1 Overview

Routing table is used for a Layer 3 device (in this configuration guide, it means the switch) to forward packets to the correct destination. When the switch receives packets of which the source IP address and destination IP address are in different subnets, it will check the routing table, find the correct outgoing interface then forward the packets.

The routing table mainly contains two types of routing entries: dynamic routing entries and static routing entries.

Dynamic routing entries are automatically generated by the switch. The switch use dynamic routing protocols to automatically calculate the best route to forward packets.

Static routing entries are manually added none-aging routing entries. In a simple network with a small number of devices, you only need to configure static routes to ensure that the devices from different subnets can communicate with each other. On a complex large-scale network, static routes ensure stable connectivity for important applications because the static routes remain unchanged even when the topology changes.

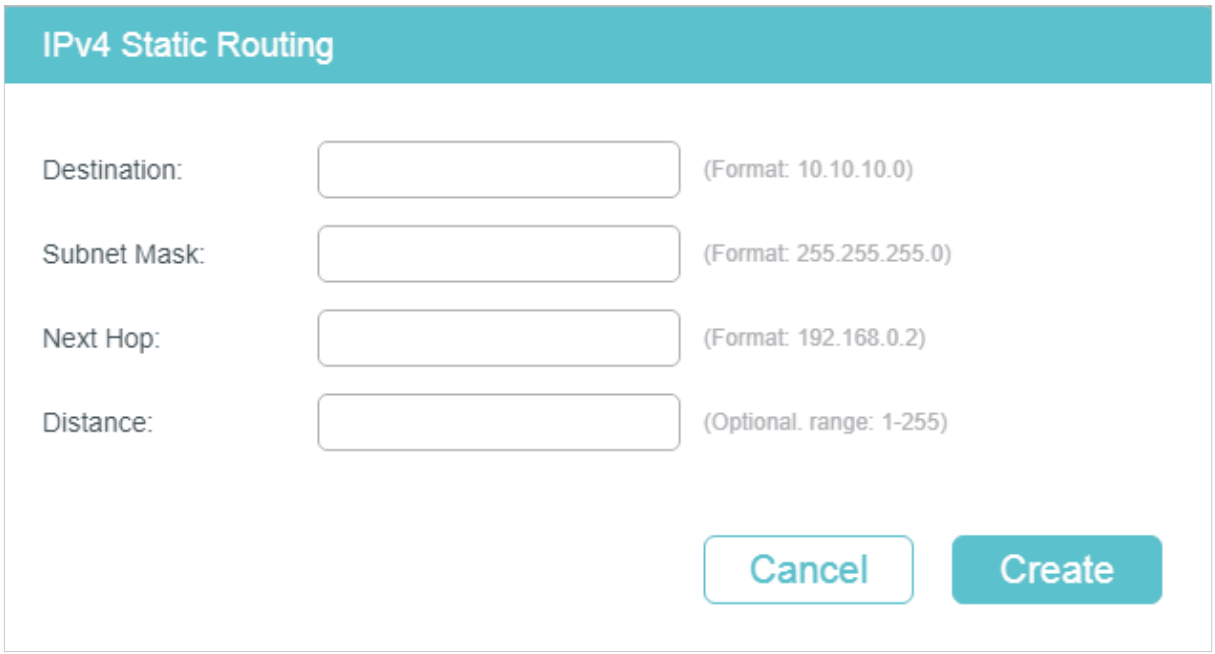
The switch supports IPv4 static routing and IPv6 static routing configuration.

2 IPv4 Static Routing Configuration

2.1 Using the GUI

Choose the menu **L3 FEATURES > Static Routing > IPv4 Static Routing** and click Add to load the following page.

Figure 2-1 Configuring the IPv4 Static Routing



Configure the corresponding parameters to add an IPv4 static routing entry. Then click **Create**.

Destination	Specify the destination IPv4 address of the packets.
Subnet Mask	Specify the subnet mask of the destination IPv4 address.
Next Hop	Specify the IPv4 gateway address to which the packet should be sent next.
Distance	Specify the administrative distance, which is the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv4 routing table. The valid value ranges from 1 to 255 and the default value is 1.

2.2 Using the CLI

Follow these steps to create an IPv4 static route.

Step 1	**configure** Enter global configuration mode.
Step 2	**ip route {** *dest-address* **} {** *mask* **} {** *next-hop-address* **} [** *distance* **]** Add an IPv4 static route. *dest-address:* Specify the destination IPv4 address of the packets. *mask:* Specify the subnet mask of the destination IPv4 address. *next-hop-address:* Specify the IPv4 gateway address to which the packet should be sent next. *distance:* Specify the administrative distance, which is a rating of the trustworthiness of the routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route that has the shortest distance will be recorded in the IP routing table. The valid values are from 1 to 255 and the default value is 1.
Step 3	**show ip route [** static | connected **]** Verify the IPv4 route entries of the specified type.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an IPv4 static route with the destination IP address as 192.168.2.0, the subnet mask as 255.255.255.0 and the next-hop address as 192.168.0.2:

Switch#configure

Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.0.2

Switch(config)#show ip route

Codes: C - connected, S - static

* - candidate default

C 192.168.0.0/24 is directly connected, Vlan1

S 192.168.2.0/24 [1/0] via 192.168.0.2, Vlan1

Switch(config)#end

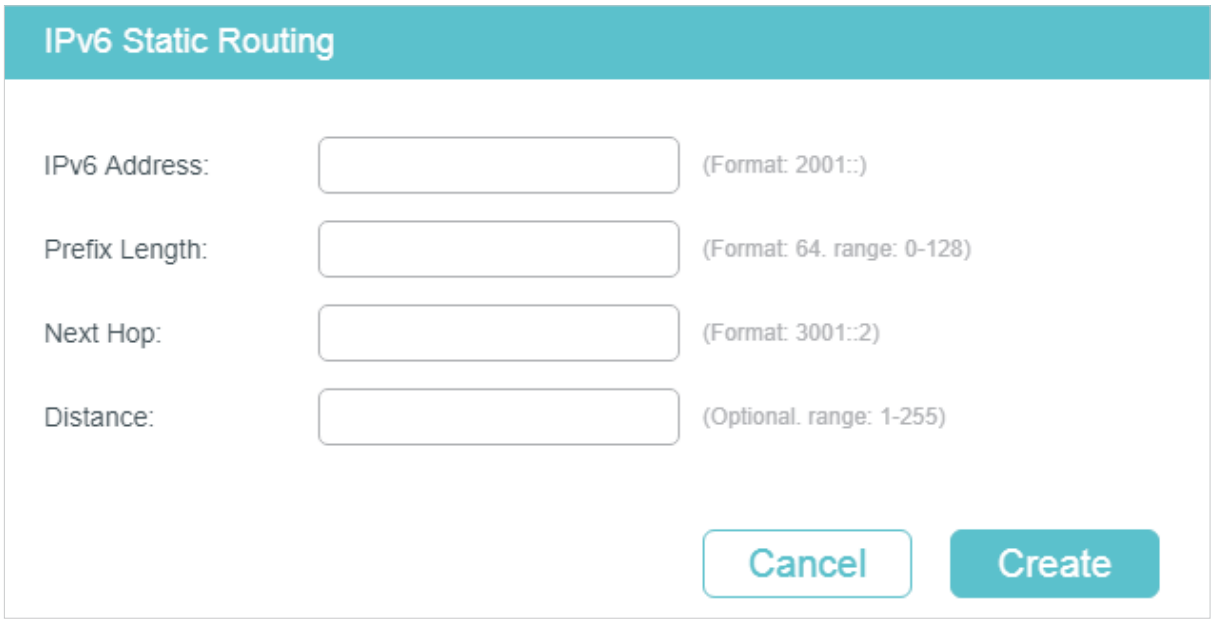
Switch#copy running-config startup-config

3 IPv6 Static Routing Configuration

3.1 Using the GUI

Choose the menu **L3 FEATURES > Static Routing > IPv6 Static Routing > IPv6 Static Routing Table** and click Add to load the following page.

Figure 3-1 Configuring the IPv6 Static Routing



Configure the corresponding parameters to add an IPv6 static routing entry. Then click **Create.**

IPv6 Address	Specify the destination IPv6 address of the packets.
Prefix Length	Specify the prefix length of the IPv6 address.
Next Hop	Specify the IPv6 gateway address to which the packet should be sent next.
Distance	Specify the administrative distance, which is the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv6 routing table. The valid value ranges from 1 to 255 and the default value is 1

3.2 Using the CLI

Follow these steps to enable IPv6 routing function and create an IPv6 static route.

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 routing** Enable the IPv6 routing function on the specified Layer 3 interface.
Step 3	**ipv6 route {** *ipv6-dest-address* **} {** *next-hop-address* **} [** *distance* **]** Add an IPv6 static route. *ipv6-dest-address:* Specify the destination IPv6 address of the packets, in the format of X:X:X:X::X/<0-128>. *next-hop-address:* Specify the IPv6 gateway address to which the packet should be sent next. *distance:* Specify the administrative distance, which is a rating of the trustworthiness of the routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route that has the shortest distance will be recorded in the IP routing table. The valid values are from 1 to 255 and the default value is 1.
Step 4	**show ipv6 route [** static | connected **]** Verify the IPv6 route entries of the specified type.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an IPv6 static route with the destination IP address as 3200::/64 and the next-hop address as 3100::1234:

Switch#configure

Switch(config)#ipv6 route 3200::/64 3100::1234

Switch(config)#show ipv6 route static

Codes: C - connected, S - static

* - candidate default

C 3000::/64 is directly connected, Vlan1

S 3200::/64 [1/0] via 3100::1234, Vlan2

Switch(config)#end

Switch#copy running-config startup-config

4 Viewing Routing Table

You can view the routing tables to learn about the network topology. The switch supports IPv4 routing table and IPv6 routing table.

4.1 Using the GUI

4.1.1 Viewing IPv4 Routing Table

Choose the menu **L3 FEATURES > Routing Table > IPv4 Routing Table > IPv4 Routing Information Summary** to load the following page.

Figure 4-1 Viewing IPv4 Routing Table

Protocol	Destination Network	Next Hop	Distance	Metric	Interface Name
Connected	192.168.0.0/24	192.168.0.26	0	1	
Static	192.168.30.0/24	192.168.0.36	5	0	
Total: 2					

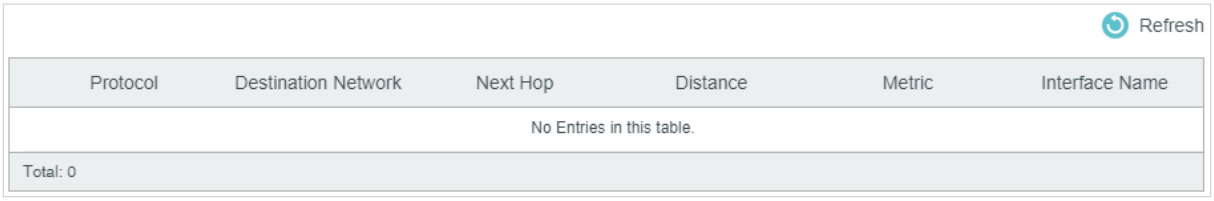
View the IPv4 routing entries.

Protocol	Displays the type of the routing entry. **Connected**: The destination network is directed connected to the switch. **Static**: The routing entry is a manually added static routing entry.
Destination Network	Displays the destination IP address and subnet mask.
Next Hop	Displays the IPv4 gateway address to which the packet should be sent next.
Distance	Displays the administrative distance, which is the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv6 routing table.
Metric	Displays the metric to reach the destination IP address.
Interface Name	Displays the name of the gateway interface.

4.1.2 Viewing IPv6 Routing Table

Choose the menu **L3 FEATURES> Routing Table > IPv6 Routing Table > IPv6 Routing Information Summary** to load the following page.

Figure 4-2 Viewing IPv6 Routing Table



View the IPv6 routing entries.

Protocol	Displays the type of the routing entry. **Connected**: The destination network is directed connected to the switch. **Static**: The routing entry is a manually added static routing entry.
Destination Network	Displays the destination IPv6 address and subnet mask.
Next Hop	Displays the IPv6 gateway address to which the packet should be sent next.
Distance	Displays the administrative distance, which is the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv6 routing table.
Metric	Displays the metric to reach the destination IPv6 address.
Interface Name	Displays the name of the gateway interface.

4.2 Using the CLI

4.2.1 Viewing IPv4 Routing Table

On privileged EXEC mode or any other configuration mode, you can use the following command to view IPv4 routing table:

show ip route [static | connected **]**

View the IPv4 route entries of the specified type. If not specified, all types of route entries will be displayed.

static: View the static routes.

connected: View the connected routes.

4.2.2 Viewing IPv6 Routing Table

On privileged EXEC mode or any other configuration mode, you can use the following command to view IPv6 routing table:

show ipv6 route [static | connected **]**

View the IPv6 route entries of the specified type. If not specified, all types of route entries will be displayed.

static: View the static IPv6 routes.

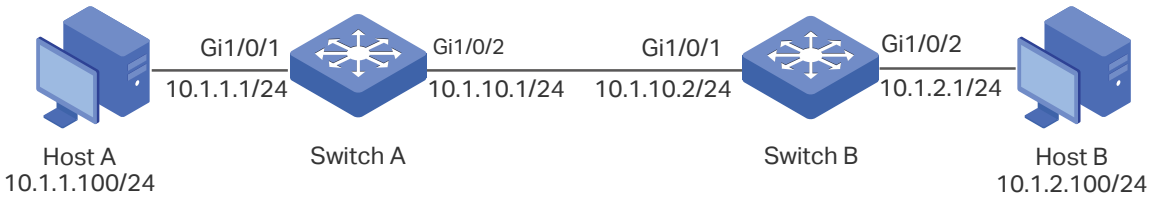
connected: View the connected IPv6 routes.

5 Example for Static Routing

5.1 Network Requirements

As shown below, Host A and Host B are on different network segments. To meet business needs, Host A and Host B need to establish a connection without using dynamic routing protocols to ensure stable connectivity.

Figure 5-1 Network Topology



5.2 Configuration Scheme

To implement this requirement, you can configure the default gateway of host A as 10.1.1.1/24, the default gateway of host B as 10.1.2.1/24, and configure IPv4 static routes on Switch A and Switch B so that hosts on different network segments can communicate with each other.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.3 Using the GUI

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example.

1) Choose the menu **L3 FEATURES > Interface** to create a routed port Gi1/0/1 with the mode as static, the IP address as 10.1.1.1, the mask as 255.255.255.0 and the admin status as Enable. Create a routed port Gi1/0/2 with the mode as static, the IP address as 10.1.10.1, the mask as 255.255.255.0 and the admin status as Enable.

