0 - 65535 (Range: 0 - 65535)
TCP Flags	Urg Set Unset Don't Care Ack Set Unset Don't Care Psh Set Unset Don't Care Rst Set Unset Don't Care Syn Set Unset Don't Care Fin Set Unset Don't Care
Type of Service	Any DSCP to match 0 (Range: 0 - 63) IP Precedence to match 0 (Range: 0 - 7)
ICMP	Any Select from list destination Protocol ID to match 0 (Range: 0 - 255)
ICMP Code	Any User Defined 0 (Range: 0 - 255)

Figure 4-10-11 IP-based ACE Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Select ACL name from this drop-down list
• **Sequence**	Set the ACL sequence
• **Action**	Indicates the forwarding action of the ACE ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped. ■ **Shutdown**: Port shutdown is disabled for the ACE.
• **Protocol**	Specify the protocol filter for this ACE ■ **Any (IP)**: No protocol filter is specified. ■ **Select from list**: If you want to filter a specific protocol with this ACE, choose this value and select protocol from this drop-down list.
• **Source IP Address**	Specify the Source IP address filter for this ACE ■ **Any**: No source IP address filter is specified. ■ **User Defined**: If you want to filter a specific source IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• **Source IP Address Value**	When "User Defined" is selected for the source IP address filter, you can enter a specific source IP address. The legal format is "xxxx:xxxx:xxxx:xxxx: xxxx:xxxx:xxxx:xxxx". A frame that hits this ACE matches this source IP address value.
• **Source IP Prefix Length**	When "User Defined" is selected for the source IP filter, you can enter a specific SIP prefix length in dotted decimal notation.
• **Destination IP Address**	Specify the Destination IP address filter for this ACE. ■ **Any**: No destination IP address filter is specified. ■ **User Defined**: If you want to filter a specific destination IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• **Destination IP Address Value**	When "User Defined" is selected for the destination IP address filter, you can enter a specific destination IP address. The legal format is " xxxx:xxxx:xxxx:xxxx: xxxx:xxxx:xxxx:xxxx ". A frame that hits this ACE matches this destination IP address value.
• **Destination IP Prefix Length**	When "User Defined" is selected for the destination IP filter, you can enter a specific DIP prefix length in dotted decimal notation.
• **Source Port**	Specify the source port for this ACE. ■ **Any**: No specifc source port is specified (source port status is "don't-care"). ■ **Single**: If you want to filter a specific source port with this ACE, you can enter a specific source port value. A field for entering a source port value appears. The allowed range is from **0** to **65535**. A frame that hits this ACE

		matches this source port value. ■ **Range**: If you want to filter a specific source port range with this ACE, you can enter a specific source port range value. A field for entering a source port value appears. The allowed range is from **0** to **65535**. A frame that hits this ACE matches this source port value.
• **Destination Port**	Specify the destination port for this ACE. ■ **Any**: No specifc destination port is specified (destination port status is "don't-care"). ■ **Single**: If you want to filter a specific destination port with this ACE, you can enter a specific destination port value. A field for entering a destination port value appears. The allowed range is from **0** to **65535**. A frame that hits this ACE matches this destination port value. ■ **Range**: If you want to filter a specific destination port range with this ACE, you can enter a specific destination port range value. A field for entering a destination port value appears.	
• **TCP Flags**	UGR	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. ■ **Set**: TCP frames where the URG field is set must be able to match this entry. ■ **Unset**: TCP frames where the URG field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. ■ **Set**: TCP frames where the ACK field is set must be able to match this entry. ■ **Unset**: TCP frames where the ACK field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	PSH	Specify the TCP "Push Function" (PSH) value for this ACE. ■ **Set**: TCP frames where the PSH field is set must be able to match this entry. ■ **Unset**: TCP frames where the PSH field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	RST	Specify the TCP "Reset the connection" (RST) value for this ACE. ■ **Set**: TCP frames where the RST field is set must be able to match this entry. ■ **Unset**: TCP frames where the RST field is set must not be able to match this entry.

		■ **Don't Care**: Any value is allowed ("don't-care").
	SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. ■ **Set**: TCP frames where the SYN field is set must be able to match this entry. ■ **Unset**: TCP frames where the SYN field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. ■ **Set**: TCP frames where the FIN field is set must be able to match this entry. ■ **Unset**: TCP frames where the FIN field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
• **Type of Service**	Specify the type of service for this ACE. ■ **Any**: No specifc type of service is specified (destination port status is "don't-care"). ■ **DSCP**: If you want to filter a specific DSCP with this ACE, you can enter a specific DSCP value. A field for entering a DSCP value appears. The allowed range is from **0** to **63**. A frame that hits this ACE matches this DSCP value. ■ **IP Recedence**: If you want to filter a specific IP recedence with this ACE, you can enter a specific IP recedence value. A field for entering an IP recedence value appears. The allowed range is from **0** to **7**. A frame that hits this ACE matches this IP recedence value.	
• **ICMP**	Specify the ICMP for this ACE. ■ **Any**: No specifc ICMP is specified (destination port status is "don't-care"). ■ **List**: If you want to filter a specific list with this ACE, you can select a specific list value. ■ **Protocol ID**: If you want to filter a specific protocol ID filter with this ACE, you can enter a specific protocol ID value. A field for entering a protocol ID value appears. The allowed range is from **0** to **255**. A frame that hits this ACE matches this protocol ID value.	
• **ICMP Code**	Specify the ICMP code filter for this ACE. ■ **Any**: No ICMP code filter is specified (ICMP code filter status is "don't-care"). ■ **User Defined**: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. The allowed range is from **0** to **255**. A frame that hits this ACE matches this ICMP code value.	

Buttons

Add: Click to add ACE list

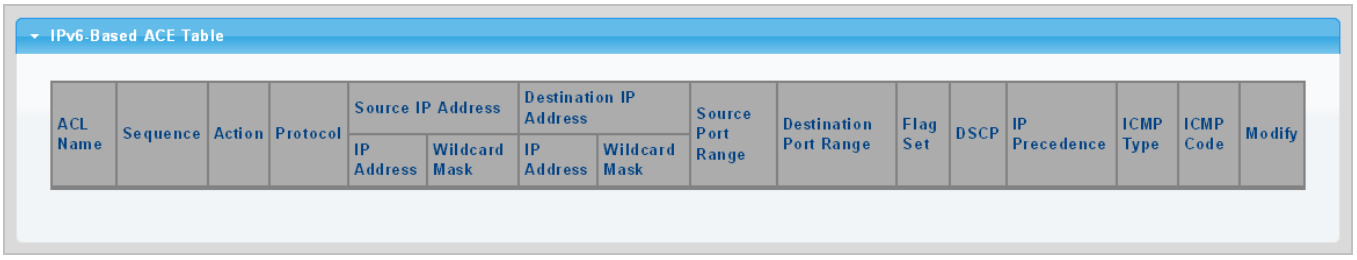


Figure 4-10-12 IPv6-based ACE Table Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Display the current ACL name
• **Sequence**	Display the current sequence
• **Action**	Display the current action
• **Protocol**	Display the current protocol
• **Source IP Address**	Display the current source IP address
• **Source IP Address Wildcard Mask**	Display the current source IP address wildcard mask
• **Destination IP Address**	Display the current destination IP address
• **Destination IP Address Wildcard Mask**	Display the current destination IP address wildcard mask
• **Source Port Range**	Display the current source port range
• **Destination Port Range**	Display the current destination port range
• **Flag Set**	Display the current flag set
• **DSCP**	Display the current DSCP
• **IP Precedence**	Display the current IP precedence
• **ICMP Type**	Display the current ICMP type
• **ICMP Code**	Display the current ICMP code
• **Modify**	Click Edit to edit IPv6-based ACL parameter. Click Delete to delete IPv6-based ACL entry.

4.10.7 ACL Binding

This page allows you to bind the Policy content to the appropriate ACLs. The ACL Policy screens in Figure 4-10-13 and Figure 4-10-14 appear.

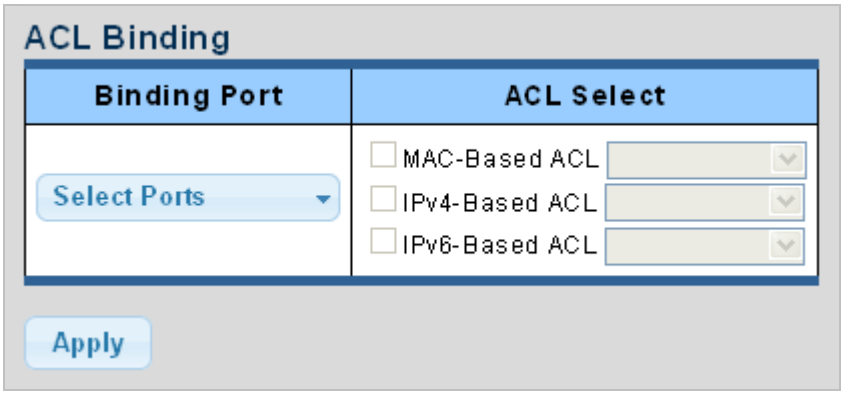


Figure 4-10-13 ACL Binding Screenshot

The page includes the following fields:

Object	Description
• **Binding Port**	Select port from this drop-down list
• **ACL Select**	Select ACL list from this drop-down list

Buttons

Apply: Click to apply changes.

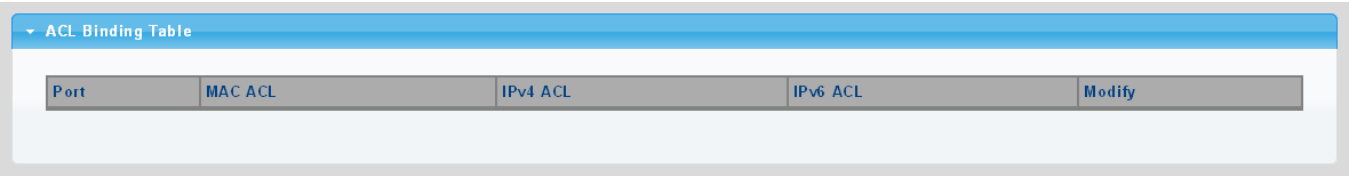


Figure 4-10-14 ACL Binding Table Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **MAC ACL**	Display the current MAC ACL
• **IPv4 ACL**	Display the current IPv4 ACL
• **IPv6 ACL**	Display the current IPv6 ACL
• **Modify**	Click Edit to edit ACL binding table parameter Click Delete to delete ACL binding entry

4.11 MAC Address Table

Switching of frames is based upon the DMAC address contained in the frame. The Managed Switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

4.11.1 Static MAC Setting

The static entries in the MAC table are shown in this table. The MAC table is sorted first by VLAN ID and then by MAC address. The Static MAC Setting screens in Figure 4-11-1 and Figure 4-11-2 appear.

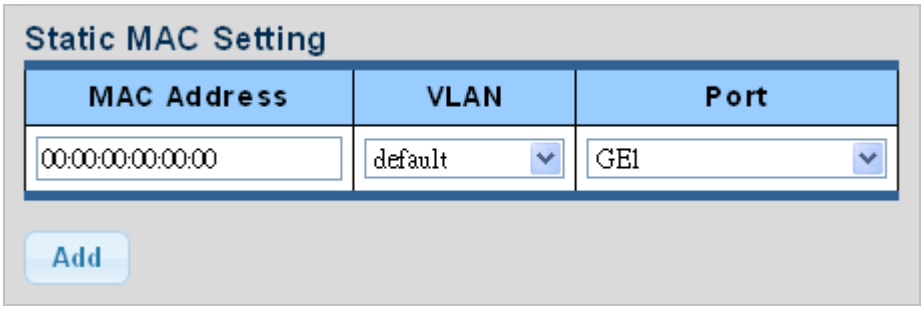


Figure 4-11-1 Statics MAC Setting Screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	Physical address associated with this interface
• **VLAN**	Select VLAN from this drop-down list
• **Port**	Select port from this drop-down list

Buttons

Add: Click to add new static MAC address.

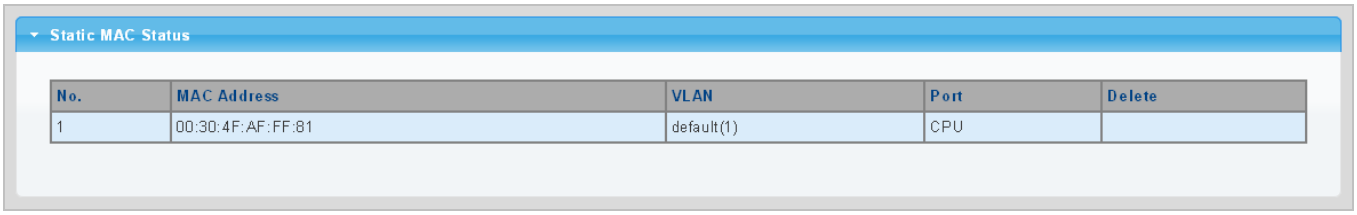


Figure 4-11-2 Statics MAC Status Screenshot

The page includes the following fields:

Object	Description
• **No.**	This is the number for entries
• **MAC Address**	The MAC address for the entry
• **VLAN**	The VLAN ID for the entry
• **Port**	Display the current port
• **Delete**	Click Delete to delete static MAC status entry

4.11.2 MAC Filtering

By filtering MAC address, the switch can easily filter the per-configured MAC address and reduce the un-safety. The Static MAC Setting screens in Figure 4-11-3 and Figure 4-11-4 appear.

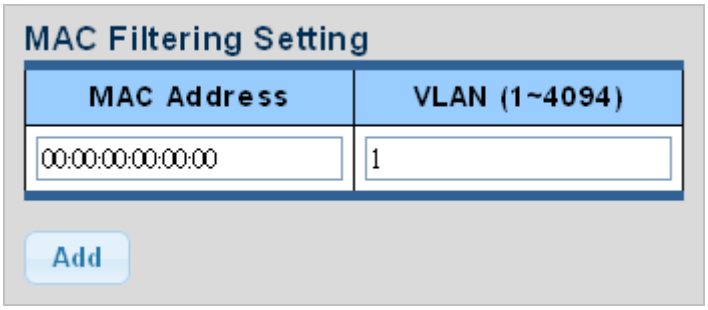


Figure 4-11-3 MAC Filtering Setting Screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	Physical address associated with this interface
• **VLAN (1~4096)**	Indicates the ID of this particular VLAN

Buttons

Add: Click to add new MAC filtering setting.

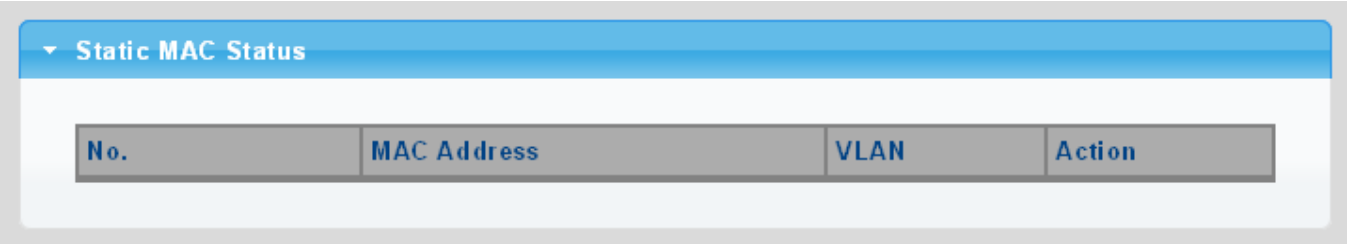


Figure 4-11-4 Statics MAC Status Screenshot

The page includes the following fields:

Object	Description
• **No.**	This is the number for entries
• **MAC Address**	The MAC address for the entry
• **VLAN**	The VLAN ID for the entry
• **Delete**	Click Delete to delete static MAC status entry.

4.11.3 Dynamic Address Setting

By default, dynamic entries are removed from the MAC table after 300 seconds. The Dynamic Address Setting/Status screens in Figure 4-11-5 and Figure 4-11-6 appear.

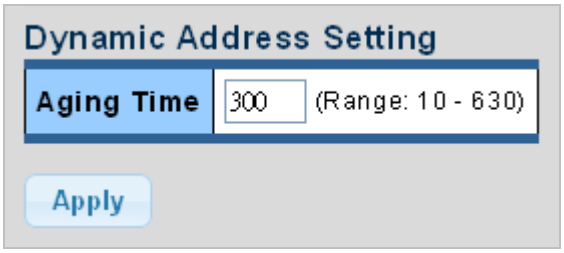


Figure 4-11-5 Dynamic Addresses Setting Screenshot

The page includes the following fields:

Object	Description
• **Aging Time**	The time after which a learned entry is discarded Range: 10-630 seconds; Default: **300 seconds**

Buttons

Apply: Click to apply changes.

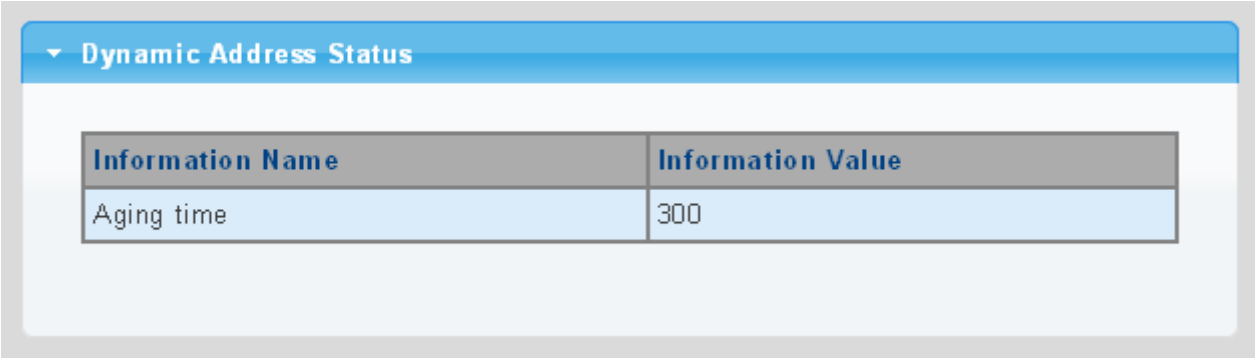


Figure 4-11-6 Dynamic Addresses Status Screenshot

The page includes the following fields:

Object	Description
• **Aging Time**	Display the current aging time

4.11.4 Dynamic Learned

Dynamic MAC Table

Dynamic Learned MAC Table is shown on this page. The MAC Table is sorted first by VLAN ID and then by MAC address. The Dynamic Learned screens in Figure 4-11-6 and Figure 4-11-7 appear.

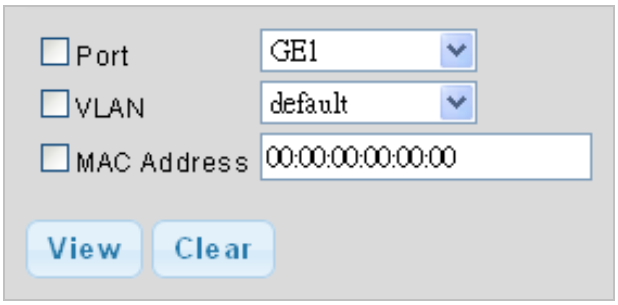


Figure 4-11-6 Dynamic Learned Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **VLAN**	Select VLAN from this drop-down list
• **MAC Address**	Physical address associated with this interface

Buttons

View: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields

Clear: Flushes all dynamic entries

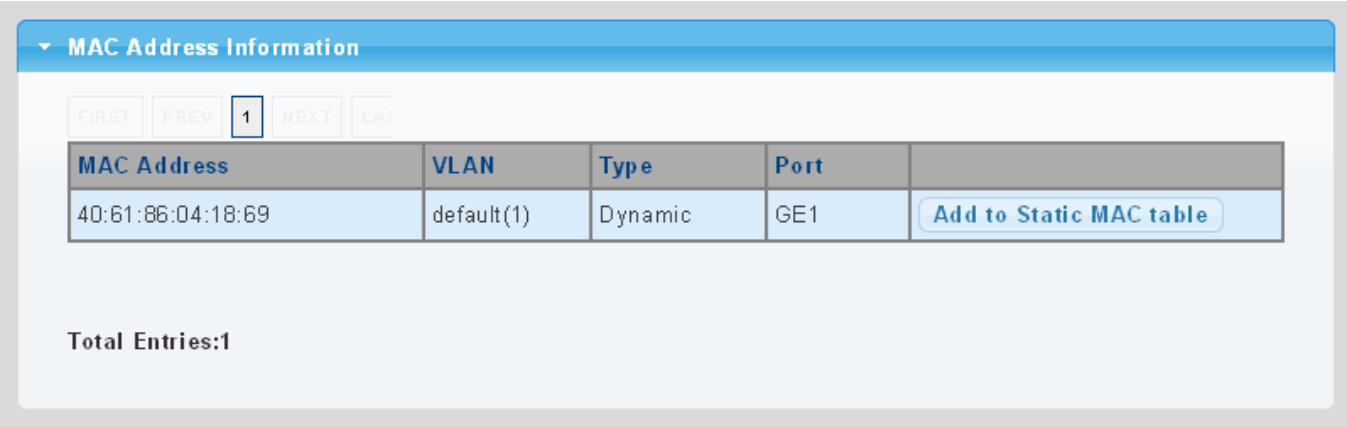


Figure 4-11-7 MAC Address Information Screenshot

Object	Description
• **MAC Address**	The MAC address of the entry
• **VLAN**	The VLAN ID of the entry
• **Type**	Indicates whether the entry is a static or dynamic entry
• **Port**	The ports that are members of the entry

Buttons

Add to Static MAC table: Click to add dynamic MAC address to static MAC address.

4.12 LLDP

4.12.1 Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in **Type Length Value (TLV)** format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

4.12.2 LLDP Global Setting

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Global Setting and Config screens in Figure 4-12-1 and Figure 4-12-2 appear.

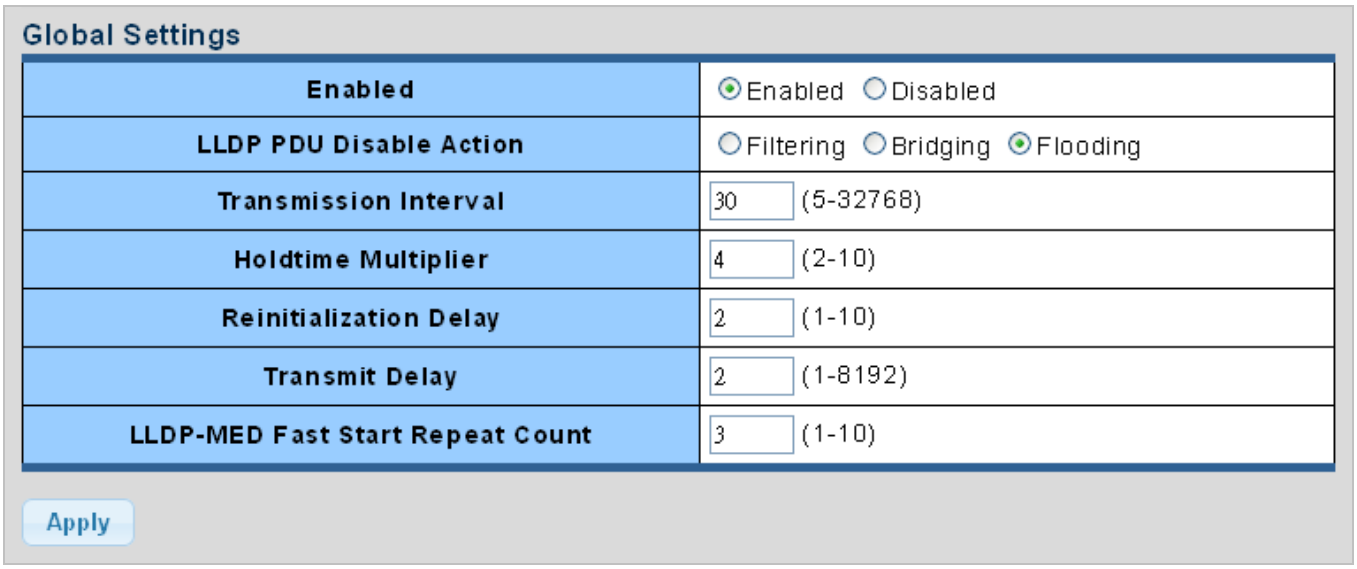


Figure 4-12-1 Global Setting Screenshot

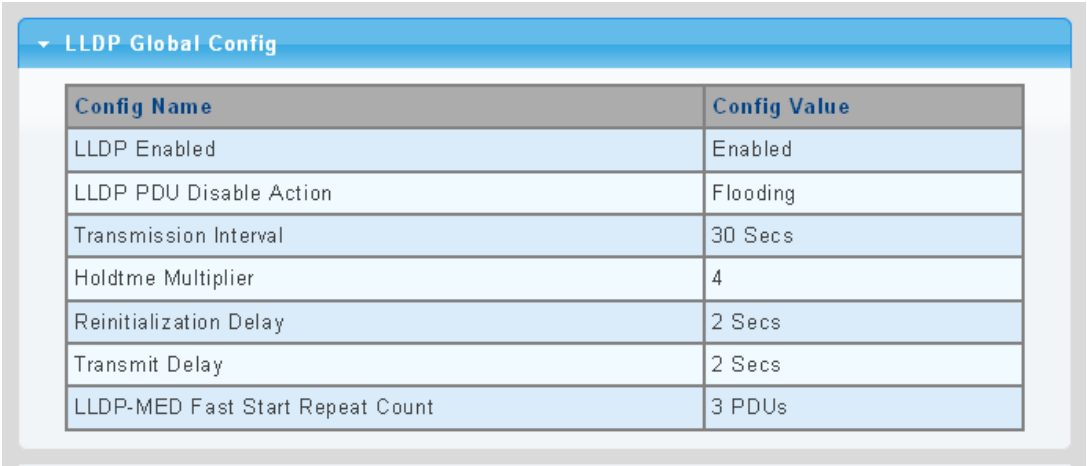
The page includes the following fields:

Object	Description
• **Enable**	Globally enable or disable LLDP function
• **LLDP PDU Disable Action**	Set LLDP PDU disable action: include "Filtering", "Bridging" and "Flooding". ■ **Filtering**: discrad all LLDP PDU. ■ **Bridging**: transmit LLDP PDU in the same VLAN. ■ **Flooding**: transmit LLDP PDU for all port.
• **Transmission Interval**	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Transmission Interval** value. Valid values are restricted to 5 - 32768 seconds. Default: **30** seconds This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)
• **Holdtime Multiplier**	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Holdtime** multiplied by **Transmission Interval** seconds. Valid values are restricted to 2 - 10 times.

	TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
• **Reinitialization Delay**	When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.
• **Transmit Delay**	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Transmit Delay** seconds. **Transmit Delay** cannot be larger than 1/4 of the **Transmission Interval** value. Valid values are restricted to 1 - 8192 seconds. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
• **LLDP-MED Fast Start Repeat Count**	Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism. Range: 1-10 packets; Default: **3** 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. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

Buttons

Apply: Click to apply changes.



LLDP Global Config

Config Name	Config Value
LLDP Enabled	Enabled
LLDP PDU Disable Action	Flooding
Transmission Interval	30 Secs
Holdtme Multiplier	4
Reinitialization Delay	2 Secs
Transmit Delay	2 Secs
LLDP-MED Fast Start Repeat Count	3 PDUs

Figure 4-12-2 LLDP Global Config Screenshot

The page includes the following fields:

Object	Description
• **LLDP Enable**	Display the current LLDP status
• **LLDP PDU Disable Action**	Display the current LLDP PDU disable action
• **Transmission Interval**	Display the current transmission interval
• **Holdtime Multiplier**	Display the current holdtime multiplier
• **Reinitialization Delay**	Display the current reinitialization delay
• **Transmit Delay**	Display the current transmit delay
• **LLDP-MED Fast Start Repeat Count**	Display the current LLDP-MED Fast Start Repeat Count

4.12.3 LLDP Port Setting

Use the LLDP Port Setting to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received. The LLDP Port Configuration and Status screens in Figure 4-12-3 and Figure 4-12-4 appear.

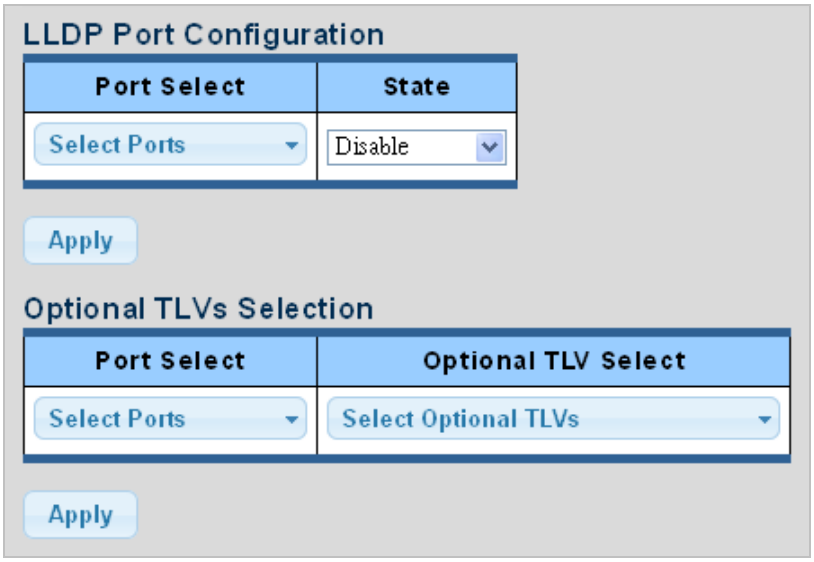


Figure 4-12-3 LLDP Port Configuration and Optional TLVs Selection Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port from this drop-down list
• **State**	Enables LLDP messages transmit and receive modes for LLDP Protocol Data Units. Options:

	■ **Tx only** ■ **Rx only** ■ **TxRx** ■ **Disabled**
• **Port Select**	Select port from this drop-down list
• **Optional TLV Select**	Configures the information included in the TLV field of advertised messages. ■ **System Name**: When checked the "System Name" is included in LLDP information transmitted. ■ **Port Description**: When checked the "Port Description" is included in LLDP information transmitted. ■ **System Description**: When checked the "System Description" is included in LLDP information transmitted. ■ **System Capability**: When checked the "System Capability" is included in LLDP information transmitted. ■ **802.3 MAC-PHY**: When checked the "802.3 MAC-PHY" is included in LLDP information transmitted. ■ **802.3 Link Aggregation**: When checked the "802.3 Link Aggregation" is included in LLDP information transmitted. ■ **802.3 Maximum Frame Size**: When checked the "802.3 Maximum Frame Size" is included in LLDP information transmitted. ■ **Management Address**: When checked the "Management Address" is included in LLDP information transmitted. ■ **802.1 PVID**: When checked the "802.1 PVID" is included in LLDP information transmitted.

Buttons

Apply: Click to apply changes

LLDP Port Status

Port	State	Selected Optional TLVs
GE1	TX&RX	802.1 PVID
GE2	TX&RX	802.1 PVID
GE3	TX&RX	802.1 PVID
GE4	TX&RX	802.1 PVID
GE5	TX&RX	802.1 PVID
GE6	TX&RX	802.1 PVID
GE7	TX&RX	802.1 PVID
GE8	TX&RX	802.1 PVID
GE9	TX&RX	802.1 PVID
GE10	TX&RX	802.1 PVID

Figure 4-12-4 LLDP Port Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **State**	Display the current LLDP status
• **Selected Optional TLVs**	Display the currently selected optional TLVs

The VLAN Name TLV VLAN Selection and LLDP Port VLAN TLV Status screens in Figure 4-12-5 and Figure 4-12-6 appear.

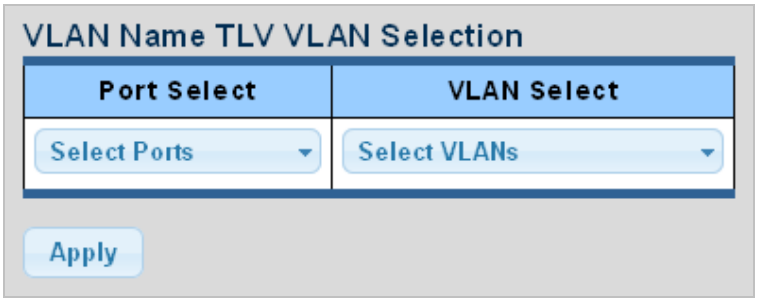


Figure 4-12-5 VLAN Name TLV Selection Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port from this drop-down list.
• **VLAN Select**	Select VLAN from this drop-down list.

Buttons

Apply: Click to apply changes.

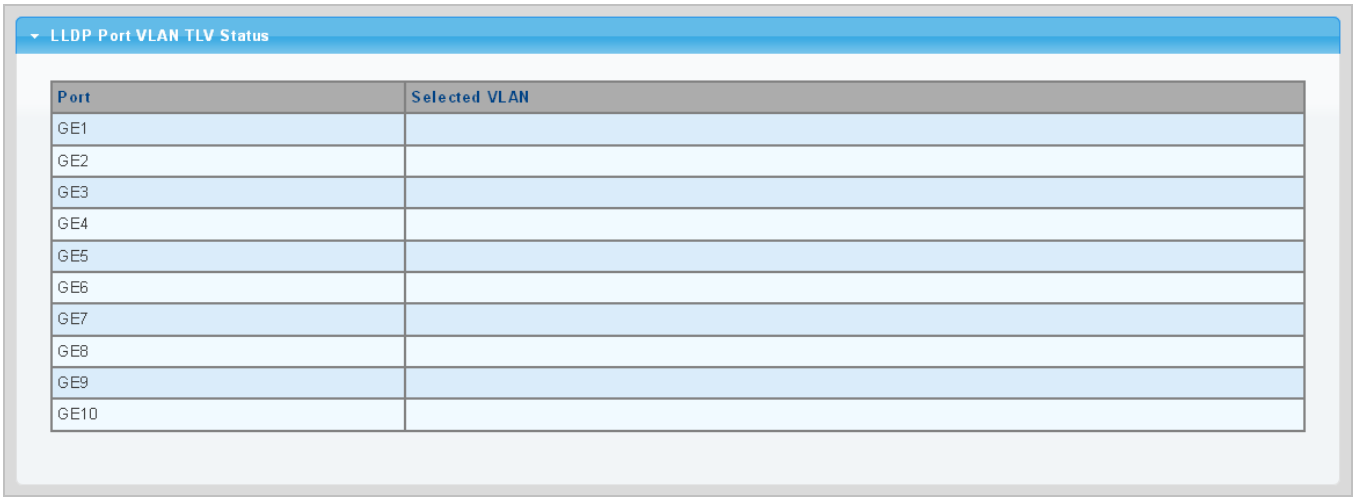


Figure 4-12-6 LLDP Port VLAN TLV Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Selected VLAN**	Display the currently selected VLAN

4.12.4 LLDP Local Device

Use the LLDP Local Device Information screen to display information about the switch, such as its **MAC address**, **chassis ID**, **management IP address**, and **port information**. The Local Device Summary and Port Status screens in Figure 4-12-7 and Figure 4-12-8 appear.