Figure 5-2 Create a Routed Port Gi1/0/1 for Switch A

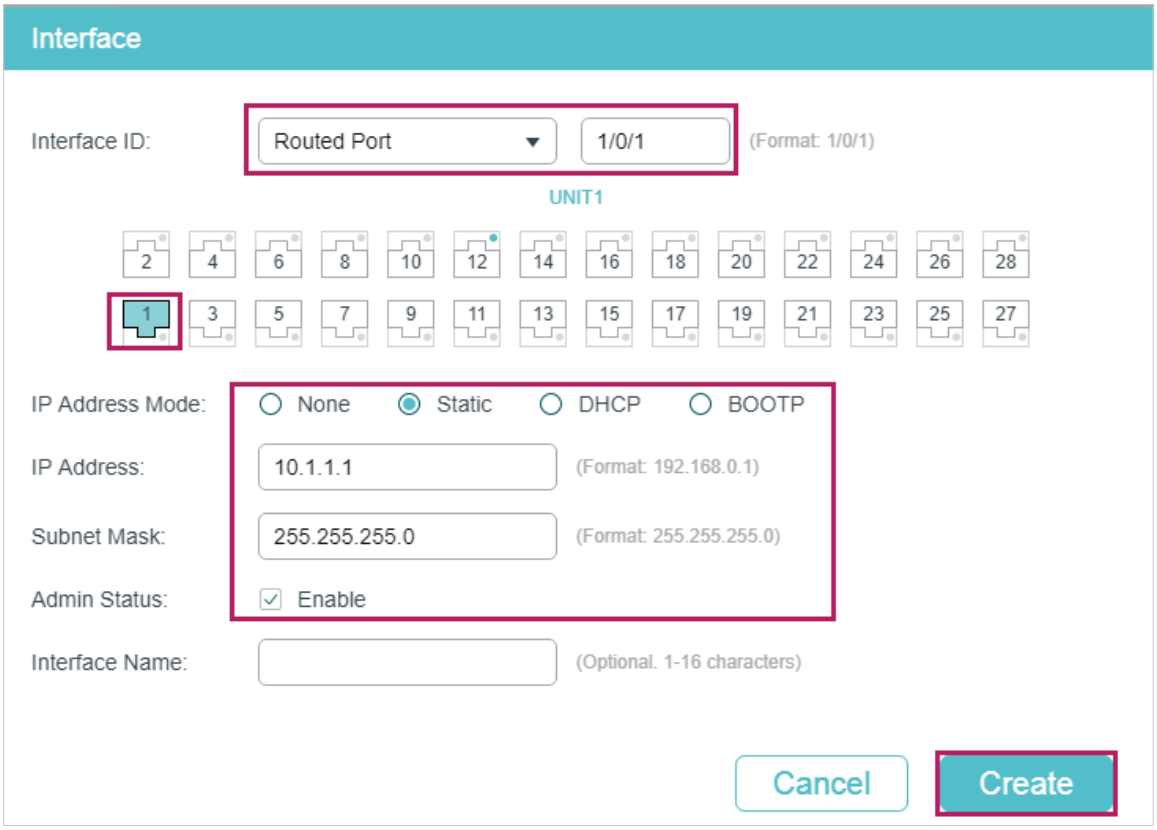
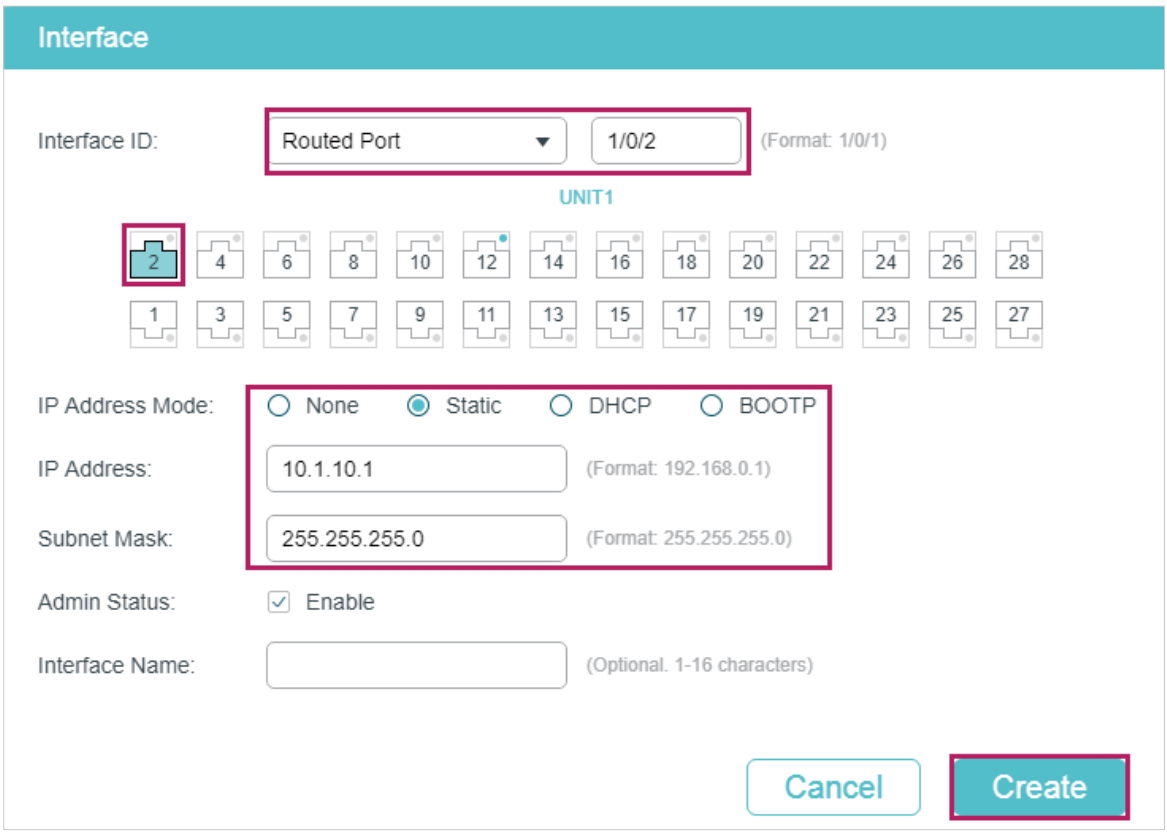


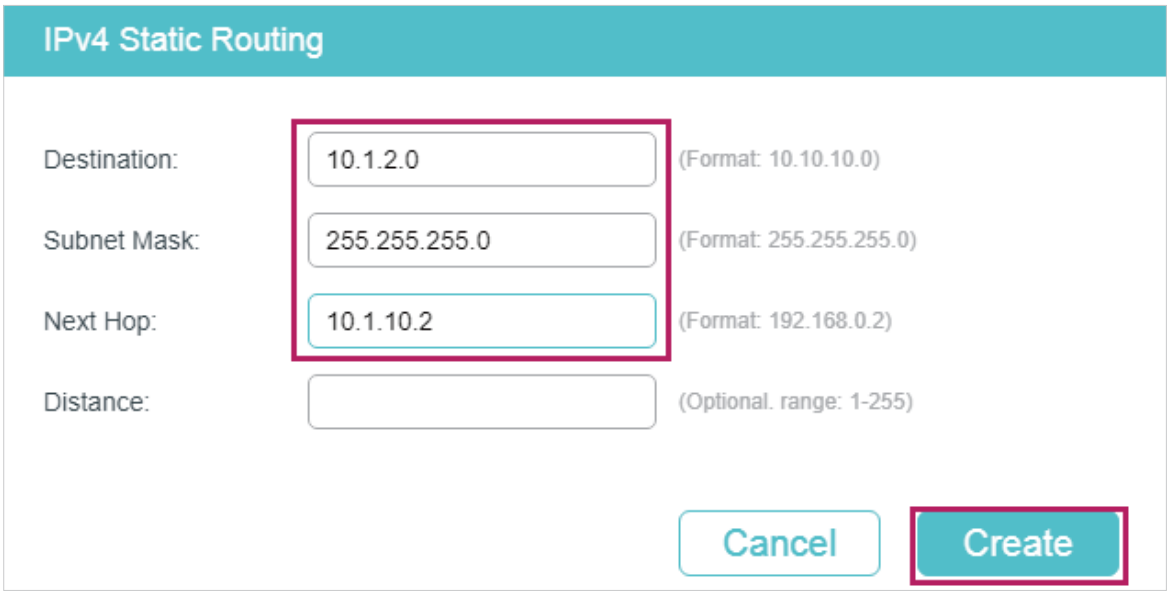
Figure 5-3 Create a Routed Port Gi1/0/2 for Switch A



2) Choose the menu **L3 FEATURES > Static Routing > IPv4 Static Routing** to load the following page. Add a static routing entry with the destination as 10.1.2.0, the subnet

mask as 255.255.255.0 and the next hop as 10.1.10.2. For switch B, add a static route entry with the destination as 10.1.1.0, the subnet mask as 255.255.255.0 and the next hop as 10.1.10.1.

Figure 5-4 Add a Static Route for Switch A



5.4 Using the CLI

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example.

1) Create a routed port Gi1/0/1 with the mode as static, the IP address as 10.1.1.1, the mask as 255.255.255.0 and the admin status as Enable. Create a routed port Gi1/0/2 with the mode as static, the IP address as 10.1.10.1, the mask as 255.255.255.0 and the admin status as Enable.

   Switch_A#configure

   Switch_A(config)#interface gigabitEthernet 1/0/1

   Switch_A(config-if)#no switchport

   Switch_A(config-if)#ip address 10.1.1.1 255.255.255.0

   Switch_A(config-if)#exit

   Switch_A(config)#interface gigabitEthernet 1/0/2

   Switch_A(config-if)#no switchport

   Switch_A(config-if)#ip address 10.1.10.1 255.255.255.0

2) Add a static route entry with the destination as 10.1.2.0, the subnet mask as 255.255.255.0 and the next hop as 10.1.10.2. For switch B, add a static route entry with the destination as 10.1.1.0, the subnet mask as 255.255.255.0 and the next hop as 10.1.10.1.

Switch_A#configure

Switch_A(config)#ip route 10.1.2.0 255.255.255.0 10.1.10.2

Switch_A(config)#end

Switch_A#copy running-config startup-config

Verify the Configurations

- Switch A

  Verify the static routing configuration:

  Switch_A#show ip route

  Codes: C - connected, S - static

  * - candidate default

  C 10.1.1.0/24 is directly connected, Vlan10

  C 10.1.10.0/24 is directly connected, Vlan20

  S 10.1.2.0/24 [1/0] via 10.1.10.2, Vlan20

- Switch B

  Verify the static routing configuration:

  Switch_B#show ip route

  Codes: C - connected, S - static

  * - candidate default

  C 10.1.2.0/24 is directly connected, Vlan30

  C 10.1.10.0/24 is directly connected, Vlan20

  S 10.1.1.0/24 [1/0] via 10.1.10.1, Vlan20

- Connectivity Between Switch A and Switch B

  Run the ping command on switch A to verify the connectivity:

  Switch_A#ping 10.1.2.1

  Pinging 10.1.2.1 with 64 bytes of data :

  Reply from 10.1.2.1 : bytes=64 time<16ms TTL=64

  Reply from 10.1.2.1 : bytes=64 time<16ms TTL=64

  Reply from 10.1.2.1 : bytes=64 time<16ms TTL=64

  Reply from 10.1.2.1 : bytes=64 time<16ms TTL=64

Ping statistics for 10.1.2.1:

Packets: Sent = 4 , Received = 4 , Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 1ms , Maximum = 3ms , Average = 1ms

Part 20

Configuring DHCP Service

CHAPTERS

1. DHCP
2. DHCP Server Configuration
3. DHCP Relay Configuration
4. DHCP L2 Relay Configuration
5. Configuration Examples
6. Appendix: Default Parameters

1 DHCP

1.1 Overview

DHCP (Dynamic Host Configuration Protocol) is widely used to automatically assign IP addresses and other network configuration parameters to network devices, enhancing the utilization of IP address.

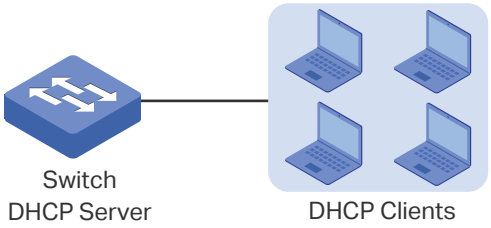
1.2 Supported Features

The supported DHCP features of the switch include DHCP Server, DHCP Relay and DHCP L2 Relay.

DHCP Server

DHCP Server is used to dynamically assign IP addresses, default gateway and other parameters to DHCP clients. As the following figure shows, the switch acts as a DHCP server and assigns IP addresses to the clients.

Figure 1-1 Application Scenario of DHCP Server



DHCP Relay

DHCP Relay is used to process and forward DHCP packets between different subnets or VLANs.

DHCP clients broadcast DHCP request packets to require for IP addresses. Without this function, clients cannot obtain IP addresses from a DHCP server in the different LAN because the broadcast packets can be transmitted only in the same LAN. To equip each LAN with a DHCP server can solve this problem, but the costs of network construction will be increased and the management of central network will become inconvenient.

A device with DHCP Relay function is a better choice. It acts as a relay agent and can forward DHCP packets between DHCP clients and DHCP servers in different LANs. Therefore, DHCP clients in different LANs can share one DHCP server.

DHCP Relay includes three features: Option 82, DHCP Interface Relay and DHCP VLAN Relay.

Option 82

Option 82 is called the DHCP Relay Agent Information Option. It provides additional security and a more flexible way to allocate network addresses compared with the traditional DHCP.

When enabled, the DHCP relay agent can inform the DHCP server of some specified information of clients by inserting an Option 82 payload to DHCP request packets before forwarding them to the DHCP server, so that the DHCP server can distribute the IP addresses or other parameters to clients based on the payload. In this way, Option 82 prevents DHCP client requests from untrusted sources. Besides, it allows the DHCP server to assign IP addresses of different address pools to clients in different groups.

An Option 82 has two sub-options, namely, the Agent Circuit ID and Agent Remote ID. The information that the two sub-options carry depends on the settings of the DHCP relay agent, and are different among devices from different vendors. To allocate network addresses using Option 82, you need to define the two sub-options on the DHCP relay agent, and create a DHCP class on the DHCP server to identify the Option 82 payload.

TP-Link switches preset a default circuit ID and remote ID in TLV (Type, Length, and Value) format. You can also configure the format to include Value only and customize the Value.

Table 1-1 and Table 1-2 show the packet formats of the Agent Circuit ID and Agent Remote ID, respectively.

Table 1-1 Packet Formats of the Agent Circuit ID with Different Option 82 Settings

Option 82 Settings		*Type (Hex)	*Length (Hex)	*Value
*Format	Circuit ID Customization			
Normal (TLV)	Disabled	00	04	Default circuit ID
	Enabled	01	Length of the customized circuit ID	Customized circuit ID
Private (Only the value)	Disabled	-	-	Default circuit ID
	Enabled	-	-	Customized circuit ID

Table 1-2 Packet Formats of the Agent Remote ID with Different Option 82 Settings

Option 82 Settings		*Type (Hex)	*Length (Hex)	*Value
*Format	Remote ID Customization			
Normal (TLV)	Disabled	00	06	Default remote ID
	Enabled	01	Length of the customized remote ID	Customized remote ID
Private (Only the value)	Disabled	-	-	Default remote ID
	Enabled	-	-	Customized remote ID

***Format**

Indicates the packet format of the sub-option field. Two options are available:

- Normal: Indicates the field consists of three parts: Type, Length, and Value (TLV).
- Private: Indicates the field consists of the value only.

***Type**

A one-byte field indicating whether the Value field is customized or not. **00** in hexadecimal means the Value field is not customized (uses the default circuit/remote ID) while **01** in hexadecimal means it is customized.

***Length**

A one-byte field indicating the length of the Value field. The length of the default circuit ID is 4 bytes and that of default remote ID is 6 bytes. For the customized circuit ID and remote ID, the length is variable, ranging from 1 to 64 bytes.

***Value**

Indicates the value of the sub-option. The switch has preset a default circuit ID and remoter ID. You can also customize them with Circuit ID Customization and Remote ID Customization enabled.

- Default circuit ID: A 4-byte value which consists of 2-byte VLAN ID and 2-byte Port ID. The VLAN ID indicates which VLAN the DHCP client belongs to, and the Port ID indicates which port the DHCP client is connected to.

  For example, if the DHCP client is connected to port 1/0/1 in VLAN 2, this field is **00:02:00:01** in hexadecimal.
- Default remote ID: A 6-byte value which indicates the MAC address of the DHCP relay agent.
- Customized circuit/remote ID: You can configure a string using up to 64 characters. The switch encodes the string using ASCII. When configuring your DHCP server to identify the string, use the correct notation that is used by your DHCP server to represent ASCII strings, or convert it into hexadecimal format if necessary.

Tips:

As shown in Table 1-1 and Table 1-2, by default, the circuit ID records the ports of the DHCP relay agent that are connected to the clients and the VLANs that the clients belong to, and the remote ID records the MAC address of the DHCP relay agent. That is, the two sub-options together record the location of the clients. To record the accruate location of clients, configure Option 82 on the switch which is closest to the clients.