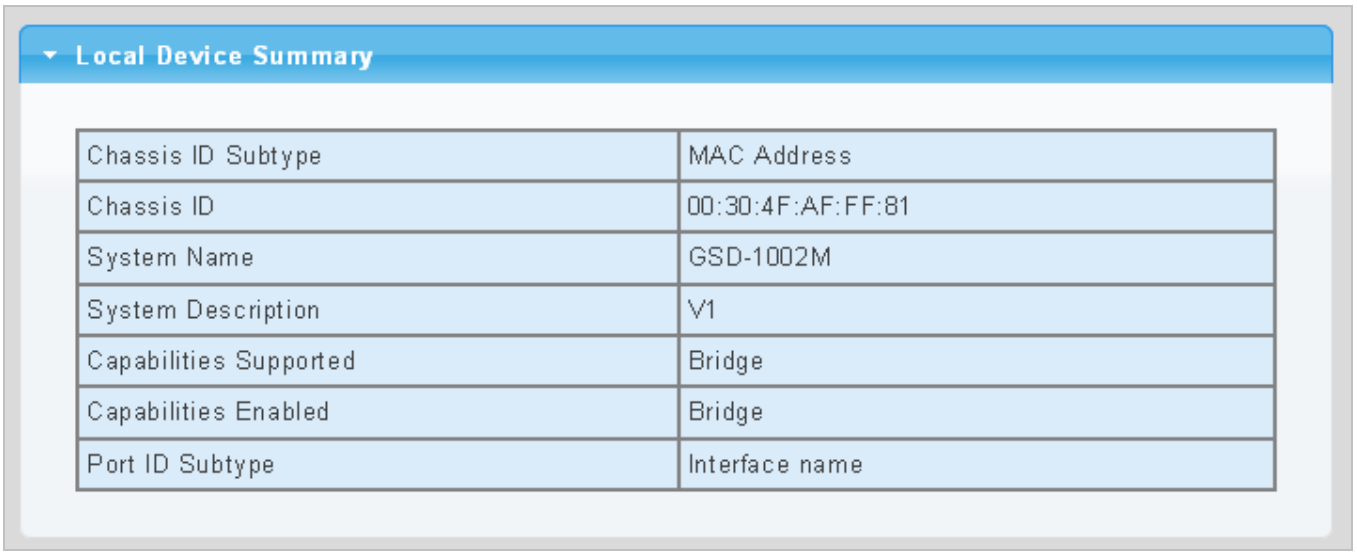
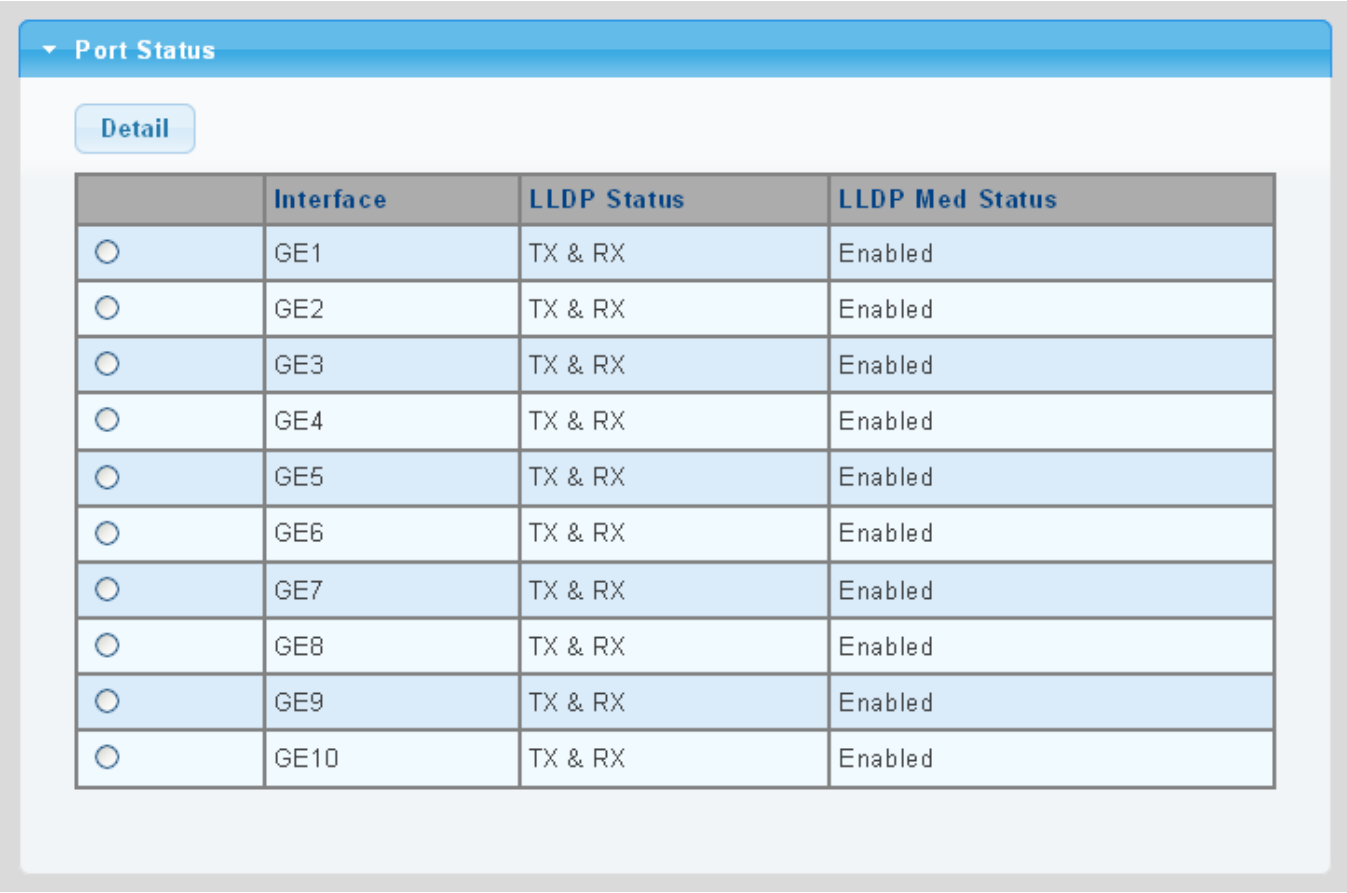


Figure 4-12-7 Local Device Summary Screenshot

The page includes the following fields:

Object	Description
• **Chassis ID Subtype**	Display the current chassis ID subtype
• **Chassis ID**	Display the current chassis ID
• **System Name**	Display the current system name
• **System Description**	Display the current system description
• **Capabilities Supported**	Display the current capabilities supported
• **Capabilities Enabled**	Display the current capabilities enabled
• **Port ID Subtype**	Display the current port ID subtype



	Interface	LLDP Status	LLDP Med Status
○	GE1	TX & RX	Enabled
○	GE2	TX & RX	Enabled
○	GE3	TX & RX	Enabled
○	GE4	TX & RX	Enabled
○	GE5	TX & RX	Enabled
○	GE6	TX & RX	Enabled
○	GE7	TX & RX	Enabled
○	GE8	TX & RX	Enabled
○	GE9	TX & RX	Enabled
○	GE10	TX & RX	Enabled

Figure 4-12-8 Port Status Screenshot

The page includes the following fields:

Object	Description
• **Interface**	The switch port number of the logical port.
• **LLDP Status**	Display the current LLDP status
• **LLDP MED Status**	Display the current LLDP MED Status

4.12.5 LLDP Remove Device

This page provides a status overview for all LLDP remove devices. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Remove Device screen in Figure 4-12-9 appears.

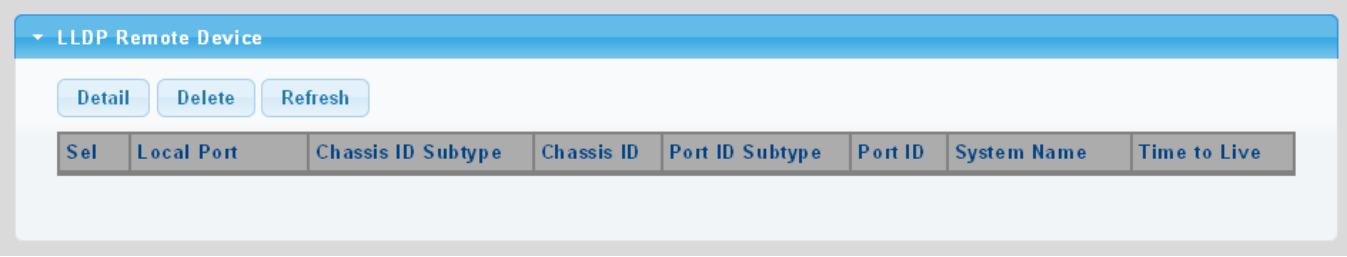


Figure 4-12-9 LLDP Remote Device Screenshot

The page includes the following fields:

Object	Description
• **Local Port**	Display the current local port
• **Chassis ID Subtype**	Display the current chassis ID subtype
• **Chassis ID**	The Chassis ID is the identification of the neighbor's LLDP frames
• **Port ID Subtype**	Display the current port ID subtype
• **Port ID**	The Remote Port ID is the identification of the neighbor port
• **System Name**	System Name is the name advertised by the neighbor unit
• **Time to Live**	Display the current time to live

Buttons

Delete: Click to delete LLDP remove device entry.

Refresh: Click to refresh LLDP remove device.

4.12.6 MED Network Policy

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

The Voice Auto Mode Configuration, Network Policy Configuration and LLDP MED Network Policy Table screen in Figure 4-12-10 and Figure 4-12-11 appears.

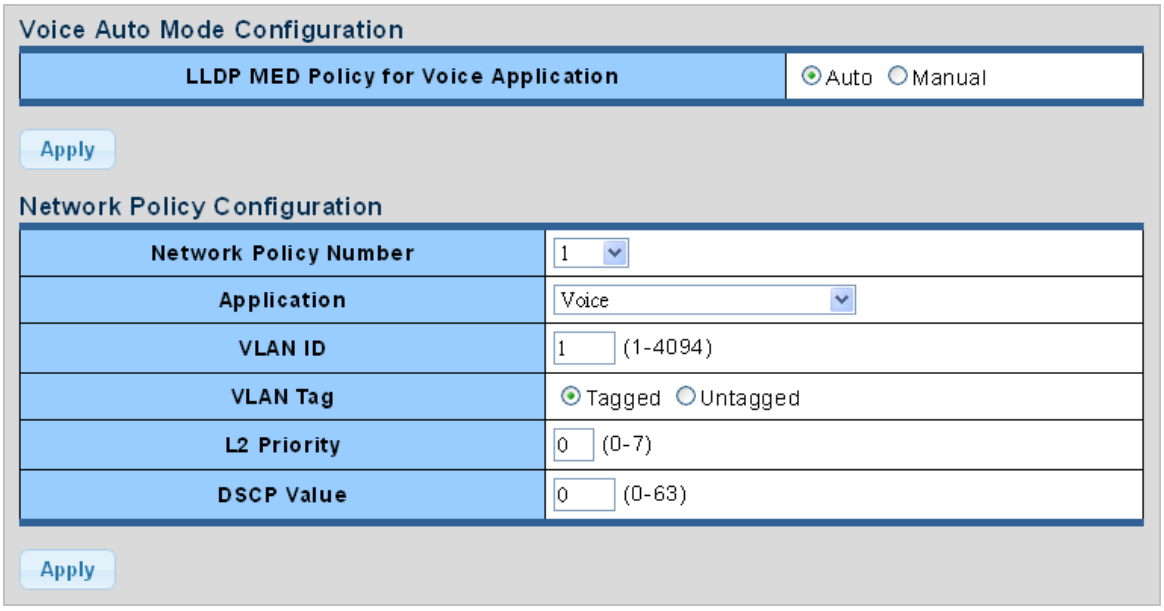


Figure 4-12-10 Voice Auto Mode Configuration and Network Policy Configuration Screenshot

The page includes the following fields:

Object	Description
• **LLDP MED Policy for Voice Application**	Set the LLDP MED policy for voice application mode
• **Network Policy Number**	Select network policy number from this drop-down list
• **Application Type**	Intended use of the application types: **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **Voice Signaling** - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. **Guest Voice Signaling** - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

	Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. **App Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. **Video Signaling** - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
• **VLAN ID**	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003
• **Tag**	**Tag** indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. **Untagged** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. **Tagged** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
• **L2 Priority**	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
• **DSCP**	DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Buttons

Apply: Click to apply changes.

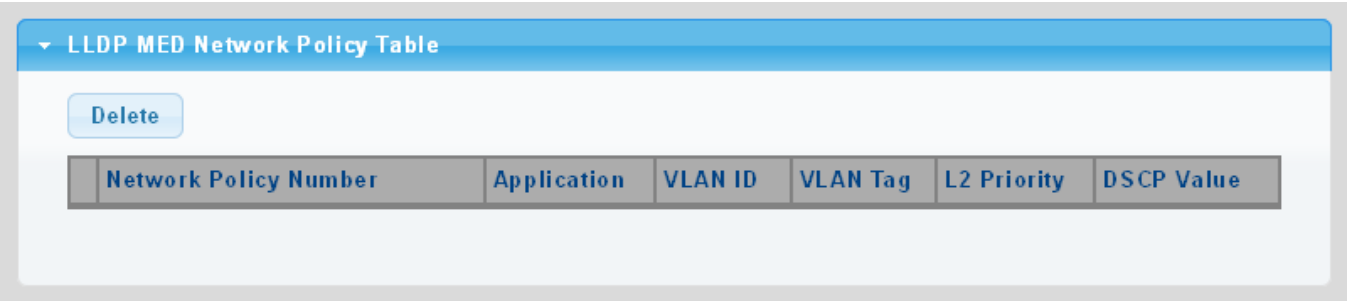


Figure 4-12-11 LLDP MED Network Policy Table Screenshot

The page includes the following fields:

Object	Description
• **Network Policy Number**	Display the current network policy number
• **Application**	Display the current application
• **VLAN ID**	Display the current VLAN ID
• **VLAN Tag**	Display the current VLAN tag status
• **L2 Priority**	Display the current L2 priority
• **DSCP Value**	Display the current DSCP value

Buttons

Delete: Click to delete LLDP MED network policy table entry.

4.12.7 MED Port Setting

The Port LLDP MED Configuration/Port Setting Table screens in Figure 4-12-12 and Figure 4-12-13 appear.

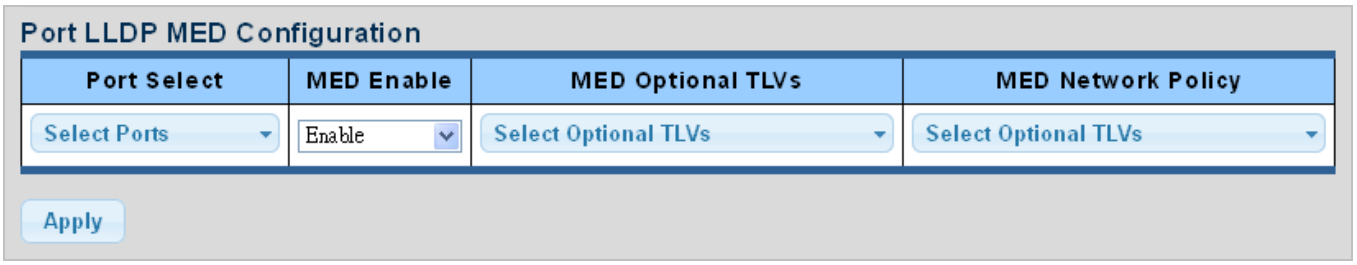


Figure 4-12-12 Port LLDP MED Configuration Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port from this drop-down list
• **MED Enable**	Enable or disable MED configuration
• **MED Optional TVLs**	Configures the information included in the MED TLV field of advertised messages. **-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. **-Location** – This option advertises location identification details. **-Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.
• **MED Network Policy**	Select MED network policy from this drop-down list

Buttons

Apply: Click to apply changes.

LLDP MED Port Setting Table

Interface	LLDP MED Status	User Defined Network Policy		Location	Inventory
		Active	Application		
GE1	Enabled	Yes		No	No
GE2	Enabled	Yes		No	No
GE3	Enabled	Yes		No	No
GE4	Enabled	Yes		No	No
GE5	Enabled	Yes		No	No
GE6	Enabled	Yes		No	No
GE7	Enabled	Yes		No	No
GE8	Enabled	Yes		No	No
GE9	Enabled	Yes		No	No
GE10	Enabled	Yes		No	No

Figure 4-12-13 Port LLDP MED Configuration Screenshot

The page includes the following fields:

Object	Description
• **Interface**	The switch port number of the logical port
• **LLDP MED Status**	Display the current LLDP MED status
• **Active**	Display the current active status
• **Application**	Display the current application
• **Location**	Display the current location
• **Inventory**	Display the current inventory

The MED Location Configuration and LLDP MED Port Location Table screens in Figure 4-12-14 and Figure 4-12-15 appear.

MED Location Configuration

Ports	Select Ports
Location Coordinate	(16 pairs of hexadecimal characters)
Location Civic Address	(6-160 pairs of hexadecimal characters)
Location ECS ELIN	(10-25 pairs of hexadecimal characters)

Apply

Figure 4-12-14 Port LLDP MED Configuration Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **Location Coordinate**	A string identifying the Location Coordinate that this entry should belong to
• **Location Civic Address**	A string identifying the Location Civic Address that this entry should belong to
• **Location ESC ELIN**	A string identifying the Location ESC ELIN that this entry should belong to

Buttons

Apply: Click to apply changes.

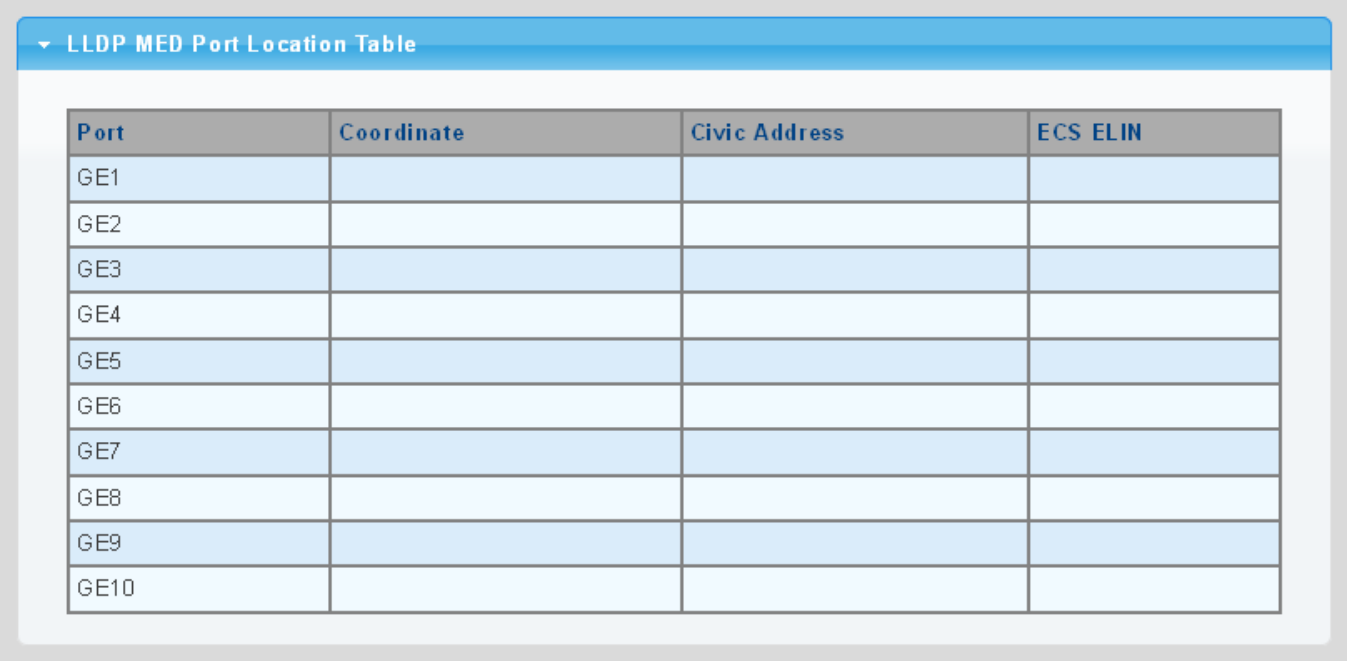


Figure 4-12-15 LLDP MED Port Location Table Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port
• **Coordinate**	Display the current coordinate
• **Civic Address**	Display the current civic address
• **ESC ELIN**	Display the current ESC ELIN

4.12.8 LLDP Overloading

The LLDP Port Overloading screen in Figure 4-12-16 appears.

LLDP Port Overloading Table

Interface	Total(Bytes)	Left to Send(Bytes)	Status	Status								
				Mandatory TLVs	MED Capabilities	MED Location	MED Network Policy	MED Extended Power via MDI	802.3 TLVs	Optional TLVs	MED Inventory	802.1 TLVs
GE1	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE2	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE3	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE4	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE5	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE6	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE7	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE8	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE9	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE10	49	1439	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)

Figure 4-12-16 LLDP Port Overloading Table Screenshot

The page includes the following fields:

Object	Description
• **Interface**	The switch port number of the logical port
• **Total (Bytes)**	Total number of bytes of LLDP information that is normally sent in a packet
• **Left to Send (Bytes)**	Total number of available bytes that can also send LLDP information in a packet
• **Status**	Gives the status of the TLVs
• **Mandatory TLVs**	Displays if the mandatory group of TLVs were transmitted or overloaded
• **MED Capabilities**	Displays if the capabilities packets were transmitted or overloaded
• **MED Location**	Displays if the location packets were transmitted or overloaded
• **MED Network Policy**	Displays if the network policies packets were transmitted or overloaded
• **MED Extended Power via MDI**	Displays if the extended power via MDI packets were transmitted or overloaded
• **802.3 TLVs**	Displays if the 802.3 TLVs were transmitted or overloaded

• **Optional TLVs**	If the LLDP MED extended power via MDI packets were sent, or if they were overloaded
• **MED Inventory**	Displays if the mandatory group of TLVs was transmitted or overloaded
• **802.1 TLVs**	Displays if the 802.1 TLVs were transmitted or overloaded

4.12.9 LLDP Statistics

Use the LLDP Device Statistics screen to general statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces. The LLDP Global and Port Statistics screens in Figure 4-12-17 and Figure 4-12-18 appear.

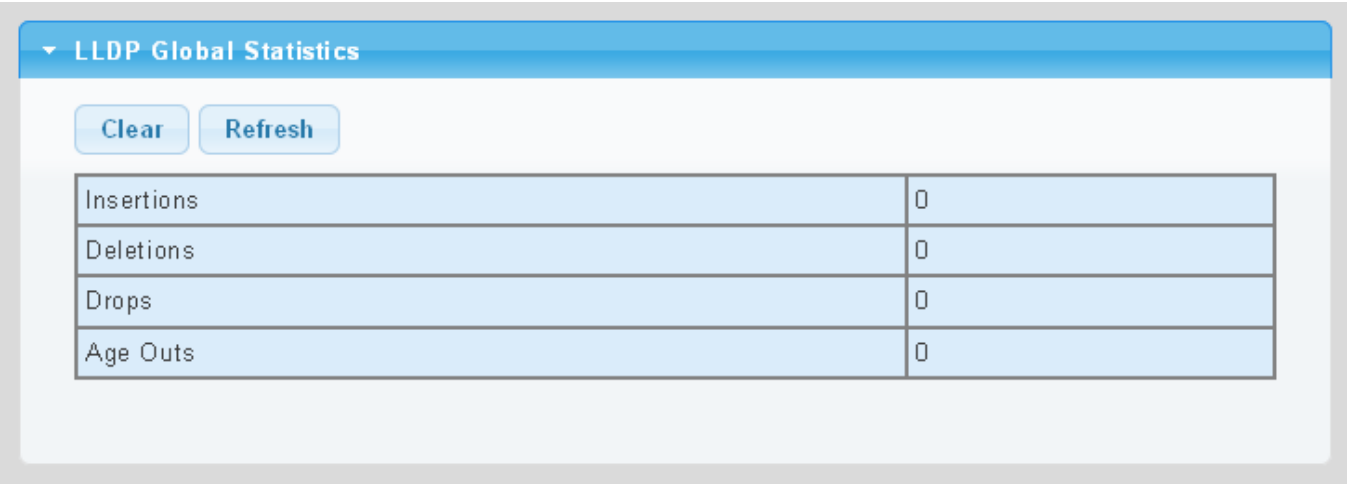


Figure 4-12-17 LLDP Global Statistics Screenshot

The page includes the following fields:

Object	Description
• **Insertions**	Shows the number of new entries added since switch reboot.\
• **Deletions**	Shows the number of new entries deleted since switch reboot.\
• **Drops**	Shows the number of LLDP frames dropped due to that the entry table was full.\
• **Age Outs**	Shows the number of entries deleted due to Time-To-Live expiring.\

Buttons

Clear: Click to clear the statistics

Refresh: Click to refresh the statistics

LLDP Port Statistics

Port	TX Frames	RX Frames			RX TLVs		RX Ageouts
	Total	Total	Discarded	Errors	Discarded	Unrecognized	Total
GE1	136	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0
GE10	0	0	0	0	0	0	0

Figure 4-12-18 LLDP Port Statistics Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port on which LLDP frames are received or transmitted
• **TX Frame – Total**	The number of LLDP frames transmitted on the port
• **RX Frame – Total**	The number of LLDP frames received on the port
• **RX Frame – Discarded**	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
• **RX Frame – Error**	The number of received LLDP frames containing some kind of error.
• **RX TLVs – Discarded**	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
• **RX TLVs – Unrecognized**	The number of well-formed TLVs, but with an unknown type value
• **RX Ageout - Total**	The number of organizationally TLVs received

4.13 Diagnostics

This section provide the Physical layer and IP layer network diagnostics tools for troubleshoot. The diagnostic tools are designed for network manager to help them quickly diagnose problems between point to point and better service customers.

Use the Diagnostics menu items to display and configure basic administrative details of the Managed Switch. Under System the following topics are provided to configure and view the system information:
This section has the following items:

- **Cable Diagnostics**
- **Ping Test**
- **IPv6 Ping Test**
- **Trace Route**

4.13.1 Cable Diagnostics

The Cable Diagnostics performs tests on copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling. There might be two statuses as follow:

- If the link is established on the twisted-pair interface in 1000Base-T mode, the Cable Diagnostics can run without disruption of the link or of any data transfer.
- If the link is established in 100Base-TX or 10Base-T, the Cable Diagnostics cause the link to drop while the diagnostics are running.

After the diagnostics are finished, the link is reestablished. And the following functions are available.

- Coupling between cable pairs.
- Cable pair termination
- Cable Length

Note

Cable Diagnostics is only accurate for cables of length from 15 to 100 meters.

The Copper test and test result screens in Figure 4-13-1 and Figure 4-13-2 appear.

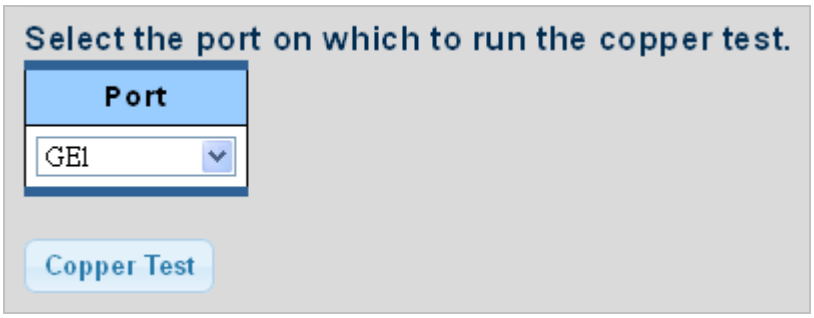


Figure 4-13-1 Copper Test Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list

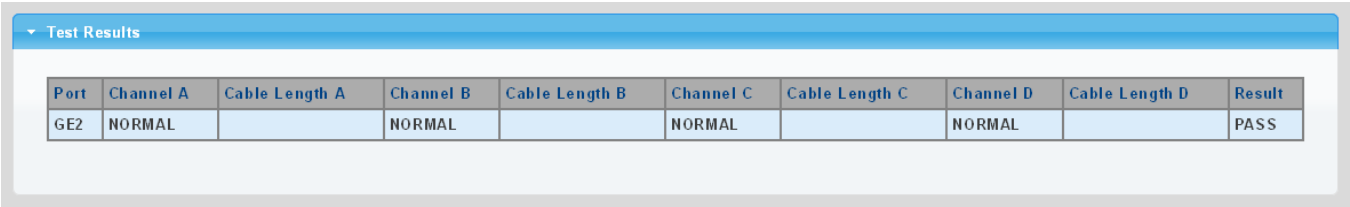


Figure 4-13-2 Test Results Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port where you are requesting Cable Diagnostics
• **Channel A~D**	Display the current channel status
• **Cable Length A~D**	Display the current cable length
• **Result**	Display the test result

4.13.2 Ping

The ping and IPv6 ping allow you to issue ICMP PING packets to troubleshoot IP connectivity issues. The Managed Switch transmits ICMP packets, and the sequence number and roundtrip time are displayed upon reception of a reply.

4.13.3 Ping Test

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press "**Apply**", ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-13-3 appears.

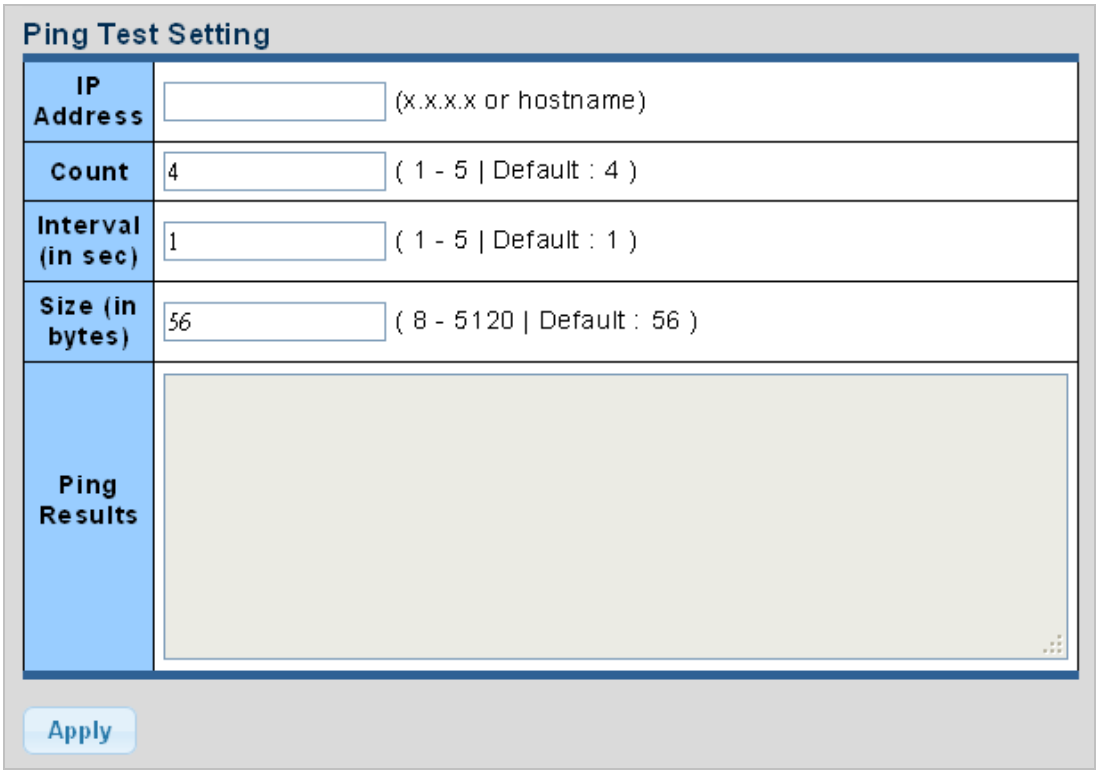


Figure 4-13-3 ICMP Ping Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address
• **Count**	Number of echo requests to send
• **Interval (in sec)**	Send interval for each ICMP packet
• **Size (in bytes)**	The payload size of the ICMP packet. Values range from 8bytes to 5120bytes.
• **Ping Results**	Display the current ping result.

Buttons

Apply: Click to transmit ICMP packets.

Note

Be sure the target IP Address is within the same network subnet of the switch, or you have to set up the correct gateway IP address.

4.13.4 IPv6 Ping Test

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press "**Apply**", 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMPv6 Ping screen in Figure 4-13-4 appears.

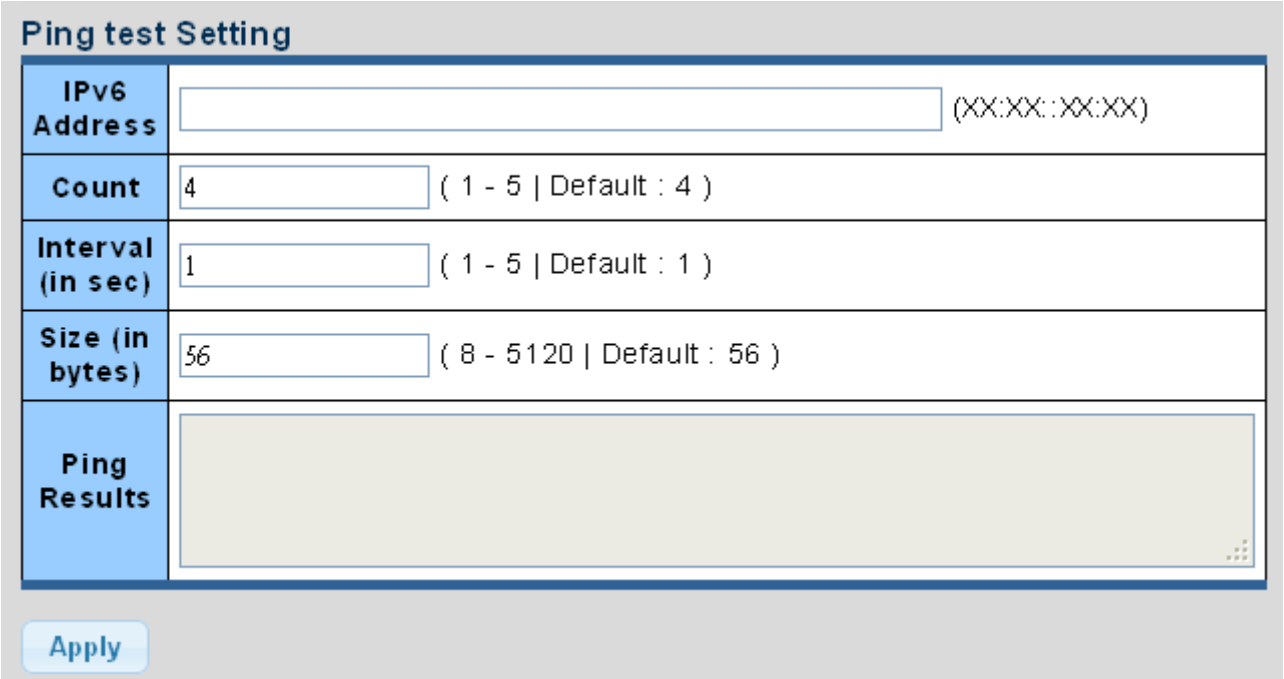


Figure 4-13-4 ICMPv6 Ping Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IPv6 Address
• **Count**	Number of echo requests to send
• **Interval (in sec)**	Send interval for each ICMP packet
• **Size (in bytes)**	The payload size of the ICMP packet. Values range from 8bytes to 5120bytes
• **Ping Results**	Display the current ping result

Buttons

Apply: Click to transmit ICMPv6 packets

4.13.5 Trace Router

Traceroute function is for testing the gateways through which the data packets travel from the source device to the destination device, so to check the network accessibility and locate the network failure.

Execution procedure of the Traceroute function consists of: first a data packet with TTL at 1 is sent to the destination address, if the first hop returns an ICMP error message to inform this packet can not be sent (due to TTL timeout), a data packet with TTL at 2 will be sent. Also the send hop may be a TTL timeout return, but the procedure will carries on till the data packet is sent to its destination. These procedures is for recording every source address which returned ICMP TTL timeout message, so to describe a path the IP data packets traveled to reach the destination. The Trace Route Setting screen in Figure 4-13-5 appears.