DHCP Interface Relay

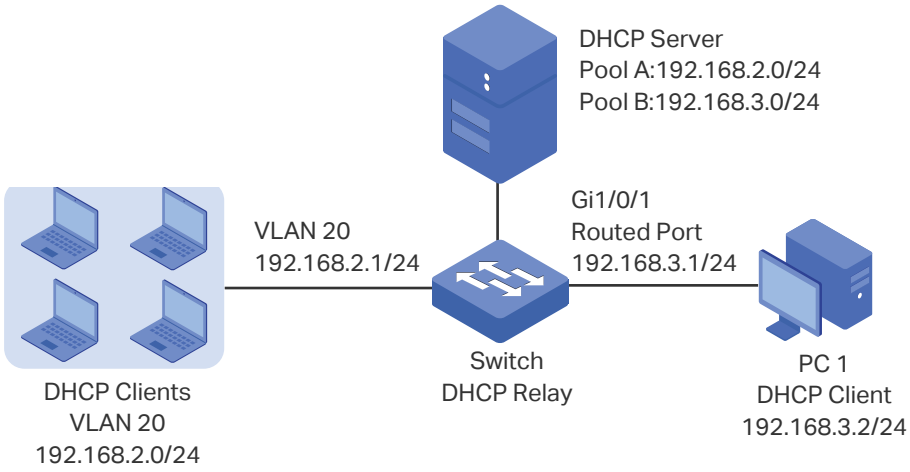
DHCP Interface Relay allows clients to obtain IP addresses from a DHCP server in a different LAN. In DHCP Interface Relay, you can specify a DHCP server for the Layer 3 interface that the clients are connected to. When receiving DHCP packets from clients, the switch fills the corresponding interface's IP address in the Relay Agent IP Address field of the DHCP packets, and forwards the packets to the DHCP server. Then the DHCP server

can assign IP addresses that are in the same subnet with the Relay Agent IP Address to the clients.

The switch supports specifying a DHCP server for multiple Layer 3 interfaces, which makes it possible to assign IP addresses to clients in different subnets from the same DHCP server.

As the following figure shows, the IP address of VLAN 20 is 192.168.2.1/24 and that of the routed port Gi1/0/1 is 192.168.3.1/24. With DHCP Interface VLAN configured, the switch fills in the Relay Agent IP Address field of the DHCP packets with the IP address of VLAN 20 (192.168.2.1/24) when applying for IP addresses for clients in VLAN 20, and fills with the IP address of Gi1/0/1 (192.168.3.1/24) when applying for an IP address for PC 1. As a result, the DHCP server will assign IP addresses in Pool A (the same subnet with the IP address of VLAN 20) to clients in VLAN 20, and assign an IP address in Pool B (the same subnet with the Gi1/0/1) to PC 1.

Figure 1-2 Application Scenario of DHCP Interface Relay



DHCP VLAN Relay

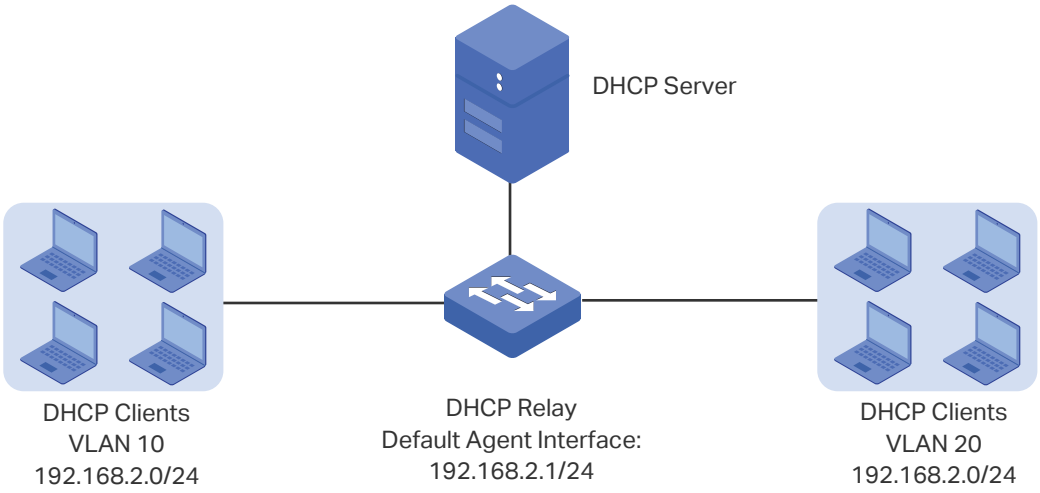
DHCP VLAN Relay allows clients in different VLANs to obtain IP addresses from the DHCP server using the IP address of a single agent interface.

In DHCP Interface Relay, to achieve this goal, you need to create a Layer 3 interface for each VLAN to ensure the reachability.

In DHCP VLAN Relay, you can simply specify a Layer 3 interface as the default agent interface for all VLANs. The switch fills this default agent interface's IP address in the Relay Agent IP Address field of the DHCP packets from all VLANs.

As the following figure shows, no IP addresses are assigned to VLAN 10 and VLAN 20, but a default relay agent interface is configured with the IP address 192.168.2.1/24. The switch fills in the Relay Agent IP Address field of the DHCP packets with the IP address of the default agent interface (192.168.2.1/24) when applying for IP addresses for clients in both VLAN 10 and VLAN 20. As a result, the DHCP server will assign IP addresses on 192.168.2.0/24 (the same subnet with the IP address of the default agent interface) to clients in both VLAN 10 and VLAN 20.

Figure 1-3 Application Scenario of DHCP VLAN Relay



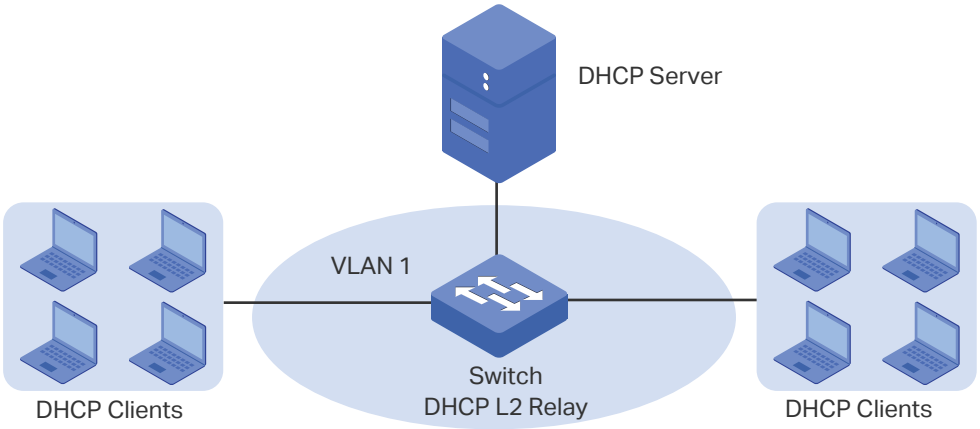
Note:

- If the VLAN already has an IP address, the switch will use the IP address of the VLAN as the relay agent IP address. The default relay agent IP address will not take effect.
- DHCP VLAN Relay will not work on routed ports or port channel interfaces, because they are not associated with any particular VLAN.

DHCP L2 Relay

Unlike DHCP relay, DHCP L2 Relay is used in the situation that the DHCP server and clients are in the same VLAN. In DHCP L2 Relay, in addition to normally assigning IP addresses to clients from the DHCP server, the switch can inform the DHCP server of some specified information, such as the location information, of clients by inserting an Option 82 payload to DHCP request packets before forwarding them to the DHCP server. This allows the DHCP server which supports Option 82 can set the distribution policy of IP addresses and other parameters, providing a more flexible way to distribute IP addresses.

Figure 1-4 Application Scenario of DHCP L2 Relay



2 DHCP Server Configuration

To complete DHCP server configuration, follow these steps:

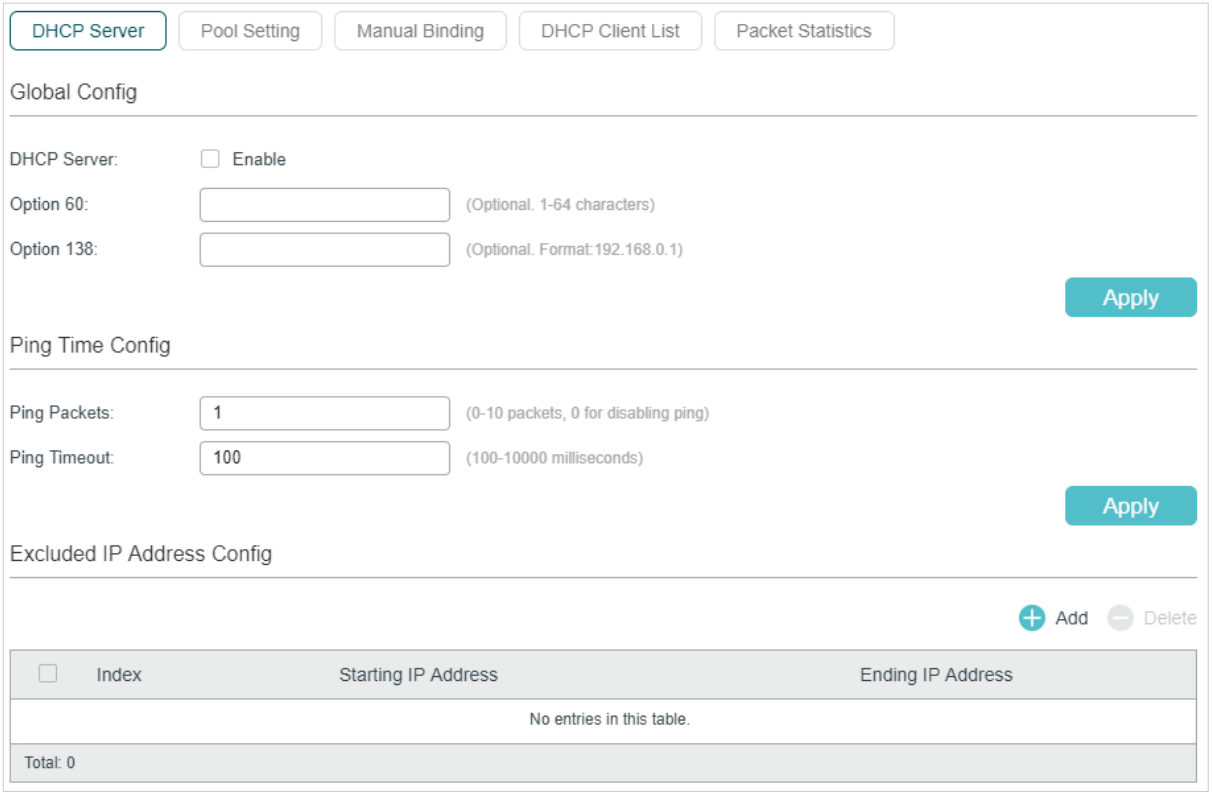
1) Enable the DHCP Server feature on the switch.
2) Configure DHCP Server Pool.
3) (Optional) Manually assign static IP addresses for some clients.

2.1 Using the GUI

2.1.1 Enabling DHCP Server

Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > DHCP Server** to load the following page.

Figure 2-1 Configure DHCP Server



Follow these steps to configure DHCP Server:

1) In the **Global Config** section, enable DHCP Server. Click **Apply**.

DHCP Server	Enable DHCP Server.

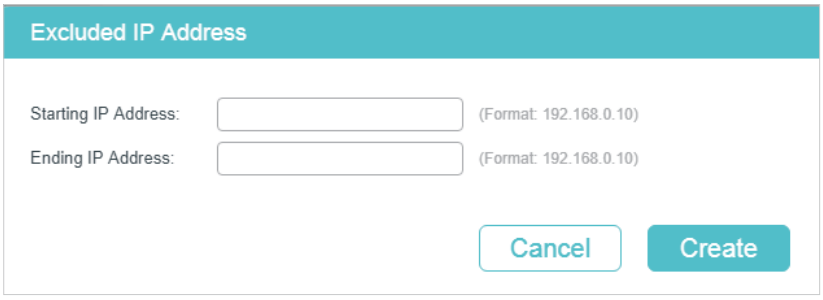
Option 60	(Optional) Specify the Option 60 for device identification. Mostly it is used for the scenarios that the APs (Access Points) apply for different IP addresses from different servers according to the needs. If an AP requests Option 60, the server will respond a packet containing the Option 60 configured here. And then the AP will compare the received Option 60 with its own. If they are the same, the AP will accept the IP address assigned by the server. Otherwise, the assigned IP address will not be accepted.
Option 138	(Optional) Specify the Option 138, which should be configured as the management IP address of an AC (Access Control) device. If the APs in the local network request this option, the server will respond a packet containing this option to inform the APs of the AC's IP address.

2) In the **Ping Time Config** section, configure Ping Packets and Ping Timeout for ping tests. Click **Apply**.

Ping Packets	Enter the number of ping packets the server can broadcast to test whether the IP address is occupied. The valid values are from 1 to 10, and the default is 1. When the switch is configured as a DHCP server to dynamically assign IP addresses to clients, the switch will deploy ping tests to avoid IP address conflicts resulted from assigning IP addresses repeatedly.
Ping Timeout	Specify the timeout period for ping tests in milliseconds. It ranges from 100 to 10000 ms, and the default is 100 ms. The DHCP server broadcasts an ICMP Echo Request (ping packet) to test whether an IP address is occupied or not. If there is no response within the timeout period, the server will broadcast the ping packet again. If the number of ping packets reaches the specified number without response, the server will assign the IP address. Otherwise, the server will record the IP address as a conflicted one and assign another IP address to the client.

3) In the **Excluded IP Address Config** section, click Add to load the following page to specify the IP addresses that should not be assigned to the clients.

Figure 2-2 Configure Excluded IP Address



Enter the Starting IP Address and Ending IP Address to specify the range of reserved IP addresses. Click **Create**.

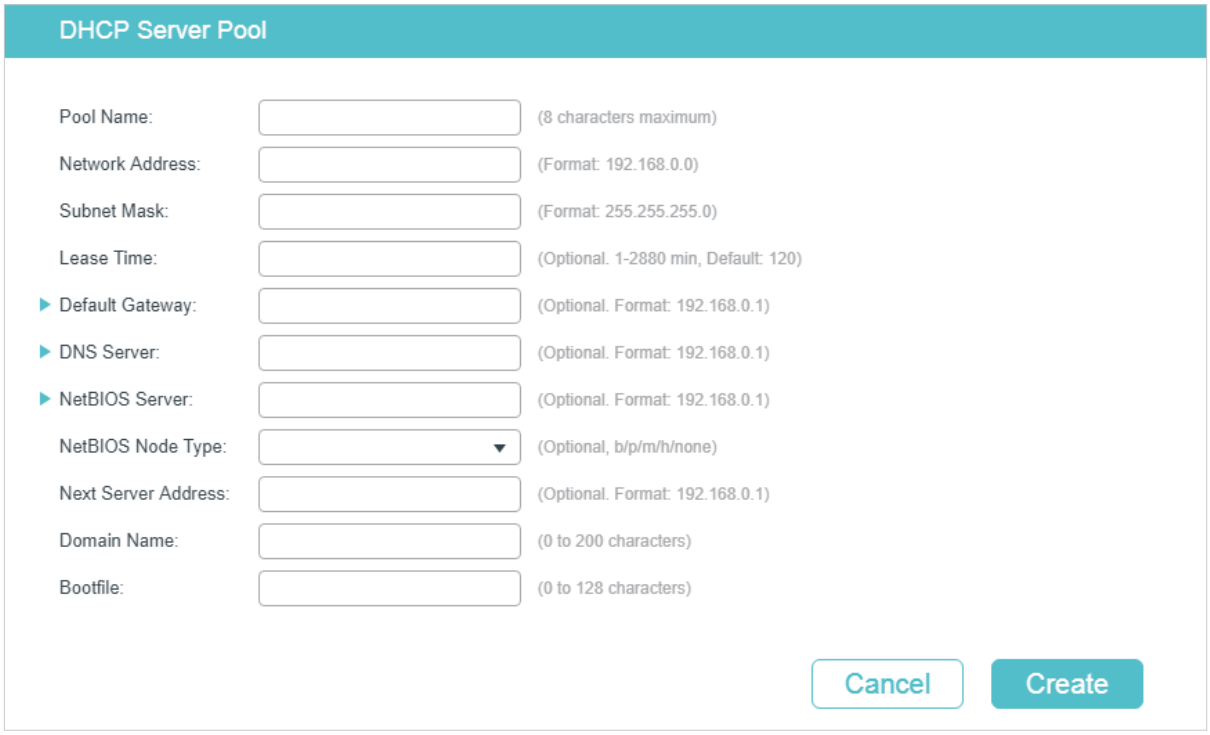
Starting IP Address/ Ending IP Address	Specify the starting IP address and ending IP address of the excluded IP address range. If the starting IP address and ending IP address are the same, the server excludes only one IP address. When configuring DHCP Server, you need to reserve certain IP addresses for each subnet, such as the default gateway address, broadcast address and DNS server address.

2.1.2 Configuring DHCP Server Pool

DHCP Server Pool defines the parameters that will be assigned to DHCP clients.

Choose the menu **L3 FEATURES > DHCP Service >DHCP Server > Pool Setting** and click Add to load the following page.

Figure 2-3 Pool Setting



Configure the parameters for DHCP Server Pool. Then click **Create**.

Pool Name	Specify a pool name for identification.
Network Address / Subnet Mask	Configure the network address and subnet mask of the DHCP server pool. The network address and subnet mask decide the range of the DHCP server pool. On the same subnet, all addresses can be assigned except the excluded addresses and addresses for special uses.
Lease Time	Specify how long the client can use the IP address assigned from this address pool. It ranges from 1 to 2880 minutes, and the default is 120 minutes.

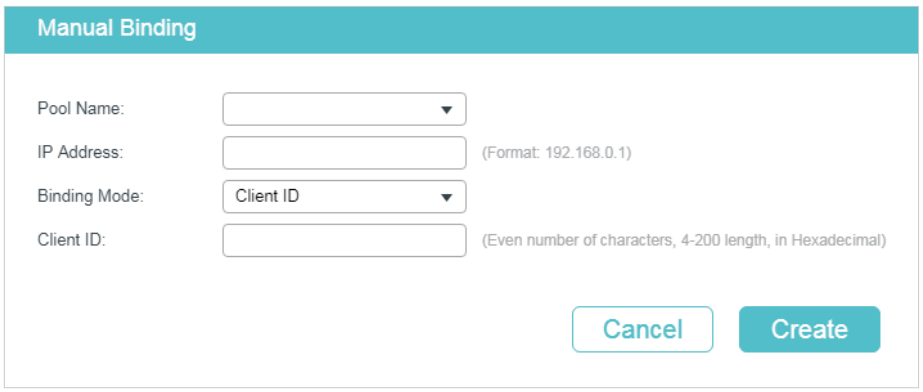
Default Gateway	(Optional) Configure the default gateway of the DHCP server pool. You can create up to 8 default gateways for each DHCP server pool. If you leave this field blank, the DHCP server will not assign this parameter to clients. In general, you can configure the IP address of the VLAN interface as the default gateway address.
DNS Server	(Optional) Specify the DNS server of the DHCP server pool. You can specify up to 8 DNS servers for each DHCP server pool. If you leave this field blank, the DHCP server will not assign this parameter to clients. In general, you can configure the IP address of the VLAN interface as the DNS server address.
NetBIOS Server	(Optional) Specify the NetBIOS name server. You can specify up to 8 NetBIOS servers for each DHCP server pool. If you leave this field blank, the DHCP server will not assign this parameter to clients. When a DHCP client uses the Network NetBIOS (Basic Input Output System) protocol for communication, the host name must be mapped to IP address. NetBIOS name server can resolve host names to IP addresses.
NetBIOS Node Type	(Optional) Specify the NetBIOS type for clients, which is the way of inquiring IP address resolution. If you leave this field blank, the DHCP server will not assign this parameter to clients. The following options are provided: **b-node Broadcast**: The client sends query messages via broadcast. **p-node Peer-to-Peer**: The client sends query messages via unicast. **m-node Mixed**: The client sends query messages via broadcast first. If it fails, the client will try again via unicast. **h-node Hybrid**: The client sends query messages via unicast first. If it fails, the client will try again via broadcast.
Next Server Address	(Optional) Specify the IP address of a TFTP server for clients. If needed, clients can get the configuration file from the TFTP server for auto installation. If you leave this field blank, the DHCP server will not assign this parameter to clients.
Domain Name	(Optional) Specify the domain name that clients should use when resolving host names via DNS. If you leave this field blank, the DHCP server will not assign this parameter to clients.
Bootfile	(Optional) Specify the name of the bootfile. If needed, clients can get the bootfile from the TFTP server for auto installation. If you leave this field blank, the DHCP server will not assign this parameter to clients.

2.1.3 Configuring Manual Binding

Some devices like web servers require static IP addresses. To meet this requirement, you can manually bind the MAC address or client ID of the device to an IP address, and the DHCP server will reserve the bound IP address to this device at all times.

Choose the menu **L3 FEATURES > DHCP Service >DHCP Server > Manual Binding** and click Add to load the following page.

Figure 2-4 Manual Binding



Select a pool name and enter the IP address to be bound. Select a binding mode and finish the configuration accordingly. Click **Create**.

Pool Name	Select a DHCP server pool from the drop-down list.
IP Address	Enter the IP address to be bound to the client.
Binding Mode	Select the binding mode: **Client ID**: Bind the IP address to the client ID of the client. **Client ID in ASCII**: Bind the IP address to the client ID in ASCII format. **Hardware Address**: Bind the IP address to the MAC address of the client.
Client ID	If you select Client ID as the binding mode, enter the client ID in this field.
Hardware Address	If you select Hardware Address as the binding mode, enter the MAC address in this field.
Hardware Type	If you select Hardware Address as the binding mode, select a hardware type. The hardware type includes Ethernet and IEEE802.

2.2 Using the CLI

2.2.1 Enabling DHCP Server

Follow these steps to enable DHCP Server and to configure ping packets and ping timeout.

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**service dhcp server** Enable DHCP Server.

Step 3	**ip dhcp server extend-option vendor-class-id** *vendor* (Optional) Specify the Option 60 for server identification. If a client requests Option 60, the server will respond a packet containing the Option 60 configured here. And then the client will compare the received Option 60 with its own. If they are the same, the client will accept the IP address assigned by the server. Otherwise, the assigned IP address will not be accepted. *vendor*: Specify the Option 60 with 1 to 64 characters.
Step 4	**ip dhcp server extend-option capwap-ac-ip** *ip-address* (Optional) Specify the Option 138, which should be configured as the management IP address of an AC (Access Control) device. If the APs (Access Points) in the local network request this option, the server will respond a packet containing this option to inform the APs of the AC's IP address. *ip-address*: Specify the IP address of the AC device that controls the APs.
Step 5	**ip dhcp server ping timeout** *value* Specify the timeout period for ping tests. The DHCP server broadcasts an ICMP Echo Request (ping packet) to test whether an IP address is occupied or not. If there is no response within the timeout period, the server will broadcast the ping packet again. If the number of ping packets reaches the specified number without response, the server will assign the IP address. Otherwise, the server will record the IP address as a conflicted IP address and assign another IP address to the client. *value*: Specify the timeout period for ping tests in milliseconds. It ranges from 100 to 10000 ms, and the default is 100 ms.
Step 6	**ip dhcp server ping packets** *num* Specify the number of ping packets the server can broadcast to test whether the IP address is occupied. When the switch is configured as a DHCP server to dynamically assign IP addresses to clients, the switch will deploy ping tests to avoid IP address conflicts resulted from assigning IP addresses repeatedly. *num*: Enter the number of ping packets. The valid values are from 1 to 10, and the default is 1.
Step 7	**ip dhcp server exclude-address** *start-ip-address end-ip-address* Specify the starting IP address and ending IP address of the excluded IP address range. If the starting IP address and the ending IP address are the same, the server excludes only one IP address. When configuring DHCP Server, you need to reserve certain IP addresses for each subnet, such as default gateway address, broadcast address and DNS server address. *start-ip-address/end-ip-address*: Specify the starting IP address and ending IP address.
Step 8	**show ip dhcp server status** Verify the DHCP status, including whether it is enabled and the configuration of ping packet number and ping packet timeout.
Step 9	**show ip dhcp server extend-option** Verify the configuration of the extended options.

Step 10	**show ip dhcp server excluded-address** Verify the configuration of the excluded IP address.
Step 11	**end** Return to Privileged EXEC Mode.
Step 12	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Server globally on the switch, configure the number of ping packets as **2** and configure the timeout period for ping tests as **200** ms:

Switch#configure

Switch(config)#service dhcp server

Switch(config)#ip dhcp server ping packets 2

Switch(config)#ip dhcp server ping timeout 200

Switch(config)#show ip dhcp server status

DHCP server is enable.

Ping packet number: 2.

Ping packet timeout: 200 milliseconds.

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to configure the Option 60 as **abc** and Option 138 as **192.168.0.155**:

Switch#configure

Switch(config)#ip dhcp server extend-option vendor-class-id abc

Switch(config)#ip dhcp server extend-option capwap-ac-ip 192.168.0.155

Switch(config)#show ip dhcp server extend-option

Option 60: abc

Option 138: 192.168.0.155

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to configure the 192.168.1.1 as the default gateway address and excluded IP address:

Switch#configure

Switch(config)#ip dhcp server excluded-address 192.168.1.1 192.168.1.1

Switch(config)#show ip dhcp server excluded-address

No. Start IP Address End IP Address

--- ------------ --------------

1 192.168.1.1 192.168.1.1

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring DHCP Server Pool

Follow these steps to configure DHCP server pool:

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**ip dhcp server pool** *pool-name* Configure a name for the DHCP server pool for identification. *pool-name*: Specify a pool name with 1 to 8 characters.
Step 3	**network** *network-address subnet-mask* Configure the network address and subnet mask of the DHCP server pool. The network address and subnet mask decide the range of the DHCP server pool. On the same subnet, all addresses can be assigned except the excluded addresses and addresses for special uses. *network-address*: Configure the network address of the DHCP server pool. *subnet-mask*: Configure the subnet mask of the DHCP server pool.
Step 4	**lease** *lease-time* Specify how long the client can use the IP address assigned from this address pool. *lease-time*: Enter the value of lease-time. It ranges from 1 to 2880 minutes, and the default is 120 minutes.
Step 5	**default-gateway** *gateway-list* (Optional) Configure the default gateway of the DHCP server pool. In general, you can configure the IP address of the VLAN interface as the default gateway address. *gateway-list*: Specify the IP address of the default gateway. You can create up to 8 default gateways for each DHCP server pool.

Step 6	**dns-server** *dns-server-list* (Optional) Specify the DNS server of the DHCP server pool. In general, you can configure the IP address of the VLAN interface as the DNS server address. *dns-server-list*: Specify the IP address of the DNS server. You can specify up to 8 DNS servers for each DHCP server pool.
Step 7	**netbios-name-server** *NBNS-list* (Optional) Specify the NetBIOS name server. You can specify up to 8 NetBIOS servers for each DHCP server pool. When a DHCP client uses the Network NetBIOS (Basic Input Output System) protocol for communication, the host name must be mapped to IP address. NetBIOS name server can resolve host names to IP addresses. *NBNS-list*: Specify the IP address of the NetBIOS server. You can specify up to 8 NetBIOS servers for each DHCP server pool.
Step 8	**netbios-node-type** *type* (Optional) Specify the NetBIOS type for the clients, which is the way of inquiring IP address resolution. *type*: Specify the NetBIOS type. The following options are provided: **b-node**: The client sends query messages via broadcast. **p-node**: The client sends query messages via unicast. **m-node**: The client sends query messages via broadcast first. If it fails, the client will try again via unicast. **h-node**: The client sends query messages via unicast first. If it fails, the client will try again via broadcast.
Step 9	**next-server** *ip-address* (Optional) Specify the IP address of a TFTP server for the clients. If needed, the clients can get the configuration file from the TFTP server for auto installation. *ip-address*: Specify the IP address of the TFTP server.
Step 10	**domain-name** *domainname* (Optional) Specify the domain name that the clients should use when resolving host names via DNS. *domainname*: Specify the domain name with up to 200 characters.
Step 11	**bootfile** *file-name* (Optional) Specify the name of the bootfile. If needed, the clients can get the bootfile from the TFTP server for auto installation. *file-name*: Specify the bootfile name with up to 128 characters.
Step 12	**show ip dhcp server pool** Verify the configuration of the DHCP server pool.
Step 13	**end** Return to Privileged EXEC Mode.

Step 14	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a DHCP server pool with the parameters shown in Table 2-1.

Table 2-1 Parameters for the DHCP Server Pool

Parameter	Value
Pool Name	pool 1
Network Address	192.168.1.0
Subnet Mask	255.255.255.0
Lease Time	180 minutes
Default Gateway	192.168.1.1
DNS Server	192.168.1.4
NetBIOS Server	192.168.1.19
NetBIOS Node Type	B-node (Broadcast)
TFTP server	192.168.1.30
Domain Name	com
Bootfile	bootfile

Switch#configure

Switch(config)#ip dhcp server pool pool1

Switch(dhcp-config)#network 192.168.1.0 255.255.255.0

Switch(dhcp-config)#lease 180

Switch(dhcp-config)#default-gateway 192.168.1.1

Switch(dhcp-config)#dns-server 192.168.1.4

Switch(dhcp-config)#netbios-name-server 192.168.1.19

Switch(dhcp-config)#netbios-node-type b-node

Switch(dhcp-config)#next server 192.168.1.30

Switch(dhcp-config)#domain-name com

Switch(dhcp-config)#bootfile bootfile

Switch(dhcp-config)#show ip dhcp server pool

Pool Name: pool1

Network Address: 192.168.1.0

Subenet Mask: 255.255.255.0

Lease Time: 180

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.4

Netbios Server: 192.168.1.19

Netbios Node Type: b-node

Next Server Address: 192.168.1.30

Domain Name: com

Bootfile Name: bootfile

Switch(dhcp-config)#end

Switch#copy running-config startup-config

2.2.3 Configuring Manual Binding

Some hosts, WWW server for example, requires a static IP address. To satisfy this requirement, you can manually bind the MAC address or client ID of the host to an IP address, and the DHCP server will reserve the bound IP address to this host at all times.

Follow these steps to configure Manual Binding:

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**ip dhcp server pool** *name* Create a DHCP server pool and enter DHCP Configuration Mode.

Step 3	Bind an IP address to a client: **address** *ip-address* **client-identifier** *client-id* Bind the specified IP address to the client with a specific hexadecimal client ID. *ip-address:* Specify the IP address to be bound. *client-id:* Specify the client ID in hexadecimal format. **address** *ip-address* **client-identifier** *client-id* **ascii** Bind the specified IP address to the client with a specific ASCII client ID. *ip-address:* Specify the IP address to be bound. *client-id:* Specify the client ID with ASCII characters. **address** *ip-address* **hardware-address** *hardware-address* **hardware-type** { ethernet | ieee802 } Bind the specified IP address to the client with a specific MAC address. *ip-address:* Specify the IP address to be bound. *hardware-address:* Enter the MAC address of the client. ethernet | ieee802: Specify a hardware type for the client, either Ethernet or IEEE802.
Step 4	**show ip dhcp server manual-binding** Verify the manual binding configuration.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind the IP address 192.168.1.33 in pool1 (on the subnet of 192.168.1.0) to the host with the MAC address 74:D4:68:22:3F:34:

Switch#configure

Switch(config)#ip dhcp server pool pool1

Switch(dhcp-config)#address 192.168.1.33 **hardware-address** 74:d4:68:22:3f:34 **hardware-type ethernet**

Switch(dhcp-config)#show ip dhcp server manual-binding

Pool Name	Client Id/Hardware Address	IP Address	Hardware Type	Bind Mode
-------	------------------	---------	----------	--------
pool1	74:d4:68:22:3f:34	192.168.1.33	Ethernet	MAC Address

Switch(dhcp-config)#end

Switch#copy running-config startup-config

3 DHCP Relay Configuration

To complete DHCP Relay configuration, follow these steps:

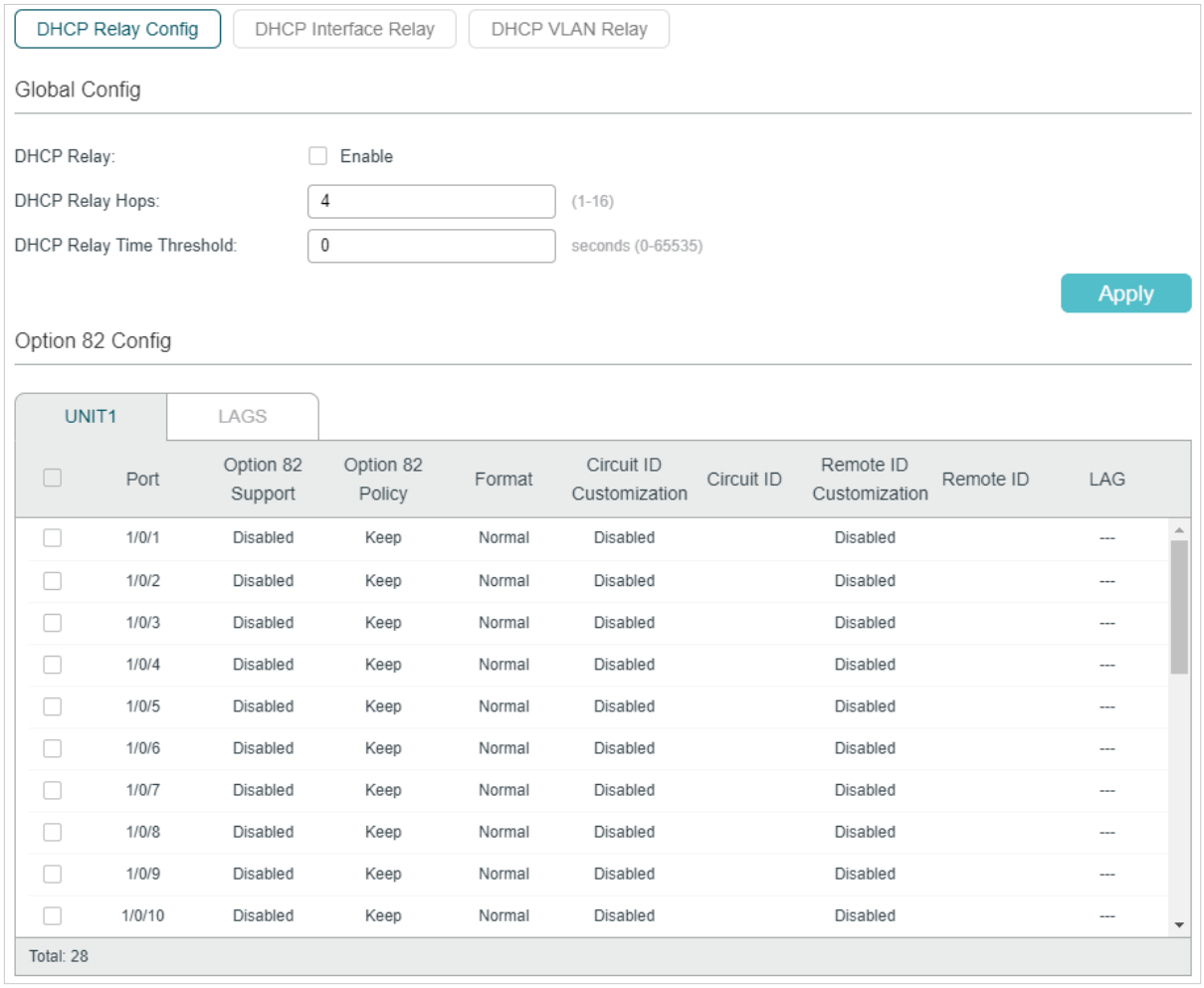
1) Enable DHCP Relay. Configure Option 82 if needed.
2) Specify DHCP server for the Interface or VLAN.

3.1 Using the GUI

3.1.1 Enabling DHCP Relay and Configuring Option 82

Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Relay Config** to load the following page.

Figure 3-1 Enable DHCP Relay and Configure Option 82



Follow these steps to enable DHCP Relay and configure Option 82:

1) In the **Global Config** section, enable DHCP Relay globally and configure the relay hops and time threshold. Click **Apply**.

DHCP Relay	Enable DHCP Relay globally.
DHCP Relay Hops	Specify the DHCP relay hops. DHCP Relay Hops defines the maximum number of hops (DHCP Relay agent) that the DHCP packets can be relayed. If a packet's hop count is more than the value you set here, the packet will be dropped.
DHCP Relay Time Threshold	Specify the threshold of the DHCP relay time. The valid values are from 0 to 65535 seconds. DHCP relay time is the time elapsed since the client began address acquisition or renewal process. There is a field in DHCP packets which specially records this time, and the switch will drop the packets if the value of this field is greater than the threshold. Value 0 means the switch will not examine this field of the DHCP packets.

2) (Optional) In the **Option 82 Config** section, configure Option 82.

Option 82 Support	Select whether to enable Option 82 or not. Enable it if you want to prevent DHCP client requests from untrusted sources, or assign different IP addresses to clients in different groups from the same DHCP server.
Option 82 Policy	Select the operation for the switch to take when receiving DHCP packets that include the Option 82 field. **Keep**: The switch keeps the Option 82 field of the packets. **Replace**: The switch replaces the Option 82 field of the packets with a new one. The switch presets a default circuit ID and remote ID in TLV (Type, Length, and Value) format. You can also configure the format to include Value only and customize the Value. **Drop**: The switch discards the packets that include the Option 82 field.
Format	Specify the packet format for the sub-option fields of Option 82. **Normal:** Indicates the fields consist of three parts: Type, Length, and Value (TLV). **Private:** Indicates the fields consist of the value only.
Circuit ID Customization	Enable or disable Circuit ID Customization. Enable it if you want to manually configure the circuit ID. Otherwise, the switch uses the default one when inserting Option 82 to DHCP packets. The default circuit ID is a 4-byte value which consists of 2-byte VLAN ID and 2-byte Port ID. The VLAN ID indicates which VLAN the DHCP client belongs to, and the Port ID indicates which port the DHCP client is connected to. For example, if the DHCP client is connected to port 1/0/1 in VLAN 2, this field is **00:02:00:01** in hexadecimal.
Circuit ID	Enter the customized circuit ID with up to 64 characters. The circuit ID configurations of the switch and the DHCP server should be compatible with each other.

Remote ID Customization	Enable or disable Remote ID Customization. Enable it if you want to manually configure the remote ID. Otherwise, the switch uses its own MAC address as the remote ID.
Remote ID	Enter the customized remote ID with up to 64 characters. The remote ID configurations of the switch and the DHCP server should be compatible with each other.

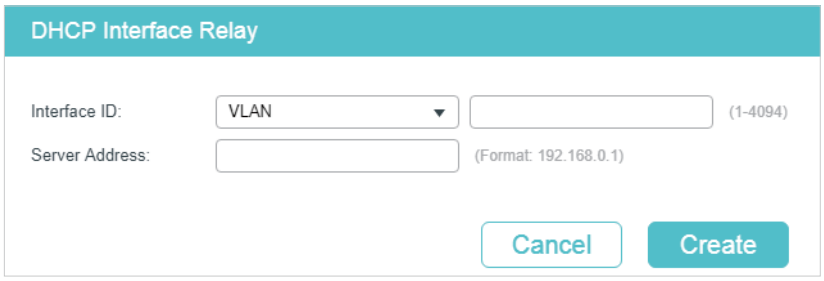
3) Click **Apply**.

3.1.2 Configuring DHCP Interface Relay

DHCP Interface Relay allows clients to obtain IP addresses from a DHCP server in a different subnet.

Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Interface Relay** and click Add to load the following page.

Figure 3-2 Configuring DHCP Interface Relay



Select the interface type and enter the interface ID, then enter the IP address of the DHCP server. Click **Create**.

Interface ID	Specify the type and ID of the interface. It is the Layer 3 interface which is connecting to the DHCP clients. The interface should be an existing Layer 3 interface.
Server Address	Enter the IP address of the DHCP server.

3.1.3 Configuring DHCP VLAN Relay

DHCP VLAN Relay allows clients in different VLANs to obtain IP addresses from a DHCP server using the IP address of a single agent interface. It is often used when the relay switch does not support configuring multiple Layer 3 interfaces.

Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP VLAN Relay** to load the following page.

Figure 3-3 Configure DHCP VLAN Relay

Follow these steps to specify DHCP Server for the specific VLAN:

1) In the **Default Relay Agent Interface** section, specify a Layer 3 interface as the default relay agent interface. Then click **Apply**.

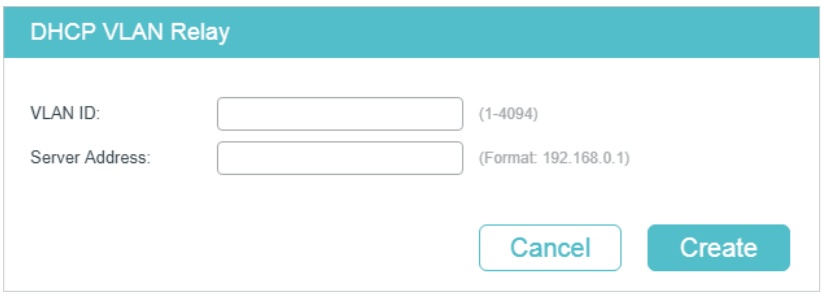
Interface ID	Specify the type and ID of the interface that needs to be configured as the default relay agent interface. You can configure any existing Layer 3 interface as the default relay-agent interface. The DHCP server will assign IP addresses in the same subnet with this relay agent interface to the clients who use this relay-agent interface to apply for IP addresses.
IP Address	Displays the IP address of this interface.

Note:

- If the VLAN the clients belong to already has an IP address, the switch will use the client's own VLAN interface as the relay-agent interface. The manually specified default relay agent will not take effect.
- DHCP VLAN Relay will not work on routed ports or port channel interfaces, because they are not associated with any particular VLAN.

2) In the **DHCP VLAN Relay Config** section, click Add to load the configuration page.

Figure 3-4 Specify a DHCP server for the VLAN



Specify the VLAN the clients belong to and the server address. Click **Create**.

VLAN ID	Specify the VLAN in which the clients can get IP addresses from the DHCP server.
Server Address	Enter the IP address of the DHCP server.

3.2 Using the CLI

3.2.1 Enabling DHCP Relay

Follow these steps to enable DHCP Relay and configure the corresponding parameters:

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**service dhcp relay** Enable DHCP Relay.
Step 3	**ip dhcp relay hops** *hops* Specify the maximum hops (DHCP relay agent) that the DHCP packets can be relayed. If a packet's hop count is more than the value you set here, the packet will be dropped. *hops:* Specify the maximum hops for DHCP packets. Valid values are from the 1 to 16, and the default value is 4.
Step 4	**ip dhcp relay time** *time* Specify the threshold for the DHCP relay time. DHCP relay time is the time elapsed since the client began address acquisition or renewal process. There is a field in DHCP packets which specially records this time, and the switch will drop the packets if the value of this field is greater than the threshold. Value 0 means the switch will not examine this field of the DHCP packets. *time:* Specify the threshold for the DHCP relay time. Valid values are from 1 to 65535. By default, the value is 0, which means the switch will not examine this field of the DHCP packets.
Step 5	**show ip dhcp relay** Verify the configuration of DHCP Relay.
Step 6	**end** Return to Privileged EXEC Mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Relay, configure the relay hops as 5 and configure the relay time as 10 seconds :

Switch#configure

Switch(config)#service dhcp relay

Switch(config)#show ip dhcp relay

Switch(config)#ip dhcp relay hops 5

Switch(config)#ip dhcp relay time 10

DHCP relay state: enabled

DHCP relay hops: 5

DHCP relay Time Threshold: 10 seconds

...

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 (Optional) Configuring Option 82

Follow these steps to configure Option 82:

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter Interface Configuration Mode.
Step 3	**ip dhcp relay information option** Enable the Option 82 feature on the port.
Step 4	**ip dhcp relay information strategy {** keep | replace | drop **}** Specify the operation for the switch to take when receiving DHCP packets that include the Option 82 field. keep: The switch keeps the Option 82 field of the packets. replace: The switch replaces the Option 82 field of the packets with a new one. The switch presets a default circuit ID and remote ID in TLV (Type, Length, and Value) format. You can also configure the format to include Value only and customize the Value. drop: The switch discards the packets that include the Option 82 field.
Step 5	**ip dhcp relay information format {** normal | private **}** Specify the packet format for the sub-option fields of Option 82. normal: Indicates the fields consist of three parts: Type, Length, and Value (TLV). private: Indicates the fields consist of the value only.

Step 6	**ip dhcp relay information circuit-id** *string* (Optional) A default circuit ID is preset on the switch, and you can also run this command to customize the circuit ID. The circuit ID configurations of the switch and the DHCP server should be compatible with each other. The default circuit ID is a 4-byte value which consists of 2-byte VLAN ID and 2-byte Port ID. The VLAN ID indicates which VLAN the DHCP client belongs to, and the Port ID indicates which port the DHCP client is connected to. For example, if the DHCP client is connected to port 1/0/1 in VLAN 2, this field is **00:02:00:01** in hexadecimal. *string:* Enter the customized circuit ID with up to 64 characters.
Step 7	**ip dhcp relay information remote-id** *string* (Optional) The switch uses its own MAC address as the default remote ID, and you can also run this command to customize the remote ID. The remote ID configurations of the switch and the DHCP server should be compatible with each other. *string:* Enter the remote ID with up to 64 characters.
Step 8	**show ip dhcp relay information interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Verify the Option 82 configurations of the port.
Step 9	**end** Return to Privileged EXEC Mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Option 82 on port 1/0/7 and configure the strategy as replace, the format as normal, the circuit-id as VLAN20 and the remote-id as Host1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/7

Switch(config-if)#ip dhcp relay information option

Switch(config-if)#ip dhcp relay information strategy replace

Switch(config-if)#ip dhcp relay information format normal

Switch(config-if)#ip dhcp relay information circut-id VLAN20

Switch(config-if)#ip dhcp relay information remote-id Host1

Switch(config-if)#show ip dhcp relay information interface gigabitEthernet 1/0/7

Interface	Option 82 Status	Operation Strategy	Format	Circuit ID	Remote ID	LAG
---	---	---	---	---	---	---
Gi1/0/7	Enable	Replace	Normal	VLAN20	Host1	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.3 Configuring DHCP Interface Relay

You can specify a DHCP server for a Layer 3 interface or for a VLAN. The following introduces how to configure DHCP Interface Relay and DHCP VLAN Relay, respectively.

Follow these steps to DHCP Interface Relay:

Step 1	**configure** Enter Global Configuration Mode.
Step 2	Enter Layer 3 Interface Configuration Mode: Enter VLAN Interface Configuration Mode: **interface vlan** *vlan-id* *vlan-id*: Specify an IEEE 802.1Q VLAN ID that already exists, ranging from 1 to 4094. Enter Routed Port Configuration Mode: **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Enter Interface Configuration Mode. *port*: Specify the Ethernet port number, for example, 1/0/1. **no switchport** Switch the Layer 2 port into the Layer 3 routed port. Enter Port-channel Interface Configuration Mode: **interface { port-cahnnel** *port-channel* **}** Enter Interface Configuration Mode. *port-channel*: Specify the port channel. Valid values are from 1 to 14. **no switchport** Switch the port channel to a Layer 3 port channel interface.
Step 3	**ip helper-address** *ip-addr* Specify DHCP server for the Layer 3 interface. *ip-addr:* Enter the IP address of the DHCP server.
Step 4	**show ip dhcp relay** Verify the configuration of DHCP Relay.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the DHCP server address as 192.168.1.7 on VLAN interface 66:

Switch#configure

Switch(config)#interface vlan 66

Switch(config-if)#ip helper-address 192.168.1.7

Switch(config-if)#show ip dhcp relay

...

DHCP relay helper address is configured on the following interfaces:

Interface	Helper address
VLAN 66	192.168.1.7

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.4 Configuring DHCP VLAN Relay

Follow these steps to configure DHCP VLAN Relay:

Step 1	**configure** Enter Global Configuration Mode.