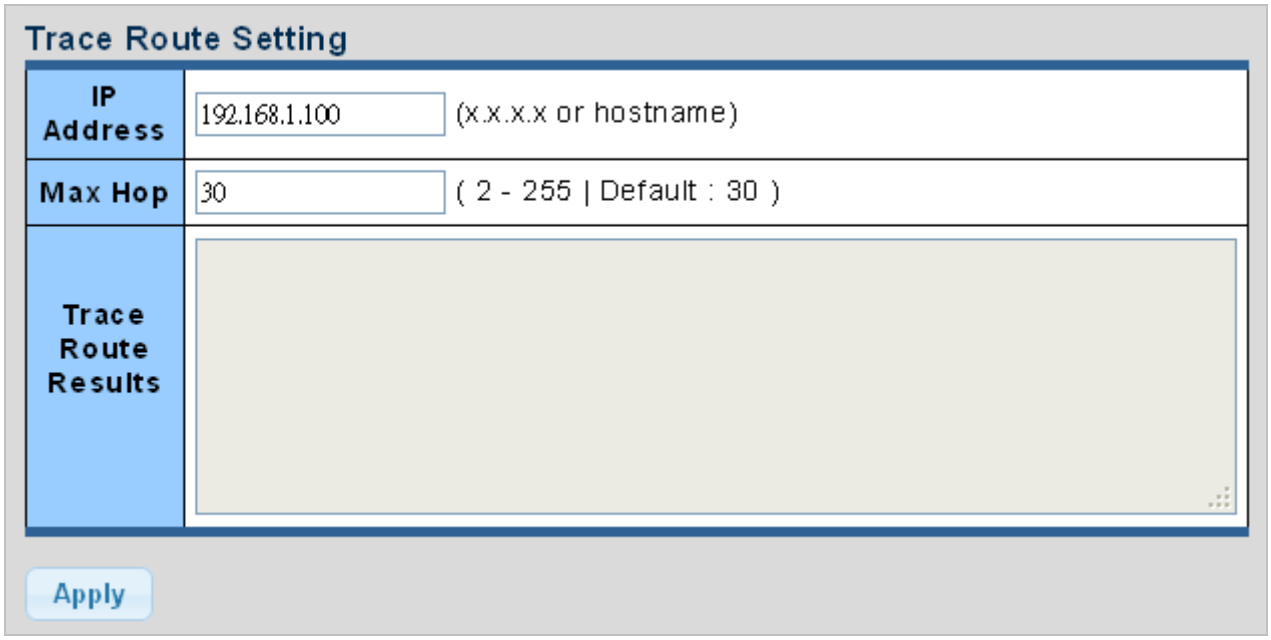


Figure 4-13-5 Trace Route Setting Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address
• **Max Hop**	The maximum gateway number allowed by traceroute function
• **Trace Route Results**	Display the current trace route result

Buttons

Apply: Click to transmit ICMPv6 packets

4.14 RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

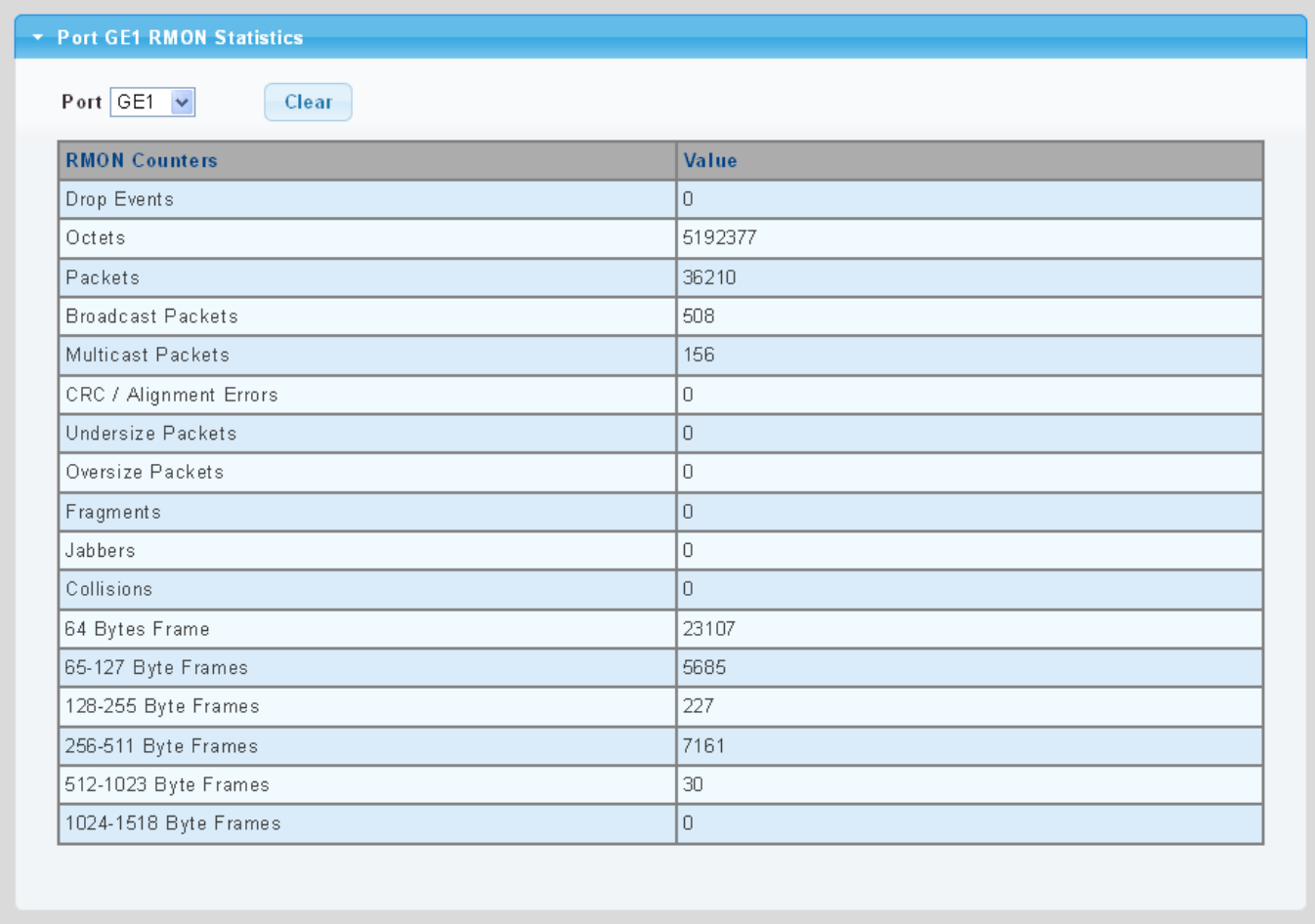
MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

- **Statistics:** Maintain basic usage and error statistics for each subnet monitored by the Agent.
- **History:** Record periodical statistic samples available from Statistics.
- **Alarm:** Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.
- **Event:** A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

4.14.1 RMON Statistics

This page provides a Detail of a specific RMON statistics entry; RMON Statistics screen in Figure 4-14-1 appears.



RMON Counters	Value
Drop Events	0
Octets	5192377
Packets	36210
Broadcast Packets	508
Multicast Packets	156
CRC / Alignment Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
64 Bytes Frame	23107
65-127 Byte Frames	5685
128-255 Byte Frames	227
256-511 Byte Frames	7161
512-1023 Byte Frames	30
1024-1518 Byte Frames	0

Figure 4-14-1: RMON Statistics Detail Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **Drop Events**	The total number of events in which packets were dropped by the probe due to lack of resources
• **Octets**	The total number of octets of data (including those in bad packets) received on the network
• **Packets**	The total number of packets (including bad packets, broadcast packets, and multicast packets) received
• **Broadcast Packets**	The total number of good packets received that were directed to the broadcast address
• **Multicast Packets**	The total number of good packets received that were directed to a multicast address
• **CRC/Alignment Errors**	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets
• **Undersize Packets**	The total number of packets received that were less than 64 octets
• **Oversize Packets**	The total number of packets received that were longer than 1518 octets
• **Fragments**	The number of frames which size is less than 64 octets received with invalid CRC
• **Jabbers**	The number of frames which size is larger than 64 octets received with invalid CRC
• **Collisions**	The best estimate of the total number of collisions on this Ethernet segment.
• **64 Bytes Frame**	The total number of packets (including bad packets) received that were 64 octets in length
• **65~127 Byte Frames**	The total number of packets (including bad packets) received that were between 65 to 127 octets in length
• **128~255 Byte Frames**	The total number of packets (including bad packets) received that were between 128 to 255 octets in length
• **256~511 Byte Frames**	The total number of packets (including bad packets) received that were between 256 to 511 octets in length
• **512~1023 Byte Frames**	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length
• **1024~1518 Byte Frames**	The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length

Buttons

Clear: Click to clear the RMON statistics

4.14.2 RMON Event

Configure RMON Event table on this page. The RMON Event screens in Figure 4-14-2 and Figure 4-14-3 appear.

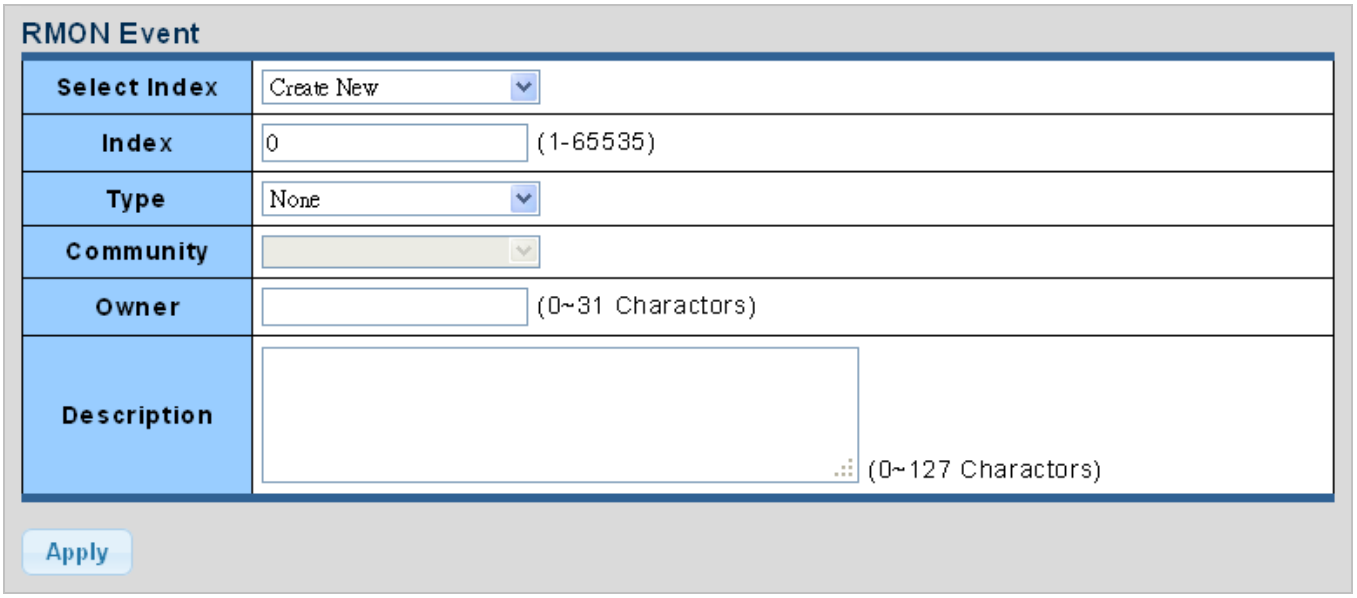


Figure 4-14-2: RMON Event Configuration Screenshot

The page includes the following fields:

Object	Description
• **Select Index**	Select index from this drop-down list to create new index or modify index
• **Index**	Indicates the index of the entry. The range is from 1 to 65535
• **Type**	Indicates the notification of the event, the possible types are: ■ **none**: The total number of octets received on the interface, including framing characters. ■ **log**: The number of uni-cast packets delivered to a higher-layer protocol. ■ **SNMP-Trap**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ■ **Log and Trap**: The number of inbound packets that are discarded even the packets are normal.
• **Community**	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
• **Owner**	Indicates the owner of this event, the string length is from 0 to 127, default is a null string
• **Description**	Indicates description of this event, the string length is from 0 to 127, default is a null string

Buttons

Apply: Click to apply changes.

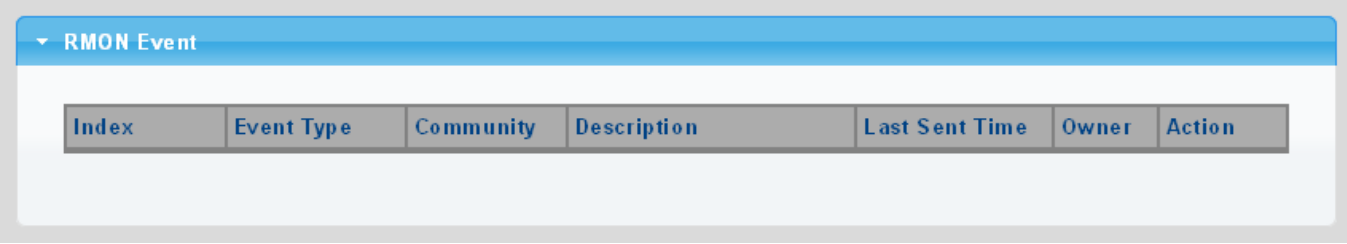


Figure 4-14-3: RMON Event Status Screenshot

The page includes the following fields:

Object	Description
• **Index**	Display the current event index
• **Event Type**	Display the current event type
• **Community**	Display the current community for SNMP trap
• **Description**	Display the current event description
• **Last Sent Time**	Display the current last sent time
• **Owner**	Display the current event owner
• **Action**	Click Delete to delete RMON event entry

4.14.3 RMON Event Log

This page provides an overview of RMON Event Log. The RMON Event Log Table screen in Figure 4-14-4 appears.

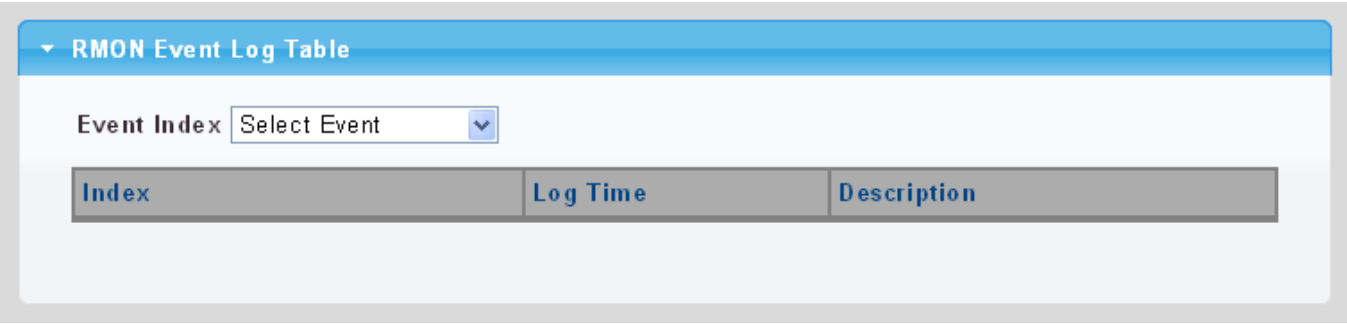


Figure 4-14-4: RMON Event Log Table Screenshot

The page includes the following fields:

Object	Description
• **Select Index**	Select index from this drop-down list
• **Index**	Indicates the index of the log entry
• **Log Time**	Indicates Event log time
• **Description**	Indicates the Event description

4.14.4 RMON Alarm

Configure RMON Alarm table on this page. The RMON Alarm screens in Figure 4-14-5 and Figure 4-14-6 appear.

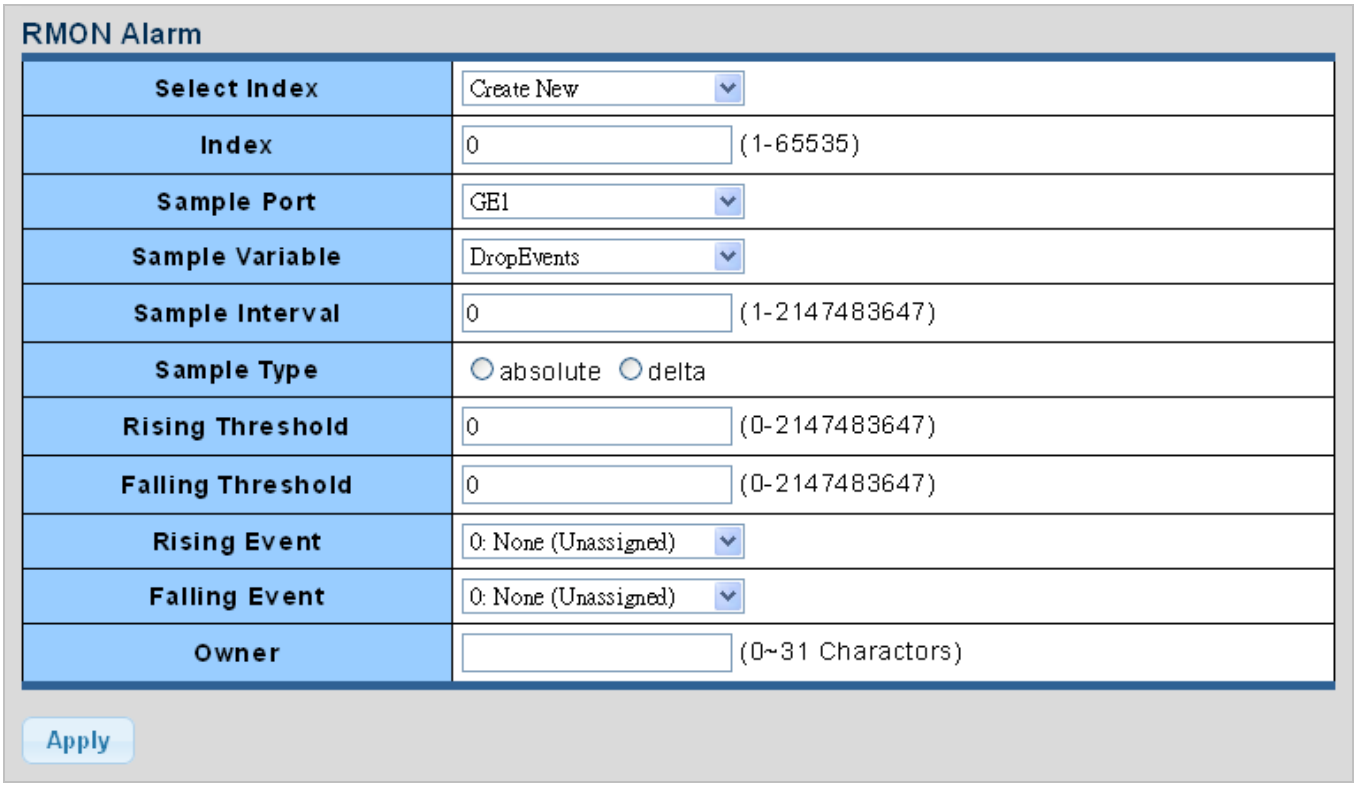


Figure 4-14-5: RMON Alarm Table Screenshot

The page includes the following fields:

Object	Description
• **Select Index**	Select index from this drop-down list to create the new index or modify the index
• **Index**	Indicates the index of the alarm entry
• **Sample Port**	Select port from this drop-down list
• **Sample Variable**	Indicates the particular variable to be sampled, the possible variables are: ■ **DropEvents**: The total number of events in which packets were dropped due to lack of resources. ■ **Octets**: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits. ■ **Pkts**: The total number of frames (bad, broadcast and multicast) received and transmitted. ■ **BroadcastPkts**: The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets. ■ **MulticastPkts**: The total number of good frames received that were directed

	to this multicast address. ■ **CRCAlignErrors**: The number of CRC/alignment errors (FCS or alignment errors). ■ **UnderSizePkts**: The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **OverSizePkts**: The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **Fragments**: The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error. ■ **Jabbers**: The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error. ■ **Collisions**: The best estimate of the total number of collisions on this Ethernet segment. ■ **Pkts64Octets**: The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets). ■ **Pkts64to172Octets**: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets). ■ **Pkts158to255Octets**: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets). ■ **Pkts256to511Octets**: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets). ■ **Pkts512to1023Octets**: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets). ■ **Pkts1024to1518Octets**: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets).
• **Sample Interval**	Sample interval (1–2147483647)
• **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: ■ **Absolute**: Get the sample directly (default).