Step 2	Enter Layer 3 Interface Configuration Mode: Enter VLAN Interface Configuration Mode: **interface vlan** *vlan-id* *vlan-id*: Specify an IEEE 802.1Q VLAN ID that already exists, ranging from 1 to 4094. Enter Routed Port Configuration Mode: **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Enter Interface Configuration Mode. *port*: Specify the Ethernet port number, for example, 1/0/1. **no switchport** Switch the Layer 2 port into the Layer 3 routed port. Enter Port-channel Interface Configuration Mode: **interface { port-cahnnel** *port-channel* **}** Enter Interface Configuration Mode. *port-channel*: Specify the port channel. Valid values are from 1 to 14. **no switchport** Switch the port channel to a Layer 3 port channel interface.
Step 3	**ip dhcp relay default-interface** Set the interface as the default relay-agent interface. If the VLAN that the clients belong to does not have an IP address, the switch will use the IP address of this interface to fill in the Relay Agent IP Address field of DHCP packets from the DHCP clients.
Step 4	**exit** Return to Global Configuration Mode.
Step 5	**ip dhcp relay vlan** *vid* **helper-address** *ip-address* Specify the VLAN ID and the DHCP server. *vid:* Enter the ID of the VLAN, in which the hosts can dynamically get the IP addresses from the DHCP server. *ip-address:* Enter the IP address of the DHCP server.
Step 6	**show ip dhcp relay** Verify the configuration of DHCP Relay.
Step 7	**end** Return to Privileged EXEC Mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the routed port 1/0/2 as the default relay agent interface and configure the DHCP server address as 192.168.1.8 on VLAN 10:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#no switchport

Switch(config-if)# ip dhcp relay default-interface

Switch(config-if)#exit

Switch(config)#ip dhcp relay vlan 10 **helper-address** 192.168.1.8

Switch(config)#show ip dhcp relay

...

DHCP VLAN relay helper address is configured on the following vlan:

vlan	Helper address
VLAN 10	192.168.1.8

Switch(config)#end

Switch#copy running-config startup-config

4 DHCP L2 Relay Configuration

To complete DHCP L2 Relay configuration, follow these steps:

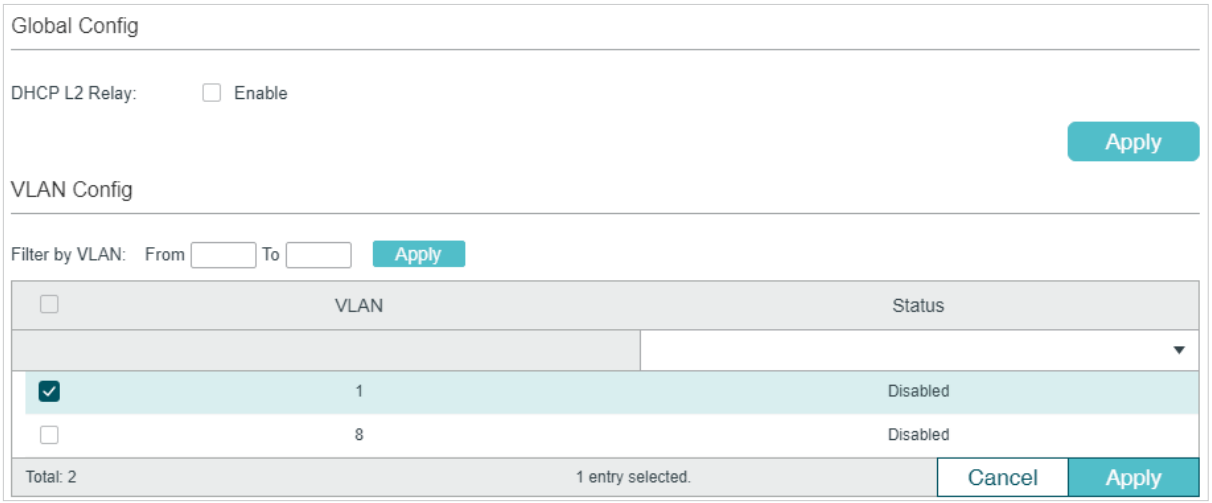
1) Enable DHCP L2 Relay.
2) Configure Option 82 for ports.

4.1 Using the GUI

4.1.1 Enabling DHCP L2 Relay

Choose the menu **L3 FEATURES > DHCP Service > DHCP L2 Relay > Global Config** to load the following page.

Figure 4-1 Enable DHCP L2 Relay



Follow these steps to enable DHCP L2 Relay globally for the specified VLAN:

1) In the **Global Config** section, enable DHCP L2 Relay globally. Click **Apply**.

DHCP L2 Relay	Enable DHCP Relay globally.

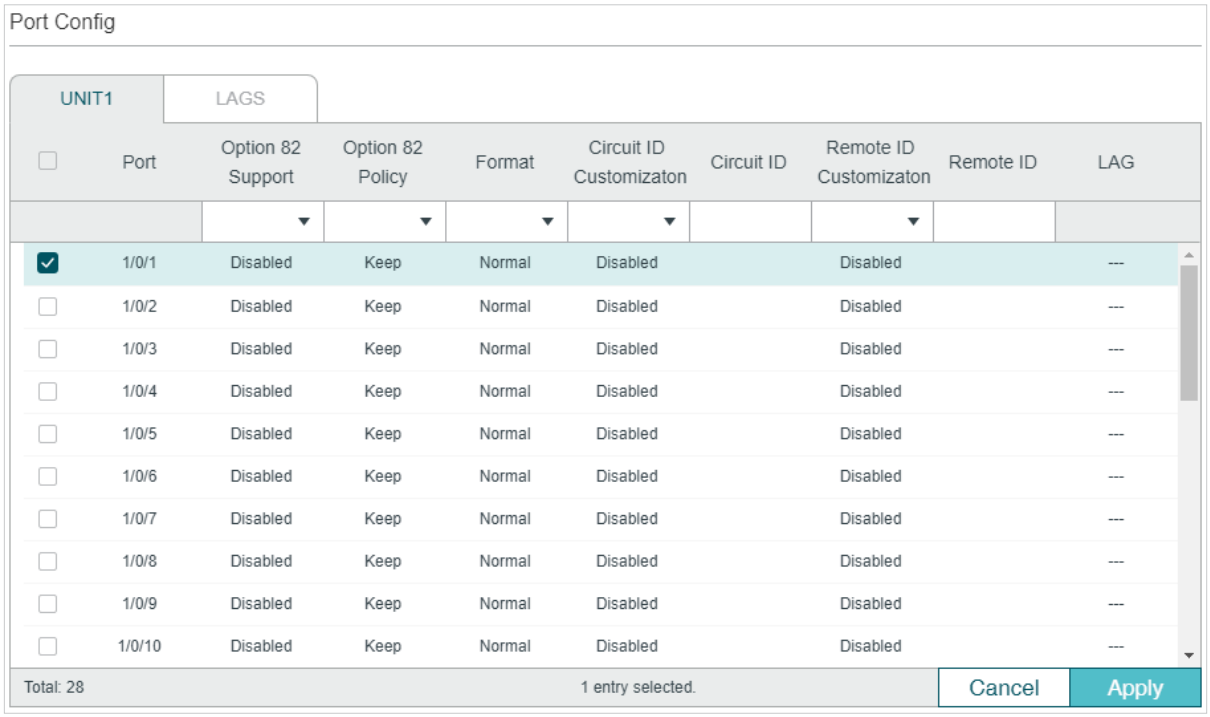
2) In the **VLAN Config** section, enable DHCP L2 Relay for the specified VLAN. Click **Apply**.

VLAN	Displays the VLAN ID.
Status	Enable DHCP L2 Relay for the specified VLAN.

4.1.2 Configuring Option 82 for Ports

Choose the menu **L3 FEATURES > DHCP Service > DHCP L2 Relay > Port Config** to load the following page.

Figure 4-2 Configure Option 82 for Ports



Follow these steps to enable DHCP Relay and configure Option 82:

1) Select one or more ports to configure Option 82.

Option 82 Support	Select whether to enable Option 82 or not. Enable it if you want to prevent DHCP client requests from untrusted sources, or assign different IP addresses to clients in different groups from the same DHCP server.
Option 82 Policy	Select the operation for the switch to take when receiving DHCP packets that include the Option 82 field. **Keep**: The switch keeps the Option 82 field of the packets. **Replace**: The switch replaces the Option 82 field of the packets with a new one. The switch presets a default circuit ID and remote ID in TLV (Type, Length, and Value) format. You can also configure the format to include Value only and customize the Value. **Drop**: The switch discards the packets that include the Option 82 field.

Format	Specify the packet format for the sub-option fields of Option 82. **Normal:** Indicates the fields consist of three parts: Type, Length, and Value (TLV). **Private:** Indicates the fields consist of the value only.
Circuit ID Customization	Enable or disable Circuit ID Customization. Enable it if you want to manually configure the circuit ID. Otherwise, the switch uses the default one when inserting Option 82 to DHCP packets. The default circuit ID is a 4-byte value which consists of 2-byte VLAN ID and 2-byte Port ID. The VLAN ID indicates which VLAN the DHCP client belongs to, and the Port ID indicates which port the DHCP client is connected to. For example, if the DHCP client is connected to port 1/0/1 in VLAN 2, this field is 00:02:00:01 in hexadecimal.
Circuit ID	Enter the customized circuit ID with up to 64 characters. The circuit ID configurations of the switch and the DHCP server should be compatible with each other.
Remote ID Customization	Enable or disable Remote ID Customization. Enable it if you want to manually configure the remote ID. Otherwise, the switch uses its own MAC address as the remote ID.
Remote ID	Enter the customized remote ID with up to 64 characters. The remote ID configurations of the switch and the DHCP server should be compatible with each other.

2) Click **Apply**.

4.2 Using the CLI

4.2.1 Enabling DHCP L2 Relay

Follow these steps to enable DHCP L2 Relay:

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**ip dhcp l2relay** Enable DHCP L2 Relay.
Step 3	**ip dhcp l2relay vlan** *vlan-list* Enable DHCP L2 Relay for specified VLANs. *vlan-list:* Specify the vlan to be enabled with DHCP L2 relay.
Step 5	**show ip dhcp l2relay** Verify the configuration of DHCP Relay.

Step 6	**end** Return to Privileged EXEC Mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP L2 Relay globally and for VLAN 2:

Switch#configure

Switch(config)#ip dhcp l2relay

Switch(config)#ip dhcp l2relay vlan 2

Switch(config)#show ip dhcp l2relay

Global Status: Enable

VLAN ID: 2

Switch(config)#end

Switch#copy running-config startup-config

4.2.2 Configuring Option 82 for Ports

Follow these steps to configure Option 82:

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter Interface Configuration Mode.
Step 3	**ip dhcp l2relay information option** Enable the Option 82 feature on the port.
Step 4	**ip dhcp l2relay information strategy {** keep | replace | drop **}** Specify the operation for the switch to take when receiving DHCP packets that include the Option 82 field. keep: The switch keeps the Option 82 field of the packets. replace: The switch replaces the Option 82 field of the packets with a new one. The switch presets a default circuit ID and remote ID in TLV (Type, Length, and Value) format. You can also configure the format to include Value only and customize the Value. drop: The switch discards the packets that include the Option 82 field.

Step 5	**ip dhcp l2relay information format {** normal | private **}** Specify the packet format for the sub-option fields of Option 82. normal: Indicates the fields consist of three parts: Type, Length, and Value (TLV). private: Indicates the fields consist of the value only.
Step 6	**ip dhcp l2relay information circuit-id** *string* (Optional) A default circuit ID is preset on the switch, and you can also run this command to customize the circuit ID. The circuit ID configurations of the switch and the DHCP server should be compatible with each other. The default circuit ID is a 4-byte value which consists of 2-byte VLAN ID and 2-byte Port ID. The VLAN ID indicates which VLAN the DHCP client belongs to, and the Port ID indicates which port the DHCP client is connected to. For example, if the DHCP client is connected to port 1/0/1 in VLAN 2, this field is **00:02:00:01** in hexadecimal. *string*: Enter the customized circuit ID with up to 64 characters.
Step 7	**ip dhcp l2relay information remote-id** *string* (Optional) The switch uses its own MAC address as the default remote ID, and you can also run this command to customize the remote ID. The remote ID configurations of the switch and the DHCP server should be compatible with each other. *string:* Enter the remote ID with up to 64 characters.
Step 8	**show ip dhcp l2relay information interface { fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Verify the Option 82 configuration of the port.
Step 9	**end** Return to Privileged EXEC Mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Option 82 on port 1/0/7 and configure the strategy as replace, the format as normal, the circuit-id as VLAN20 and the remote-id as Host1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/7

Switch(config-if)#ip dhcp l2relay information option

Switch(config-if)#ip dhcp l2relay information strategy replace

Switch(config-if)#ip dhcp l2relay information format normal

Switch(config-if)#ip dhcp l2relay information circut-id VLAN20

Switch(config-if)#ip dhcp l2relay information remote-id Host1

Switch(config-if)#show ip dhcp l2relay information interface gigabitEthernet 1/0/7

Interface	Option 82 Status	Operation Strategy	Format	Circuit ID	Remote ID	LAG
---	---	---	---	---	---	---
Gi1/0/7	Enable	Replace	Normal	VLAN20	Host1	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

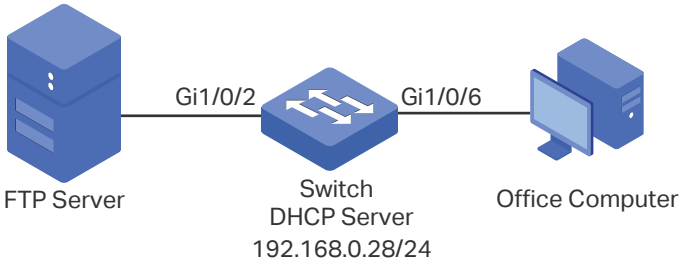
5 Configuration Examples

5.1 Example for DHCP Server

5.1.1 Network Requirements

As the network topology shows, the administrator uses the switch as the DHCP server to assign IP addresses to all the connected devices. The office computers need to obtain IP addresses dynamically, while the FTP server needs a fixed IP address.

Figure 5-1 Network Topology for DHCP Server



5.1.2 Configuration Scheme

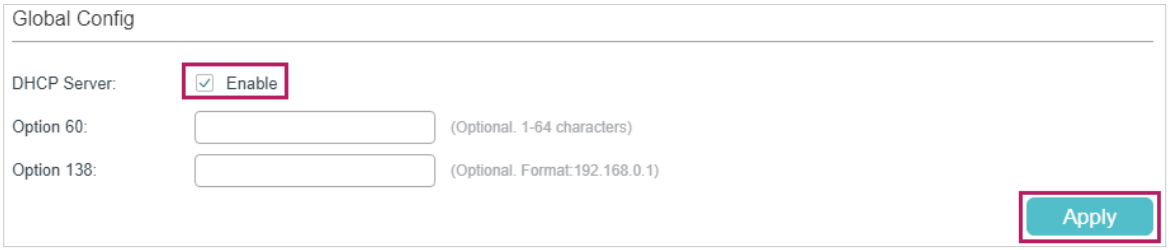
You can enable the DHCP Server service on the switch and create a DHCP IP pool for all the connected devices. Then manually bind the MAC address of the FTP server to an IP address specified for the FTP server.

Demonstrated with T1600G-28TS, the following sections provide configuration procedures in two ways: using the GUI and using the CLI.

5.1.3 Using the GUI

1) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > DHCP Server** to load the following page. In the **Global Config** section, enable DHCP Server and click **Apply**.

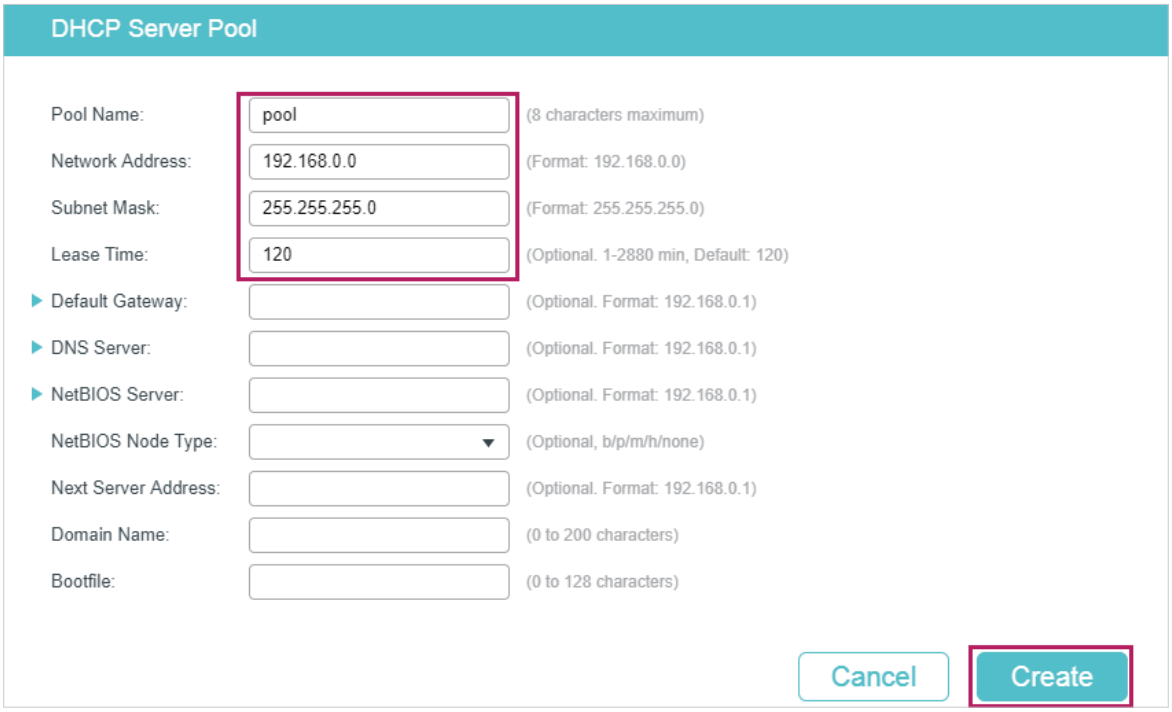
Figure 5-2 Configuring DHCP Server



2) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > Pool Setting** and click Add to load the following page. Specify the Pool Name, Network Address,

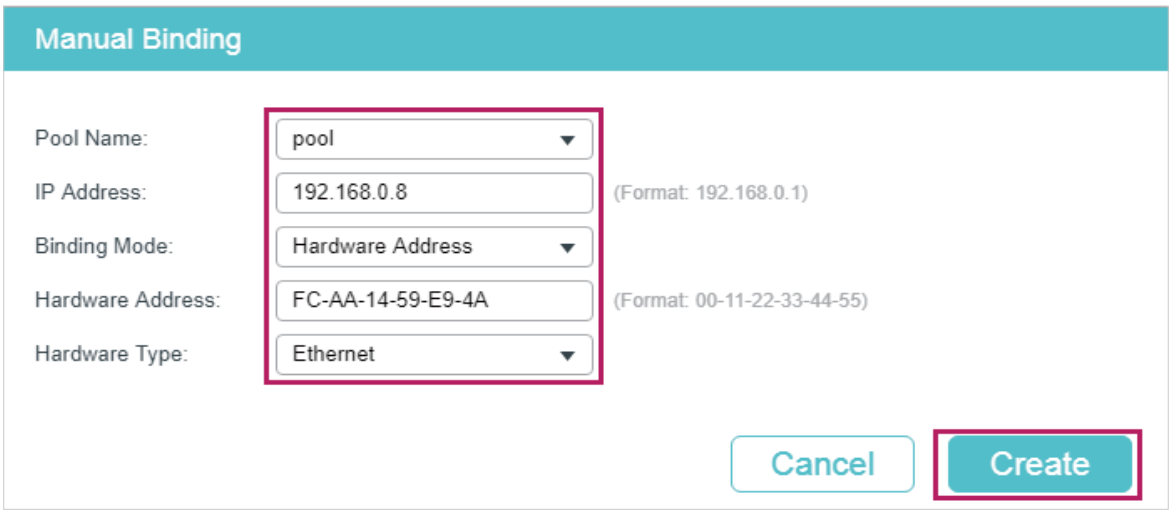
Subnet Mask, Lease Time, Default Gateway and DNS Server as shown below. Click **Create**.

Figure 5-3 Configuring DHCP Server Pool



3) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > Manual Binding** and click Add to load the following page. Select the DHCP server pool you just created, and enter the IP address of the FTP server in the IP Address field. Select Hardware Address as the binding mode, and enter the MAC address of the FTP server in the Hardware Address field. Select Ethernet as the Hardware Type. Click **Create**.

Figure 5-4 Configuring Manual Binding



4) Click Save to save the settings.

5.1.4 Using the CLI

1) Enable DHCP Server.

   Switch#configure

   Switch(config)#service dhcp server

2) Specify the Pool Name, Network Address, Subnet Mask and Lease Time.

   Switch(config)#ip dhcp server pool pool

   Switch(dhcp-config)#network 192.168.0.0 255.255.255.0

   Switch(dhcp-config)#lease 120

   Switch(dhcp-config)#exit

3) Bind the specified IP address to the MAC address of the FTP server.

   Switch(config)# ip dhcp server pool pool

   Switch(dhcp-config)# address 192.168.0.8 hardware-address FC-AA-14-59-E9-4A hardware-type ethernet

   Switch(dhcp-config)#end

   Switch#copy running-config startup-config

Verify the Configuration

Switch#show ip dhcp server binding

IP Address	Client id/Hardware Address	Type	Lease Time Left
192.168.0.2	01-d43d-7ebf-615f	Automatic	01:57:27
192.168.0.8	01-fcaa-1459-e94a	Manual	Infinite

5.2 Example for DHCP Interface Relay

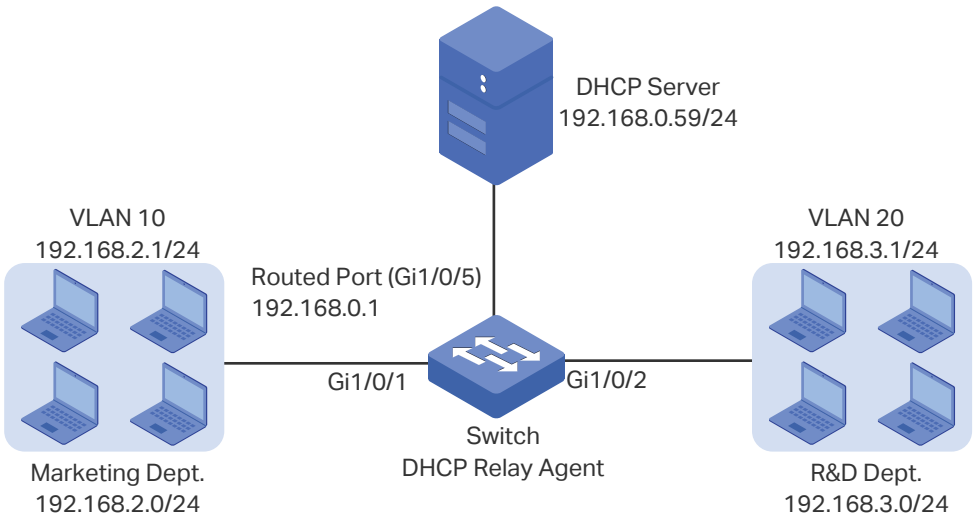
5.2.1 Network Requirements

The administrator deploys one DHCP server on the network, and wants the server to assign IP addresses to the computers in the Marketing department and the R&D department. It is required that computers in the same department should be on the same subnet, while computers in different departments should be on different subnets.

After adding the DHCP server, the network topology will be as shown in Figure 5-5. The Marketing department and the R&D department belong to VLAN 10 and VLAN 20, respectively. The IP address of VLAN interface 10 is 192.168.2.1/24, and the IP address of VLAN interface 20 is 192.168.3.1/24. The DHCP server is connected to the routed port of

the switch. The Marketing department is connected to port 1/0/1 of the relay agent, and the R&D department is connected to port 1/0/2 of the relay agent.

Figure 5-5 Network Topology for DHCP Interface Relay



5.2.2 Configuration Scheme

In the given situation, the DHCP server and the computers are isolated in different network segments, so the DHCP requests from the clients cannot be directly forwarded to the DHCP server. To assign IP addresses in two different subnets to two departments respectively, we recommend you to configure DHCP Interface Relay to satisfy the requirement.

The overview of the configurations are as follows:

1) Before configuring DHCP Interface Relay, create two DHCP IP pools on the DHCP server for the two departments, respectively. Then create static routes or enable dynamic routing protocol like RIP on the DHCP server to make sure the DHCP server can reach the clients in the two VLANs.
2) Configure 802.1Q VLAN on the DHCP relay agent. Add all computers in the marketing department to VLAN 10, and add all computers in the R&D department to VLAN 20.
3) Create VLAN interfaces for VLAN 10 and VLAN 20 on the DHCP relay agent.
4) Configure DHCP Interface Relay on the DHCP relay agent. Enable DHCP Relay globally, and specify the DHCP server address for each VLAN.

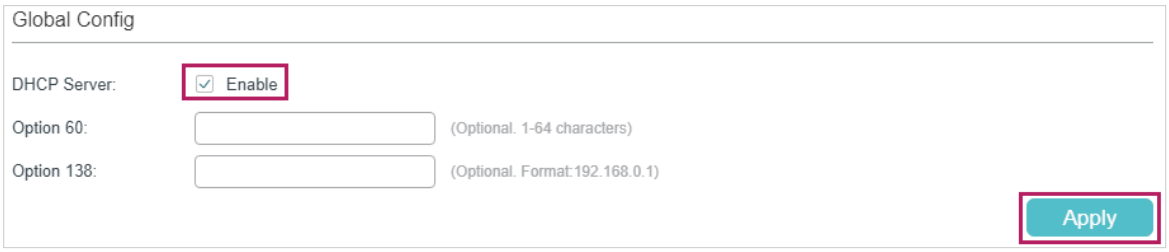
In this example, the DHCP server is demonstrated with T1600G-52TS and the DHCP relay agent is demonstrated with T1600G-28TS. This section provides configuration procedures in two ways: using the GUI and using the CLI.

5.2.3 Using the GUI

Configuring the DHCP Server

1) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > DHCP Server** to load the following page. In the **Global Config** section, enable DHCP Server globally.

Figure 5-6 Configuring DHCP Server



2) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > Pool Setting** and click Add to load the following page. Create pool 1 for VLAN 10 and pool 2 for VLAN 20. Configure the corresponding parameters as the following pictures show.

Figure 5-7 Configuring DHCP Pool 1 for VLAN 10

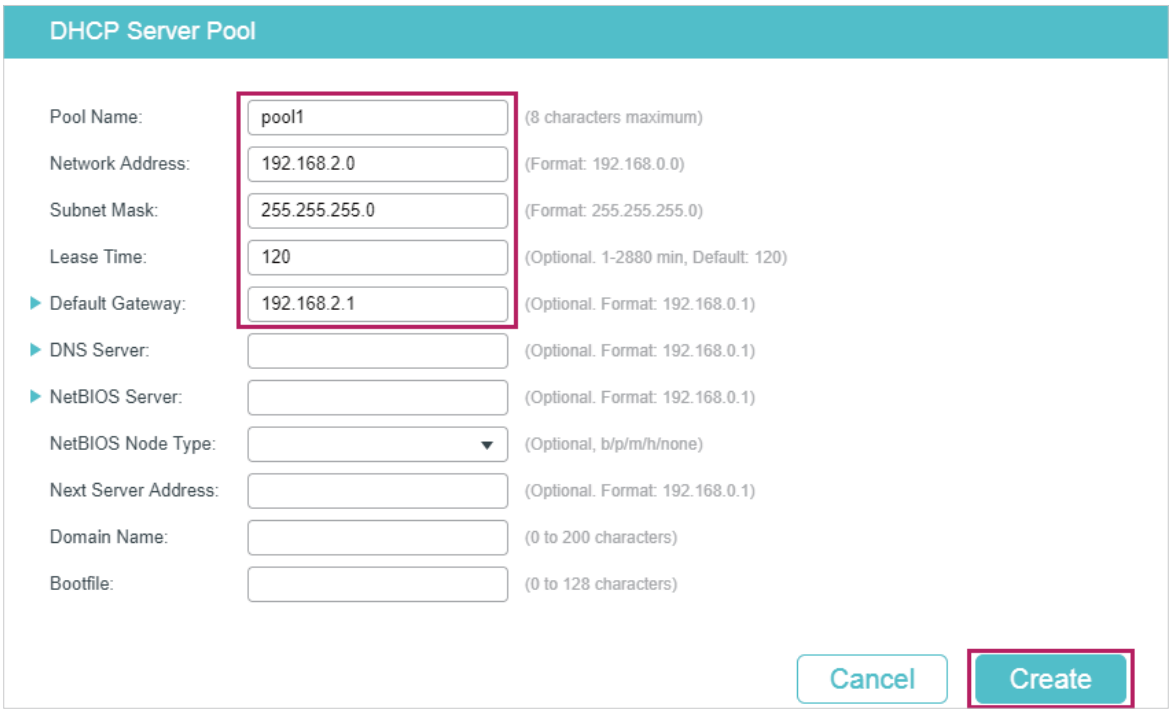
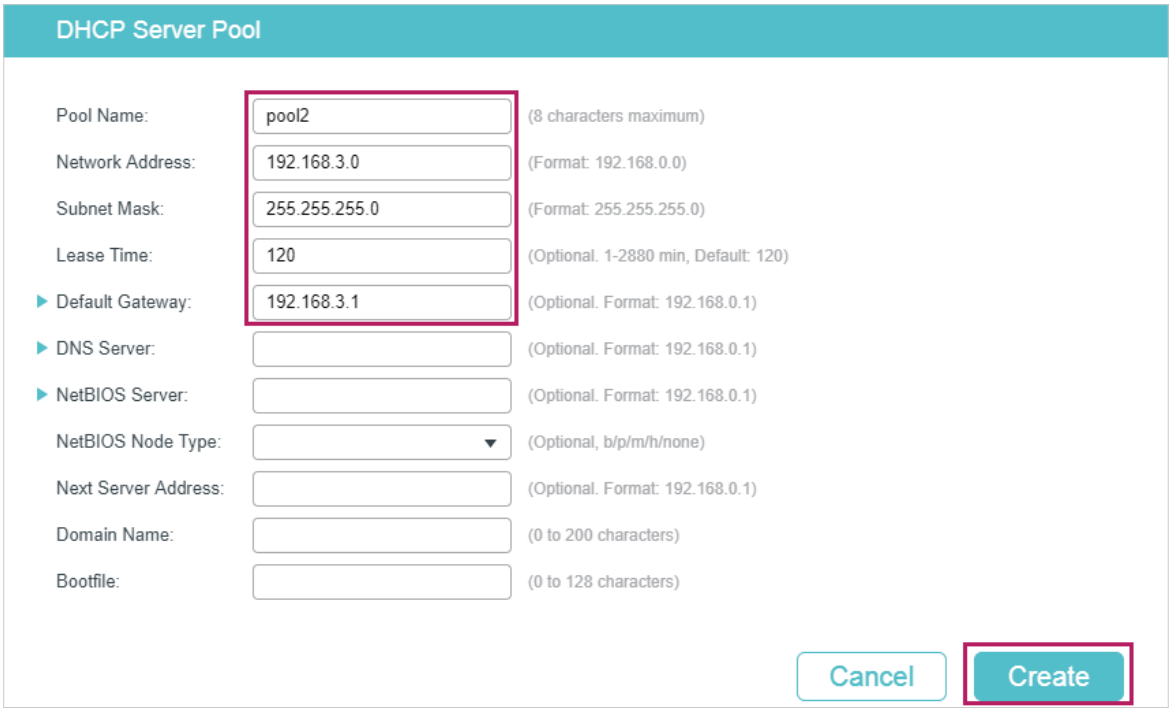


Figure 5-8 Configuring DHCP Pool 2 for VLAN 20



3) Choose the menu **L3 FEATURES > Static Routing > IPv4 Static Routing** and click Add to load the following page. Create two static routing entries for the DHCP server to make sure that the DHCP server can reach the clients in the two VLANs.