	■ **Delta**: Calculate the difference between samples.
• **Rising Threshold**	Rising threshold value (0–2147483647)
• **Falling Threshold**	Falling threshold value (0–2147483647)
• **Rising Event**	Event to fire when the rising threshold is crossed
• **Falling Event**	Event to fire when the falling threshold is crossed
• **Owner**	Specify an owner for the alarm

Buttons

Apply: Click to apply changes.

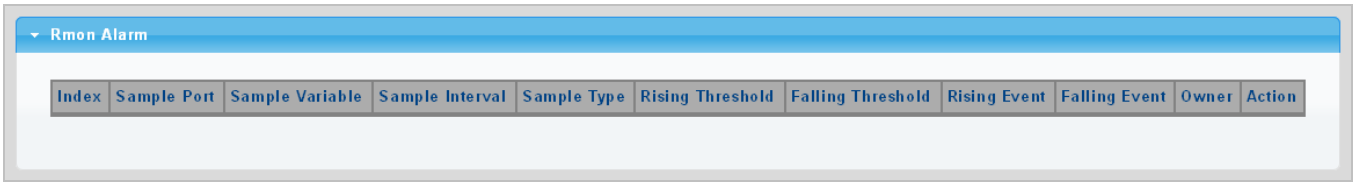


Figure 4-14-6: RMON Alarm Status Screenshot

The page includes the following fields:

Object	Description
• **Index**	Indicates the index of Alarm control entry
• **Sample Port**	Display the current sample port
• **Sample Variable**	Display the current sample variable
• **Sample Interval**	Display the current interval
• **Sample Type**	Display the current sample type
• **Rising Threshold**	Display the current rising threshold
• **Falling Threshold**	Display the current falling threshold
• **Rising Event**	Display the current rising event
• **Falling Event**	Display the current falling event
• **Owner**	Display the current owner
• **Action**	Click Delete to delete RMON alarm entry

4.14.5 RMON History

Configure RMON History table on this page. The RMON History screens in Figure 4-14-7 and Figure 4-14-8 appear.

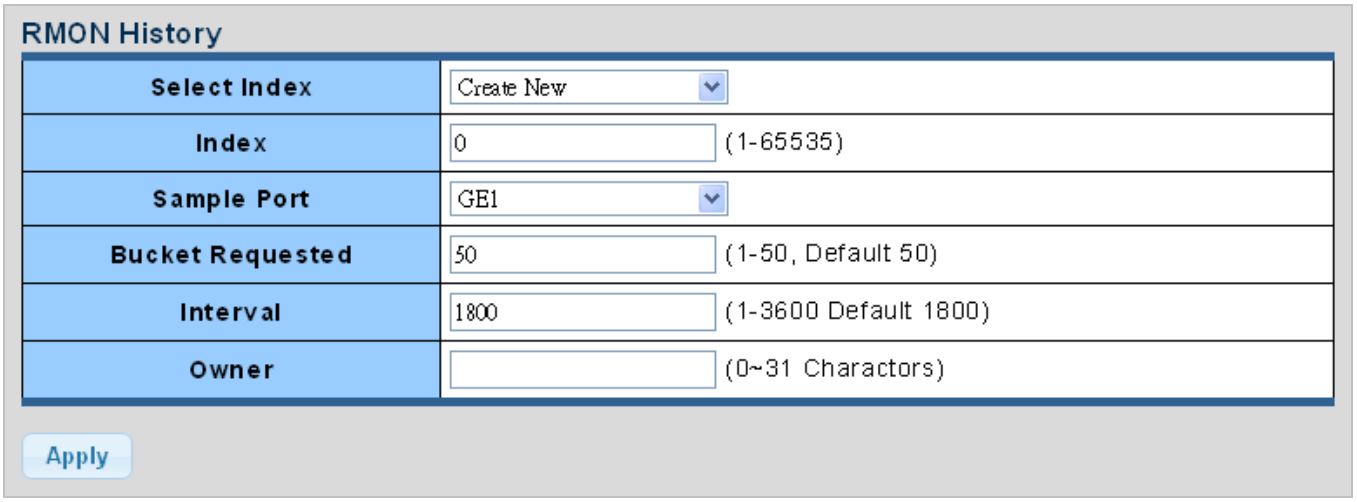


Figure 4-14-7: RMON History Table Screenshot

The page includes the following fields:

Object	Description
• **Select Index**	Select index from this drop-down list to create the new index or modify the index
• **Index**	Indicates the index of the history entry
• **Sample Port**	Select port from this drop-down list
• **Bucket Requested**	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 50, default value is 50
• **Interval**	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
• **Owner**	Specify an owner for the history

Buttons

Apply: Click to apply changes.

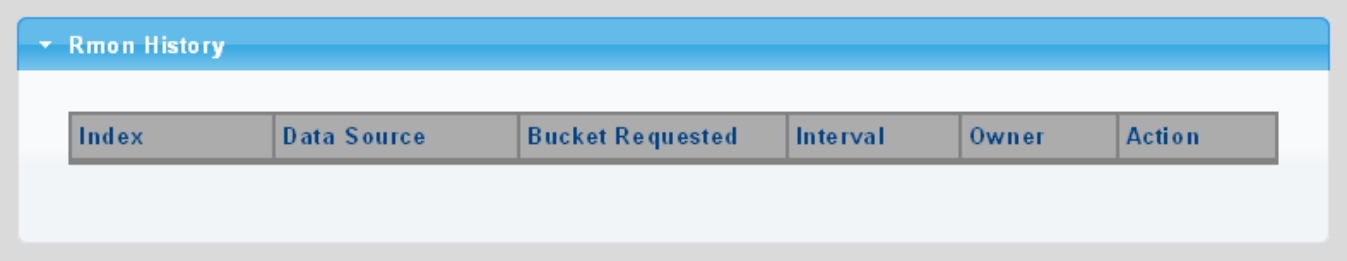


Figure 4-14-8: RMON History Status Screenshot

The page includes the following fields:

Object	Description
• **Index**	Display the current index
• **Data Source**	Display the current data source
• **Bucket Requested**	Display the current bucket requested
• **Interval**	Display the current interval
• **Owner**	Display the current owner
• **Action**	Click Delete to delete RMON history entry.

4.14.6 RMON History Log

This page provides a detail of RMON history entries; screen in Figure 4-14-9 appears.

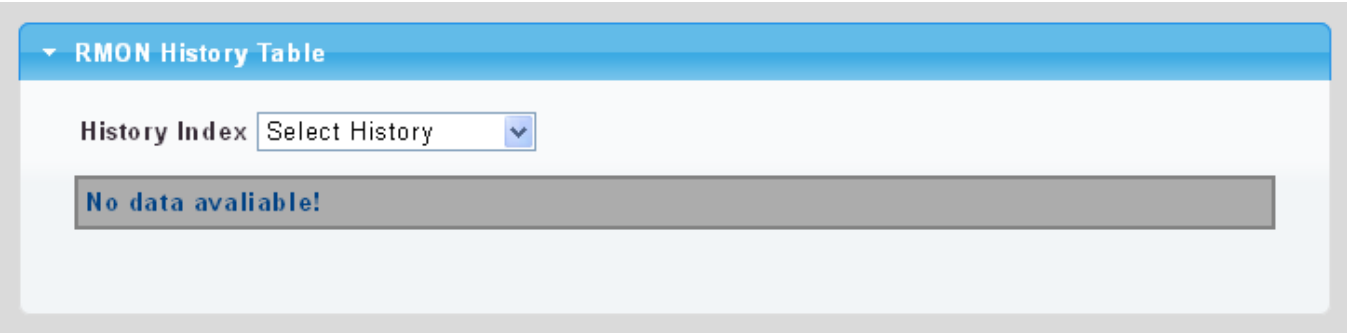


Figure 4-14-9: RMON History Status Screenshot

The page includes the following fields:

Object	Description
• **History Index**	Select history index from this drop-down list

Buttons

Apply: Click to apply changes.

4.15 Power over Ethernet

The GS-4210 PoE Switch Series can easily build a power central-controlled IP phone system, IP camera system and AP group for the enterprise. For instance, cameras / APs can be easily installed around the corner in the company for surveillance demands or build a wireless roaming environment in the office. Without the power-socket limitation, the GS-4210 PoE Switch Series makes the installation of cameras or WLAN APs easier and more efficient.

PoE Power Budget list for GS-4210 PoE switch series

Model Name	PoE Budget @ 25 degrees C	PoE Budget @ 50 degrees C
GS-4210-8P2T2S	120 watts	100 watts
GS-4210-8P2T2S	240 watts	200 watts
GS-4210-16P4C	220 watts	190 watts
GS-4210-24P4C	220 watts	190 watts
GS-4210-24PL4C	440 watts	380 watts

Figure 4-16-1: Power over Ethernet Status

4.15.1 Power over Ethernet Powered Device

 3~5 watts	**Voice over IP phones** Enterprise can install POE VoIP Phone, ATA and other Ethernet/non-Ethernet end-devices in the central area where UPS is installed for un-interruptible power system and power control system.
 6~12 watts	**Wireless LAN Access Points** Museums, sightseeing spots, airports, hotels, campuses, factories, and warehouses can install the Access Point anywhere.
 10~12 watts	**IP Surveillance** Enterprises, museums, campuses, hospitals and banks can install IP camera without the limit of the installation location. Electrician is not needed to install AC sockets.
 3~12 watts	**PoE Splitter** PoE Splitter splits the PoE 56V DC over the Ethernet cable into 5/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
 3~25 watts	**High Power PoE Splitter** High PoE Splitter splits the PoE 56V DC over the Ethernet cable into 24/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
 30 watts	**High Power Speed Dome** This state-of-the-art design is considerable to fit in various network environments like traffic centers, shopping malls, railway stations, warehouses, airports, and production facilities for the most demanding outdoor surveillance applications. Electrician is not needed to install AC sockets.

Note

Since the GS-4210 PoE Switch Series per PoE port supports 56V DC PoE power output, please check and assure the Powered Device's (PD) acceptable DC power range is 56V DC; otherwise, it will damage the Powered Device (PD).

4.15.2 System Configuration

In a power over Ethernet system, operating power is applied from a power source (PSU-power supply unit) over the LAN infrastructure to **powered devices (PDs)**, which are connected to ports. Under some conditions, the total output power required by PDs can exceed the maximum available power provided by the PSU. The system with a PSU is capable of supplying less power than the total potential power consumption of all the PoE ports in the system. In order to maintain the function of the majority of the ports, power management is implemented.

The PSU input power consumption is monitored by measuring voltage and current .The input power consumption is equal to the system's aggregated power consumption .The power management concept allows all ports to be active and activates additional ports, as long as the aggregated power of the system is lower than the power level at which additional PDs cannot be connected .When this value is exceeded, ports will be deactivated, according to user-defined priorities. The power budget is managed according to the following user-definable parameters: maximum available power, ports priority and maximum allowable power per port.

Reserved Power

There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports.

- **Classification mode**

  In this mode each port automatic determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 and 30.8 watts.

Class	Usage	Range of maximum power used by the PD	Class Description
0	Default	0.44 to 12.95 watts	Classification unimplement
1	Optional	0.44 to 3.84 watts	Very low power
2	Optional	3.84 to 6.49 watts	Low power
3	Optional	6.49 to 12.95 watts (or to 15.4 watts)	Mid power
4	Optional	12.95 to 25.50 watts (or to 30.8 watts)	High power

Table 4-16-1: Standard PoE Parameters and Comparison

Note

1. In this mode the **Maximum Power fields** have no effect.
2. The PoE chip of PD69008 / PD69012 designed to that Class level 0 will be assigned to 15.4 watts in AF mode and 30.8 watts in AT mode under classification power limit mode. It is hardware limited.

- **Allocation mode**

  In this mode, the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. The ports are shut down when total reserved power exceeds the amount of power that the power supply can deliver.

Note

In this mode, the port power is not turned on if the PD requests more available power.

4.15.3 Power over Ethernet Configuration

This section allows the user to inspect and configure the current PoE configuration setting as screen in Figure 4-16-1 appears.

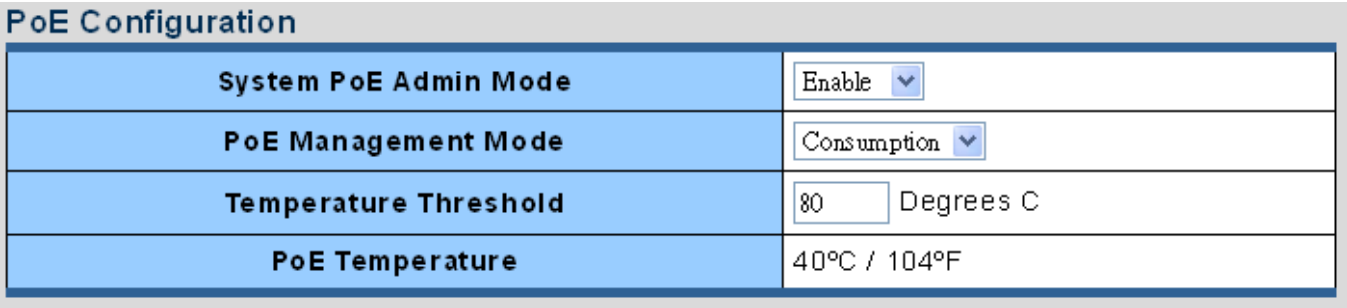


Figure 4-16-1: PoE Configuration Screenshot

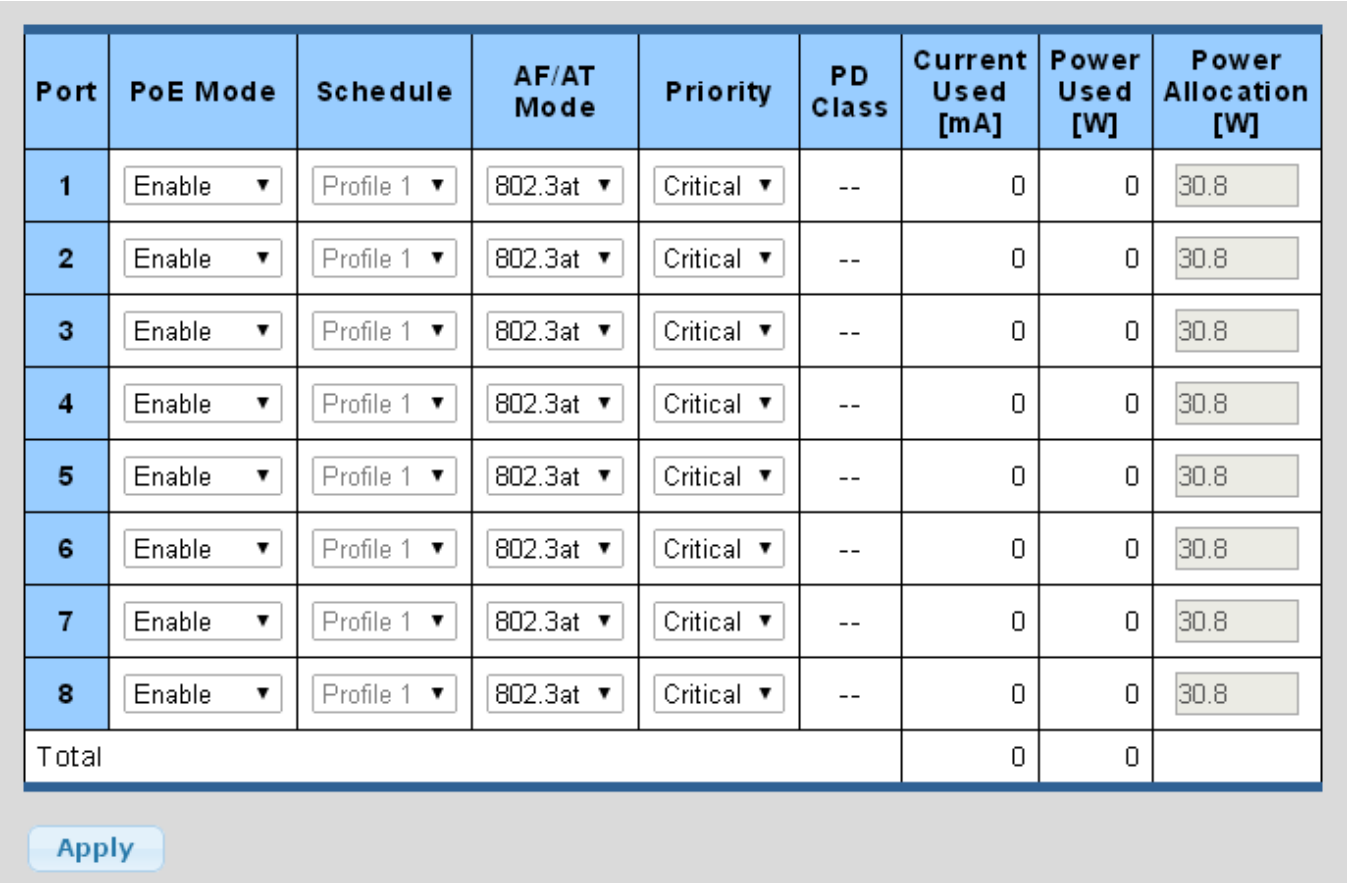
The page includes the following fields:

Object	Description
• **System PoE Admin Mode**	Allows user to enable or disable PoE function. It will cause all of PoE ports to supply or not to supply power.
• **PoE Management Mode**	There are six modes for configuring how the ports/PDs may reserve power and when to shut down ports. ■ **Classification mode:** The system reserves PoE power to PD according to PoE class level. ■ **Consumption mode:** The system offers PoE power according to PD real power consumption. ■ **Allocation mode:** Users allow to assign how much PoE power to each port and the system will reserve PoE power to PD.
• **Temperature Threshold**	Allows setting over temperature protection threshold value. If the system temperature is overly high, the system will lower the total PoE power budget automatically.
• **PoE Temperature**	Display the PoE Chip Temperature

This section displays the **PoE Power Usage** of Current Power Consumption as Figure 4-16-2 shows.

Figure 4-16-2: Current Power Consumption Screenshot

This section allows the user to inspect and configure the current PoE port settings as Figure 4-16-3 shows.



Port	PoE Mode	Schedule	AF/AT Mode	Priority	PD Class	Current Used [mA]	Power Used [W]	Power Allocation [W]
1	Enable	Profile 1	802.3at	Critical	--	0	0	30.8
2	Enable	Profile 1	802.3at	Critical	--	0	0	30.8
3	Enable	Profile 1	802.3at	Critical	--	0	0	30.8
4	Enable	Profile 1	802.3at	Critical	--	0	0	30.8
5	Enable	Profile 1	802.3at	Critical	--	0	0	30.8
6	Enable	Profile 1	802.3at	Critical	--	0	0	30.8
7	Enable	Profile 1	802.3at	Critical	--	0	0	30.8
8	Enable	Profile 1	802.3at	Critical	--	0	0	30.8
Total						0	0	

Apply

Figure 4-16-3: Power over Ethernet Configuration Screenshot

The page includes the following fields:

Object	Description
• **PoE Mode**	There are three modes for PoE mode. ■ **Enable**: enable PoE function.. ■ **Disable**: disable PoE function. ■ **Schedule**: enable PoE function in schedule mode.
• **Schedule**	Indicates the scheduled profile mode. Possible profiles are: ■ **Profile1** ■ **Profile2** ■ **Profile3** ■ **Profile4**
• **AF/AT Mode**	Allows user to select 802.3at or 802.3af compatibility mode. The default value is 802.3at mode. This function will affect PoE power reservation in Classification power limit mode

	only, as **802.3af mode**, the system is going to reserve a maximum of **15.4W** for PD that supports Class3 level. As IEEE **802.3at mode**, the system is going to reserve **30.8 watts** for PD that supports Class4 level. From class1 to class3 level in the 802.3at mode, it will reserve the same PoE power as in 802.3af mode.
• **Priority**	The Priority represents PoE ports priority. There are three levels of power priority named **Low**, **High** and **Critical**. The priority is used in case the total power consumption is over the total power budget. In this case the port with the lowest priority will be turned off, and offer power for the port of higher priority.
• **PD Class**	Displays the class of the PD attached to the port, as established by the classification process. Class 0 is the default for PDs. The PD is powered based on PoE Class level if the system is working in Classification mode. The PD will return to Class 0 to 4 in accordance with the maximum power draw as specified by **Table 4-16-1**.
• **Current Used [mA]**	The **Power Used** shows how much current the PD currently is using.
• **Power Used [W]**	The **Power Used** shows how much power the PD currently is using.
• **Power Allocation**	It can limit the port PoE supply watts. Per port maximum value must be less than **30.8 watts**. Total port values must be less than the Power Reservation value. Once power overload is detected, the port will auto shut down and keep in detection mode until PD's power consumption is lower than the power limit value

Buttons

Apply: Click to apply changes.

4.15.4 PoE Schedule

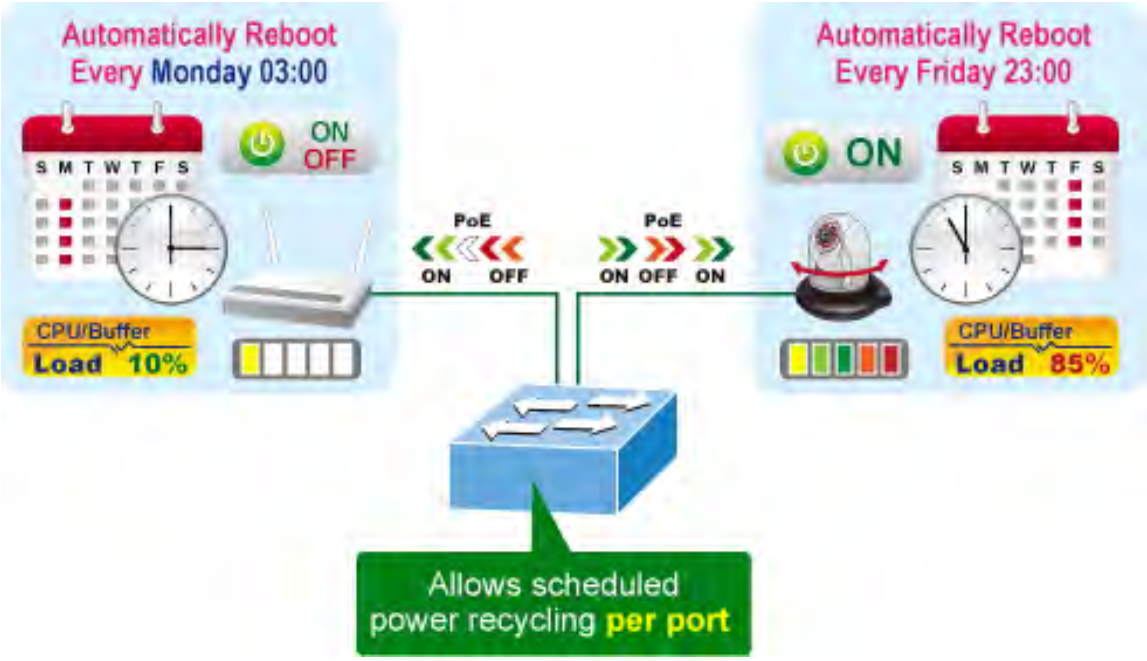
This page allows the user to define PoE schedule and scheduled power recycling.

PoE Schedule

Besides being used as an IP Surveillance, the Managed PoE switch is certainly applicable to construct any PoE network including VoIP and Wireless LAN. Under the trend of energy saving worldwide and contributing to the environmental protection on the Earth, the Managed PoE switch can effectively control the power supply besides its capability of giving high watts power. The "**PoE schedule**" function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMB or Enterprise saving power and money.

Scheduled Power Recycling

The Managed PoE switch allows each of the connected PoE IP cameras to reboot at a specified time each week. Therefore, it will reduce the chance of IP camera crash resulting from buffer overflow.



The screen in Figure 4-16-4 appears.

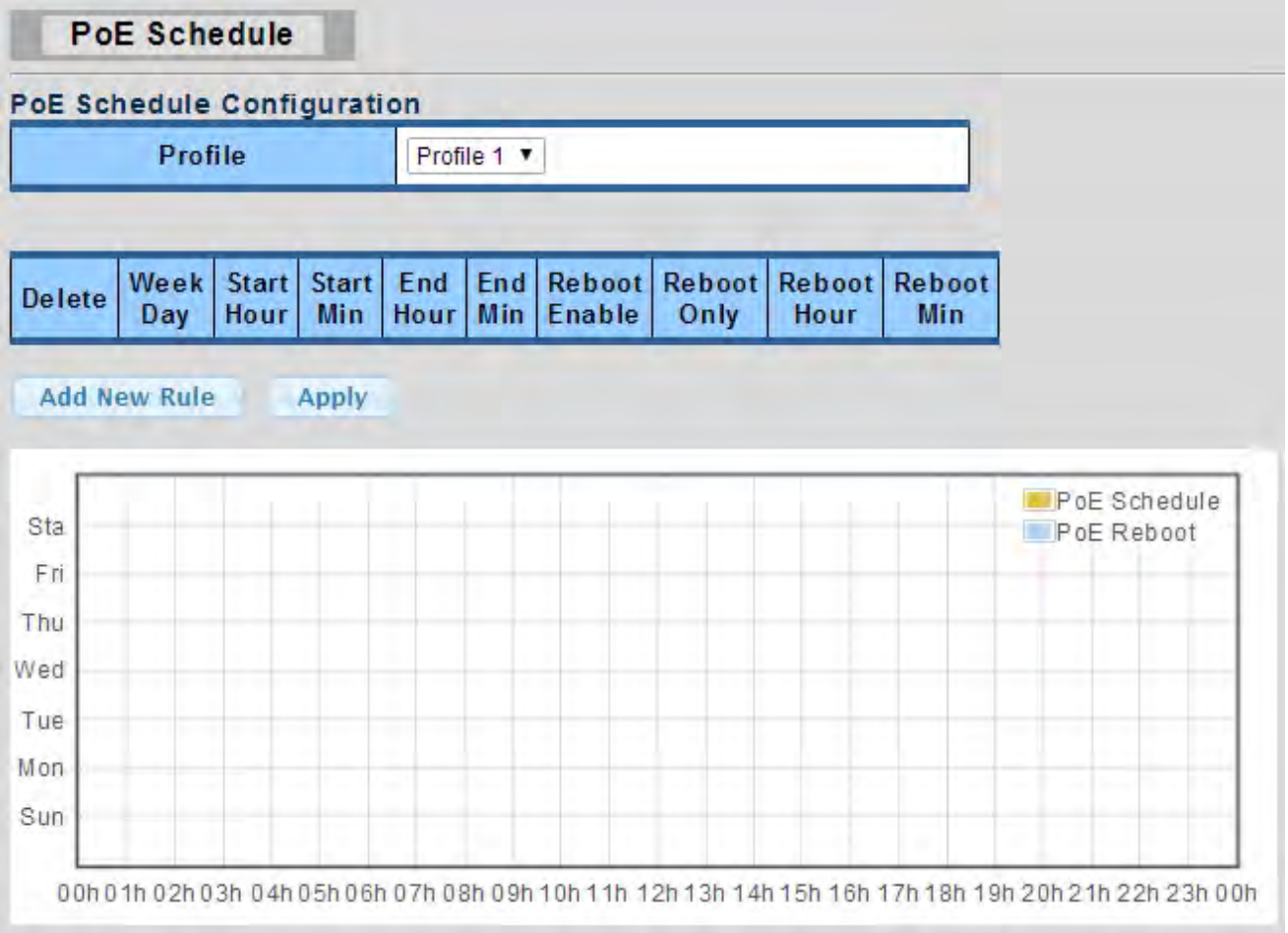


Figure 4-16-4: PoE Schedule Screenshot

Please press **Add New Rule** button to start setting PoE Schedule function. You have to set PoE schedule to profile and then go back to PoE Port Configuration, and select "**Schedule**" mode from per port "**PoE Mode**" option to enable you to indicate which schedule profile could be applied to the PoE port.

The page includes the following fields:

Object	Description
• **Profile**	Set the schedule profile mode. Possible profiles are: **Profile1** **Profile2** **Profile3** **Profile4**
• **Week Day**	Allows user to set week day for defining PoE function by enabling it on the day.
• **Start Hour**	Allows user to set what hour PoE function does by enabling it.

• **Start Min**	Allows user to set what minute PoE function does by enabling it.
• **End Hour**	Allows user to set what hour PoE function does by disabling it.
• **End Min**	Allows user to set what minute PoE function does by disabling it.
• **Reboot Enable**	Allows user to enable or disable the whole PoE port reboot by PoE reboot schedule. Please note that if you want PoE schedule and PoE reboot schedule to work at the same time, please use this function, and don't use **Reboot Only** function. This function offers administrator to reboot PoE device at an indicated time if administrator has this kind of requirement.
• **Reboot Only**	Allows user to reboot PoE function by PoE reboot schedule. Please note that if administrator enables this function, PoE schedule will not set time to profile. This function is just for PoE port to reset at an indicated time.
• **Reboot Hour**	Allows user to set what hour PoE reboots. This function is only for PoE reboot schedule.
• **Reboot Min**	Allows user to set what minute PoE reboots. This function is only for PoE reboot schedule.

Buttons

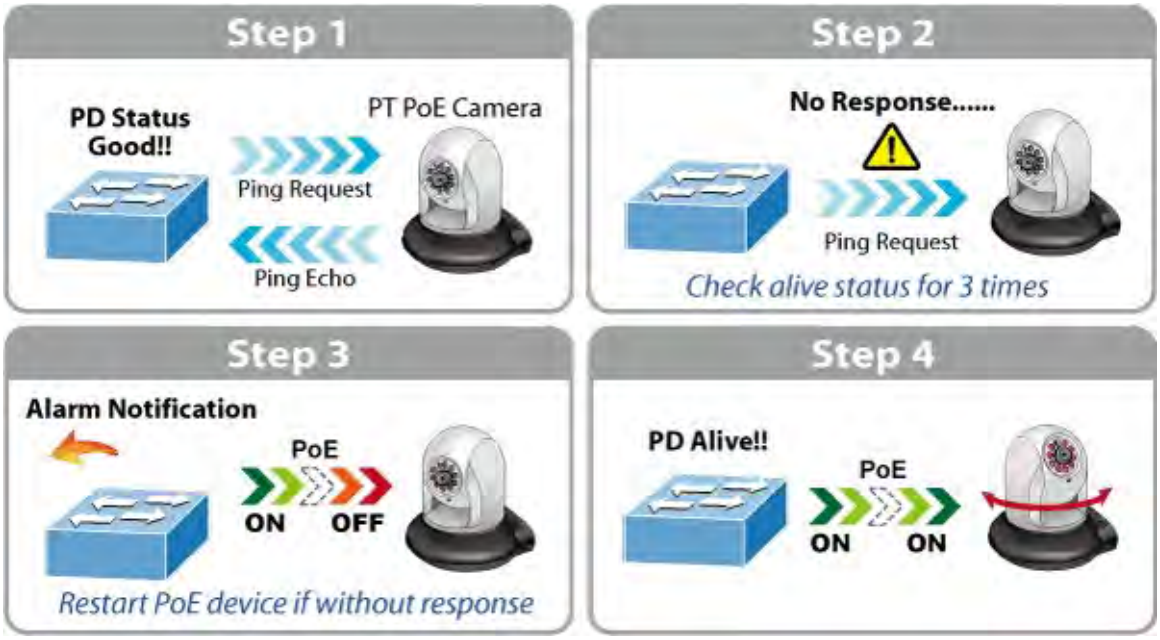
Add New Rule : Click to add new rule.

Apply : Click to apply changes

Delete : Check to delete the entry.

4.15.5 PoE Alive Check Configuration

The GS-4210 PoE Switch Series can be configured to monitor connected PD's status in real-time via ping action. Once the PD stops working and without response, the PoE Switch is going to restart PoE port power, and bring the PD back to work. It will greatly enhance the reliability and reduces administrator management burden.



This page provides you with how to configure PD Alive Check. The screen in Figure 4-16-5 appears.

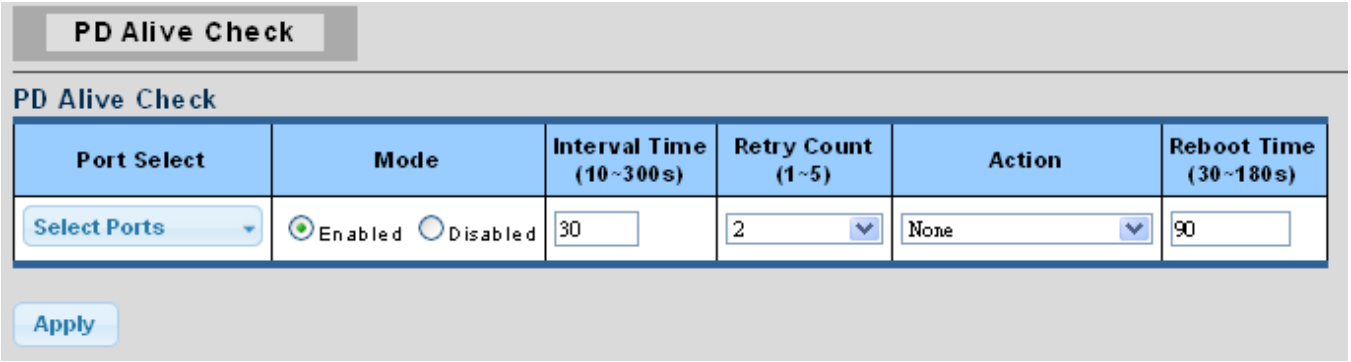


Figure 4-15-5: PD Alive Check Configuration Screenshot

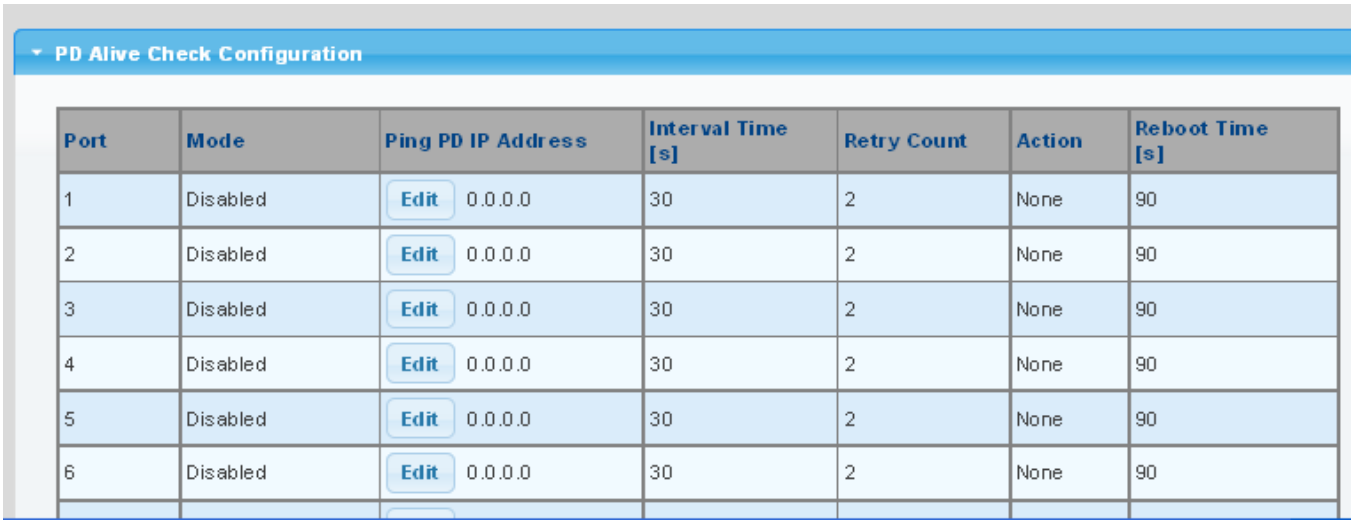
The page includes the following fields:

Object	Description
• **Mode**	Allows user to enable or disable per port PD Alive Check function. By default, all ports are disabled.
• **Ping PD IP Address**	This column allows user to set PoE device IP address for system making ping to the PoE device. Please note that the PD's IP address must be set to the same network segment with the PoE Switch.

• **Interval Time (10~300s)**	This column allows user to set how long system should issue a ping request to PD for detecting whether PD is alive or dead. Interval time range is from 10 seconds to 300 seconds.
• **Retry Count (1~5)**	This column allows user to set the number of times system retries ping to PD. For example, if we set count 2, it means that if system retries ping to the PD and the PD doesn't response continuously, the PoE port will be reset.
• **Action**	Allows user to set which action will be applied if the PD is without any response. The PoE Switch Series offers the following 3 actions: ■ **PD Reboot:** It means system will reset the PoE port that is connected to the PD. ■ **PD Reboot and Alarm:** It means system will reset the PoE port and issue an alarm message via Syslog. ■ **Alarm:** It means system will issue an alarm message via Syslog.
• **Reboot Time (30~180s)**	This column allows user to set the PoE device rebooting time as there are so many kinds of PoE devices on the market and they have a different rebooting time. The PD Alive-check is not a defining standard, so the PoE device on the market doesn't report reboot done information to the PoE Switch. Thus, user has to make sure how long the PD will take to finish booting, and then set the time value to this column. System is going to check the PD again according to the reboot time. If you are not sure of the precise booting time, we suggest you set it longer.

Buttons

Apply: Click to apply changes.



Port	Mode	Ping PD IP Address	Interval Time [s]	Retry Count	Action	Reboot Time [s]
1	Disabled	Edit 0.0.0.0	30	2	None	90
2	Disabled	Edit 0.0.0.0	30	2	None	90
3	Disabled	Edit 0.0.0.0	30	2	None	90
4	Disabled	Edit 0.0.0.0	30	2	None	90
5	Disabled	Edit 0.0.0.0	30	2	None	90
6	Disabled	Edit 0.0.0.0	30	2	None	90

Figure 4-15-6: PD Alive Check Configuration Screenshot

4.16 Maintenance

Use the Maintenance menu items to display and configure basic configurations of the Managed Switch. Under maintenance, the following topics are provided to back up, upgrade, save and restore the configuration. This section has the following items:

- **Factory Default** — You can reset the configuration of the switch on this page.
- **Reboot Switch** — You can restart the switch on this page. After restart, the switch will boot normally.
- **Backup Manager** — You can back up the switch configuration.
- **Upgrade Manager** — You can upgrade the switch configuration.
- **Dual Image** — Select active or backup image on this page.

4.16.1 Factory Default

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in Figure 4-15-1 appears and click to reset the configuration to Factory Defaults.

Figure 4-15-1 Factory Default Screenshot

After the "**Factory**" button is pressed and rebooted, the system will load the default IP settings as follows:

- Default IP address: **192.168.0.100**
- Subnet mask: **255.255.255.0**
- Default Gateway: **192.168.0.254**
- The other setting value is back to disable or none.

To reset the Managed Switch to the Factory default setting, you can also press the hardware reset button at the front panel about 10 seconds. After the device be rebooted. You can login the management WEB interface within the same subnet of 192.168.0.xx.

4.16.2 Reboot Switch

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user has to re-login the Web interface for about 60 seconds. The Reboot Switch screen in Figure 4-16-2 appears and click to reboot the system.

Figure 4-16-2 Reboot Switch Screenshot

4.16.3 Backup Manager

This function allows backup of the current image or configuration of the Managed Switch to the local management station. The Backup Manager screen in Figure 4-16-3 appears.

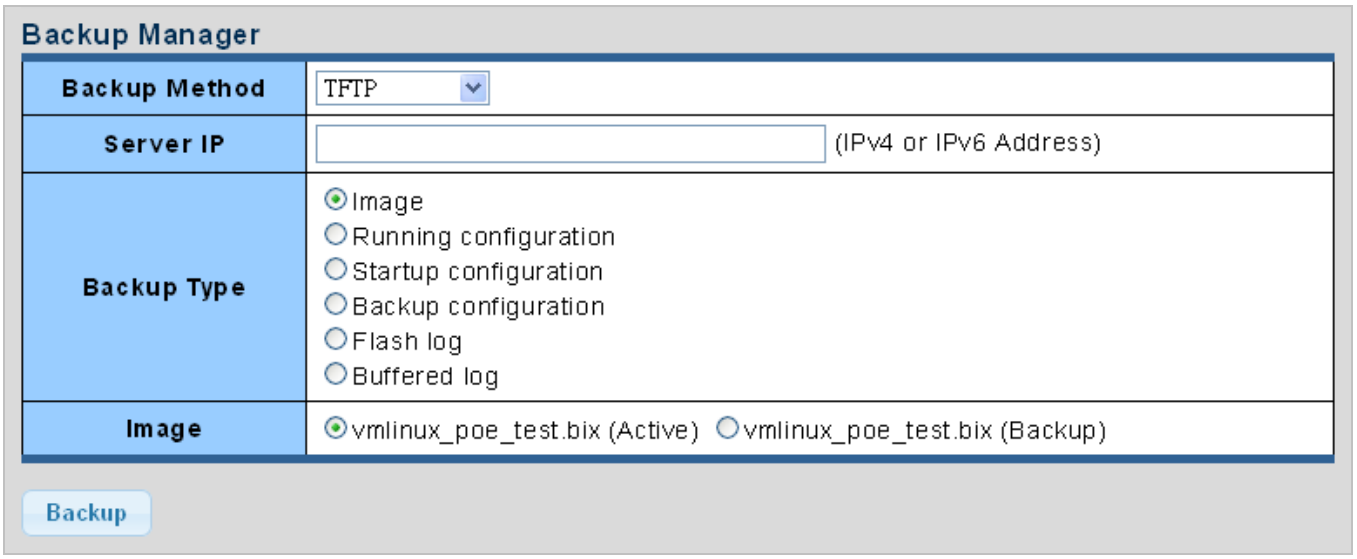


Figure 4-16-3 Backup Manager Screenshot

The page includes the following fields:

Object	Description
• **Backup Method**	Select backup method from this drop-down list.
• **Server IP**	Fill in your TFTP server IP address.
• **Backup Type**	Select backup type.
• **Image**	Select active or backup image.

Buttons

Backup: Click to back up image, configuration or log.

4.16.4 Upgrade Manager

This function allows reloading of the current image or configuration of the Managed Switch to the local management station. The Upgrade Manager screen in Figure 4-16-4 appears.

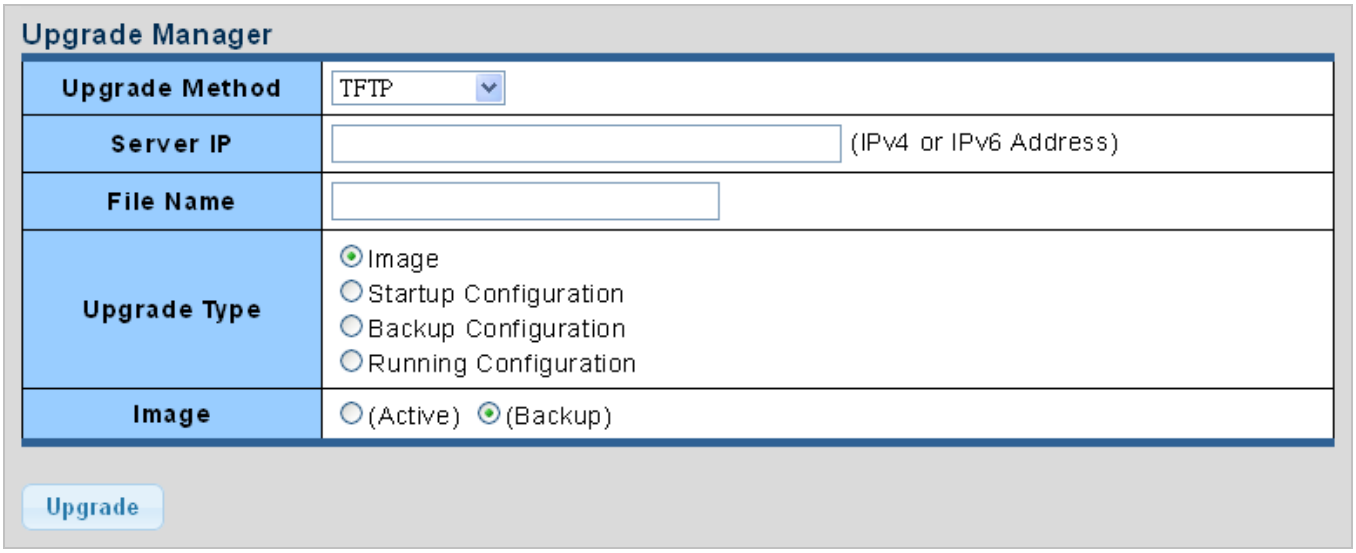


Figure 4-16-4 Upgrade Manager Screenshot

The page includes the following fields:

Object	Description
• **Upgrade Method**	Select upgrade method from this drop-down list.
• **Server IP**	Fill in your TFTP server IP address.
• **File Name**	The name of firmware image or configuration.
• **Upgrade Type**	Select upgrade type.
• **Image**	Select active or backup image.

Buttons

Upgrade: Click to upgrade image or configuration.

4.16.5 Dual Image

This page provides information about the active and backup firmware images in the device, and allows you to revert to the backup image. The web page displays two tables with information about the active and backup firmware images. The Dual Image Configuration and Information screens in Figure 4-16-5 and Figure 4-16-6 appear.

Figure 4-15-5: Dual Image Configuration Screenshot

The page includes the following fields:

Object	Description
• **Active Image**	Select the active or backup image

Buttons

Apply: Click to apply active image.

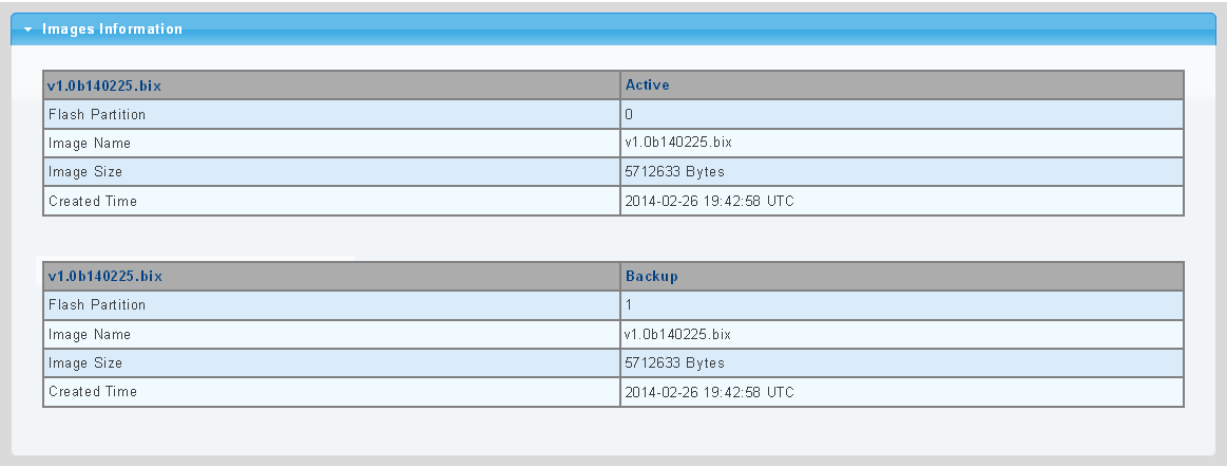


Figure 4-16-6: Dual Image Information Screenshot

The page includes the following fields:

Object	Description
• **Flash Partition**	Display the current flash partition
• **Image Name**	Display the current image name
• **Image Size**	Display the current image size
• **Created Time**	Display the created time

5. SWITCH OPERATION

5.1 Address Table

The Switch is implemented with an address table. This address table is composed of many entries. Each entry is used to store the address information of some nodes on the network, including MAC address, port no, etc. This information comes from the learning process of Ethernet Switch.

5.2 Learning

When one packet comes in from any port, the Switch will record the source address, port number and the other related information in the address table. This information will be used to decide either forwarding or filtering for future packets.

5.3 Forwarding and Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will look up the address table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at a different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from the address table. But, if the destination address is located at the same port with this packet, then this packet will be filtered, thereby increasing the network throughput and availability

5.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer and does the complete error checking before transmission. Therefore, no error packets occur. It is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existence hubs, which nearly always improves the overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using the conventional cabling and adapters.

Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet is stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduces the overall load on the network.

The Switch performs "Store and forward"; therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

5.5 Auto-Negotiation

The STP ports on the Switch have a built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detecting the modes and speeds when both devices are connected. Both 10BASE-T and 100BASE-TX devices can connect with the port in either half- or full-duplex mode.

If attached device is:	100BASE-TX port will set to:
10Mbps, without auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10BASE-T/full-duplex)
100Mbps, without auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100BASE-TX/full-duplex)

6. TROUBLESHOOTING

This chapter contains information to help you solve your issue. If the Managed Switch is not functioning properly, make sure the Managed Switch is set up according to instructions in this manual.

■ **The Link LED is not lit**

Solution:

Check the cable connection and remove duplex mode of the Managed Switch

■ **Some stations cannot talk to other stations located on the other port**

Solution:

Please check the VLAN settings, trunk settings, or port enabled / disabled status.

■ **Performance is bad**

Solution:

Check the full duplex status of the Managed Switch. If the Managed Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ **Why the Switch doesn't connect to the network**

Solution:

1. Check the LNK/ACT LED on the Managed Switch
2. Try another port on the Managed Switch
3. Make sure the cable is installed properly
4. Make sure the cable is the right type
5. Turn off the power. After a while, turn on power again

■ **100BASE-TX port link LED is lit, but the traffic is irregular**

Solution:

Check that the attached device is not set to full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

■ **Switch does not power up**

Solution:

1. AC power cord is not inserted or faulty
2. Check whether the AC power cord is inserted correctly
3. Replace the power cord if the cord is inserted correctly. Check whether the AC power source is working by connecting a different device in place of the switch.

4. If that device works, refer to the next step.
5. If that device does not work, check the AC power

■ **Why the PoE Ethernet Switch doesn't connect to the network**

Solution:

Check the LNK/ACT LED on the PoE Ethernet Switch. Try another port on the PoE Ethernet Switch. Make sure the cable is installed properly and make sure the cable is the right type. Turn off the power. After a while, turn on power again.

■ **When I connect my PoE device to PoE Ethernet Switch, it cannot be powered on**

Solution:

1. Please check the cable type of the connection from the PoE Ethernet Switch (port 1 to port 8) to the other end. The cable should be an 8-wire UTP, Category 5 or above, EIA568 cable within 100 meters. A cable with only 4-wire, short loop or over 100 meters will affect the power supply.
2. Please check and assure the device is fully complied with IEEE 802.3af / 802.3at standard.

APPENDIX A Switch's RJ45 Pin Assignments

A.1 1000Mbps, 1000BASE-T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

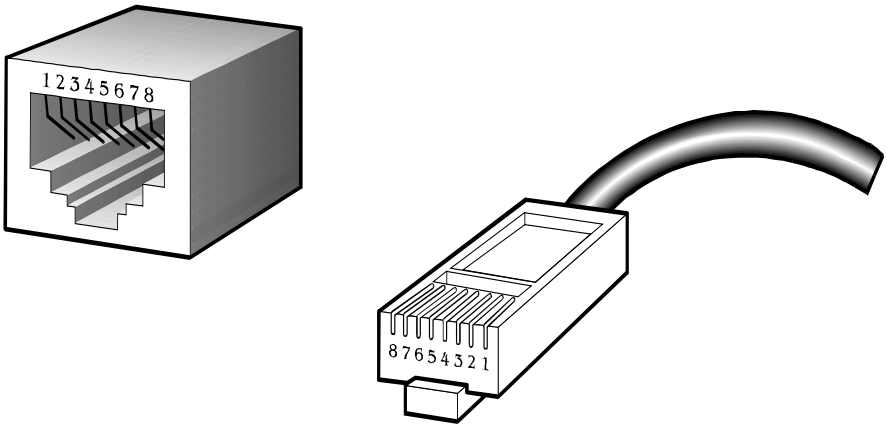
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100BASE-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/ connector and their pin assignments:

RJ45 Connector pin assignment		
Contact	MDI Media Dependent Interface	MDI-X Media Dependent Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ45 pin assignment



The standard RJ45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

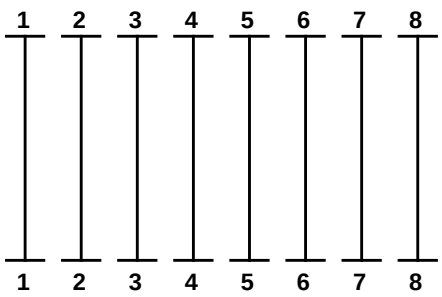
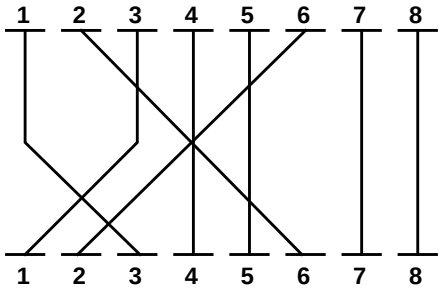
Straight-through Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange	1 = White / Orange
		2 = Orange	2 = Orange
		3 = White / Green	3 = White / Green
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Green
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown
Crossover Cable		**SIDE 1**	**SIDE 2**
	SIDE 1	1 = White / Orange	1 = White / Green
		2 = Orange	2 = Green
		3 = White / Green	3 = White / Orange
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Orange
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown

Figure A-1: Straight-through and Crossover Cable

Please make sure your connected cables are with the same pin assignment and color as the above table before deploying the cables into your network.