Figure 5-9 Creating the Static Routing Entry for VLAN 10

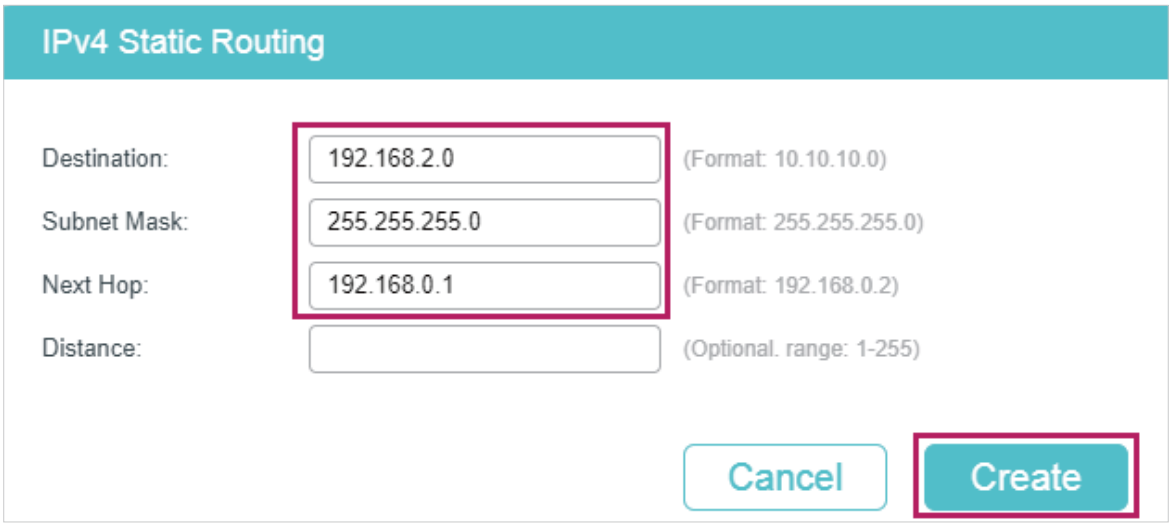
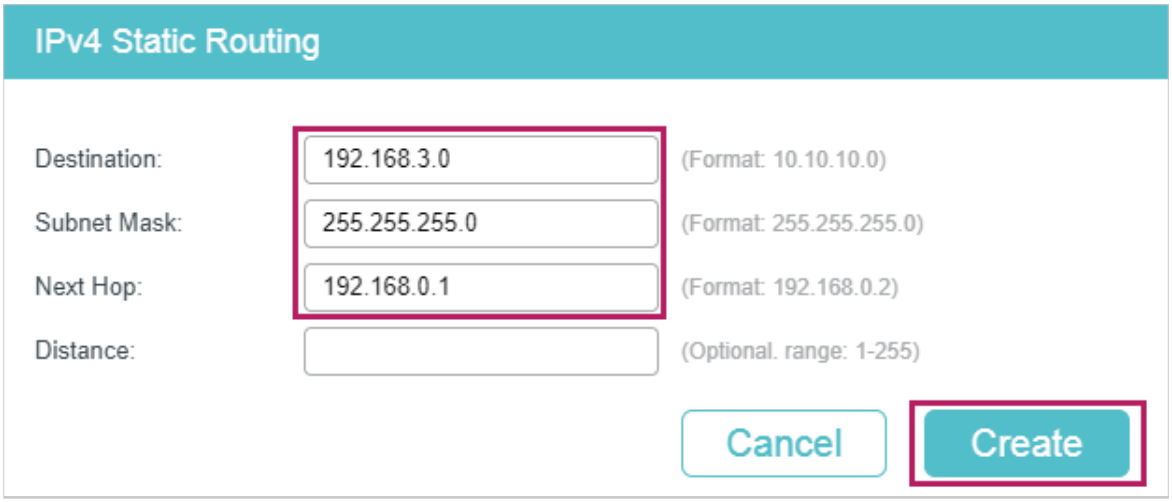


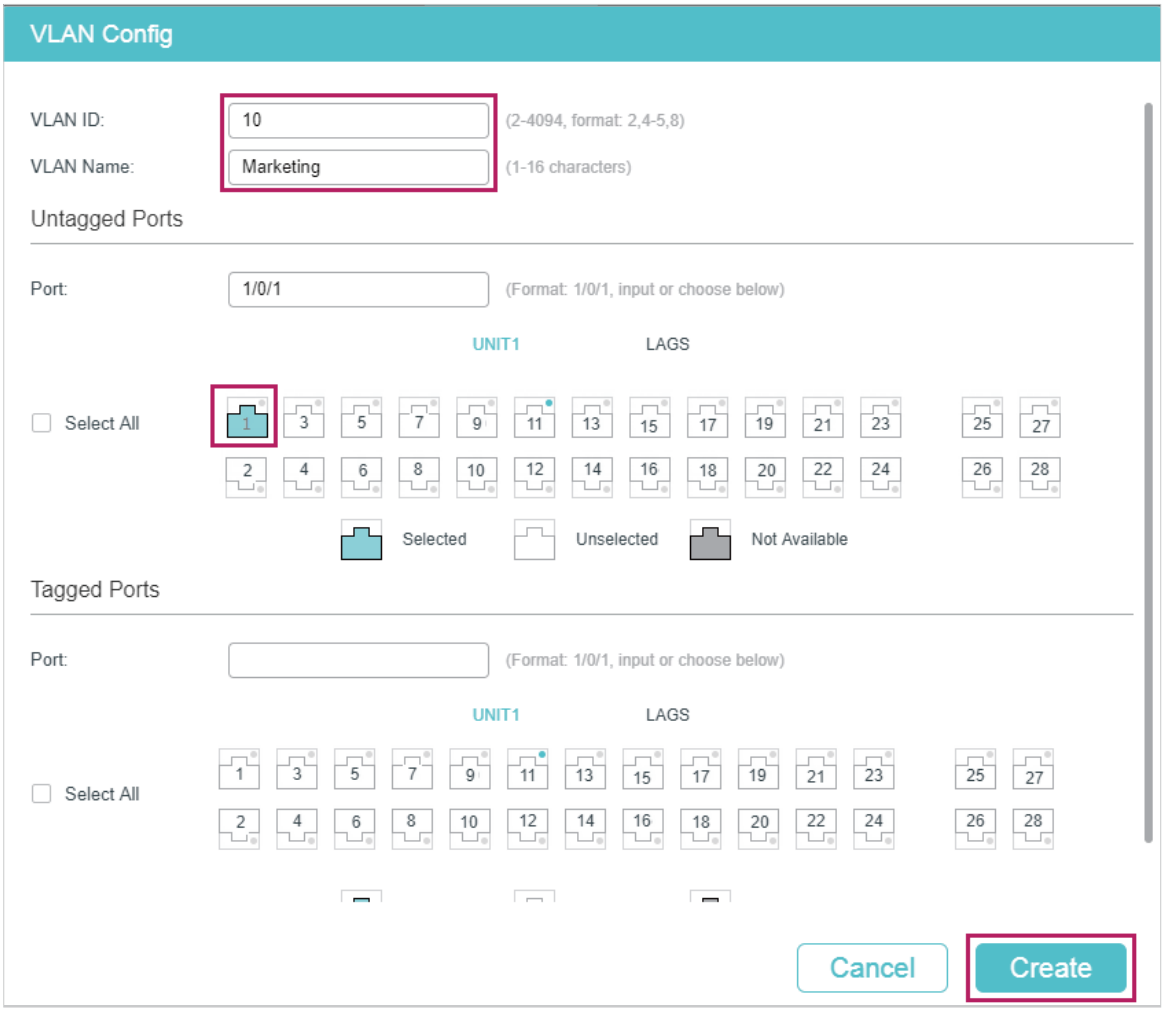
Figure 5-10 Creating the Static Routing Entry for VLAN 20



Configuring the VLANs on the Relay Agent

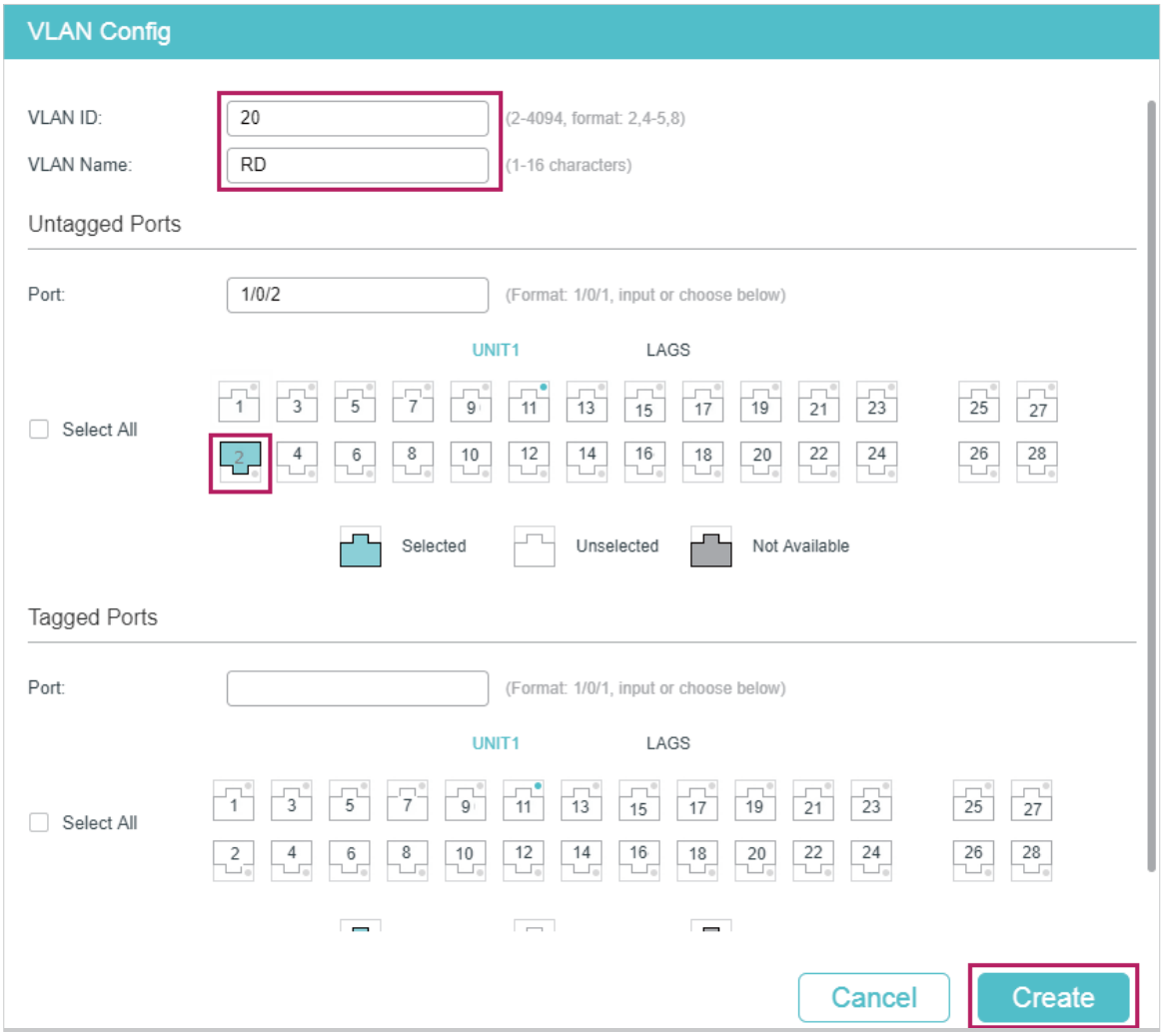
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 10 for the Marketing department and add port 1/0/1 as an untagged port to the VLAN.

Figure 5-11 Creating VLAN 10



2) On the same page, click Add again to create VLAN 20 for the R&D department and add port 1/0/2 as an untagged port to the VLAN.

Figure 5-12 Creating VLAN 20



- Configuring the VLAN Interface and Routed Port on the Relay Agent

1) Choose the menu **L3 FEATURES > Interface** and click Add to load the following page. Create VLAN interface 10 and VLAN interface 20. Configure port 1/0/5 as the routed port.

Figure 5-13 Creating VLAN Interface 10

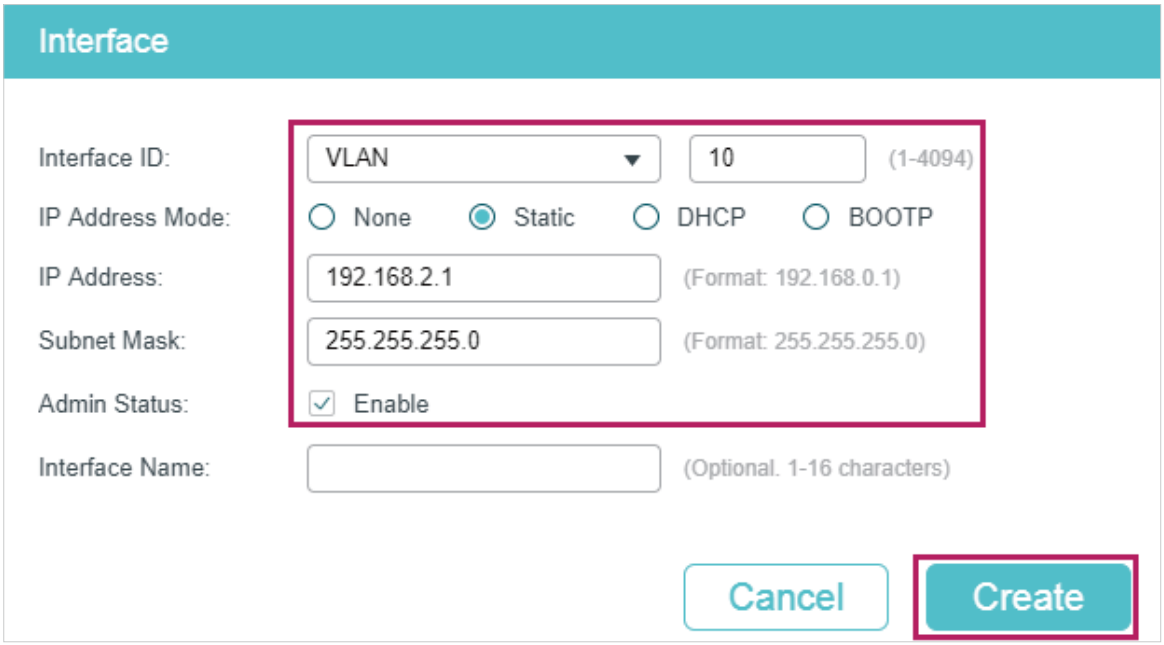
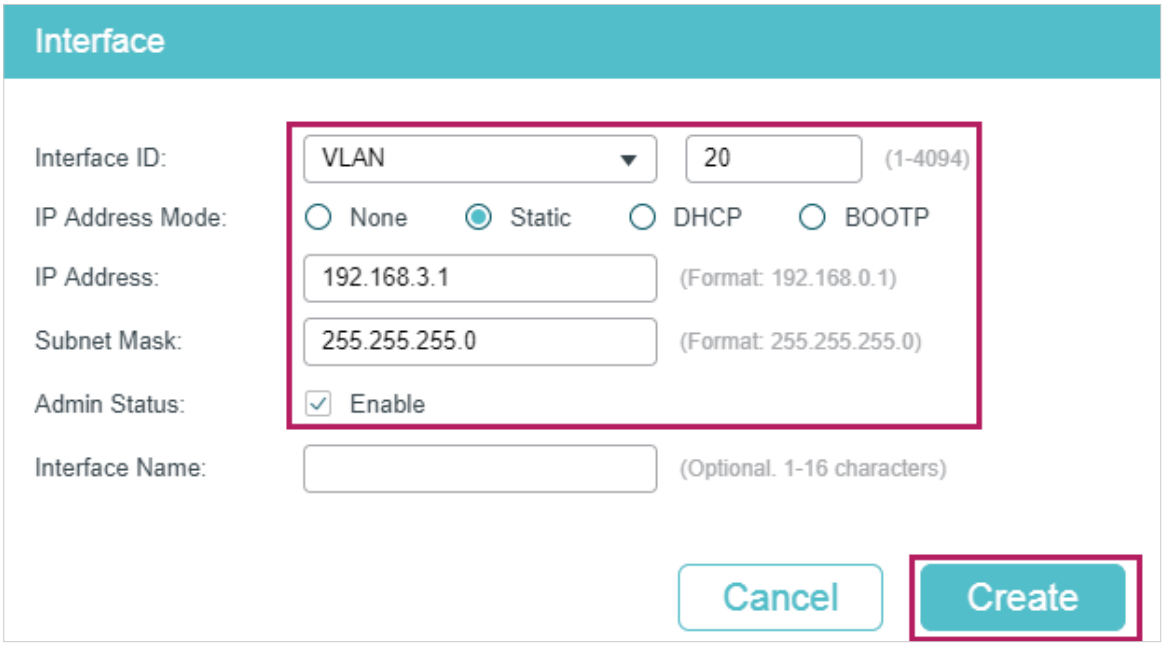
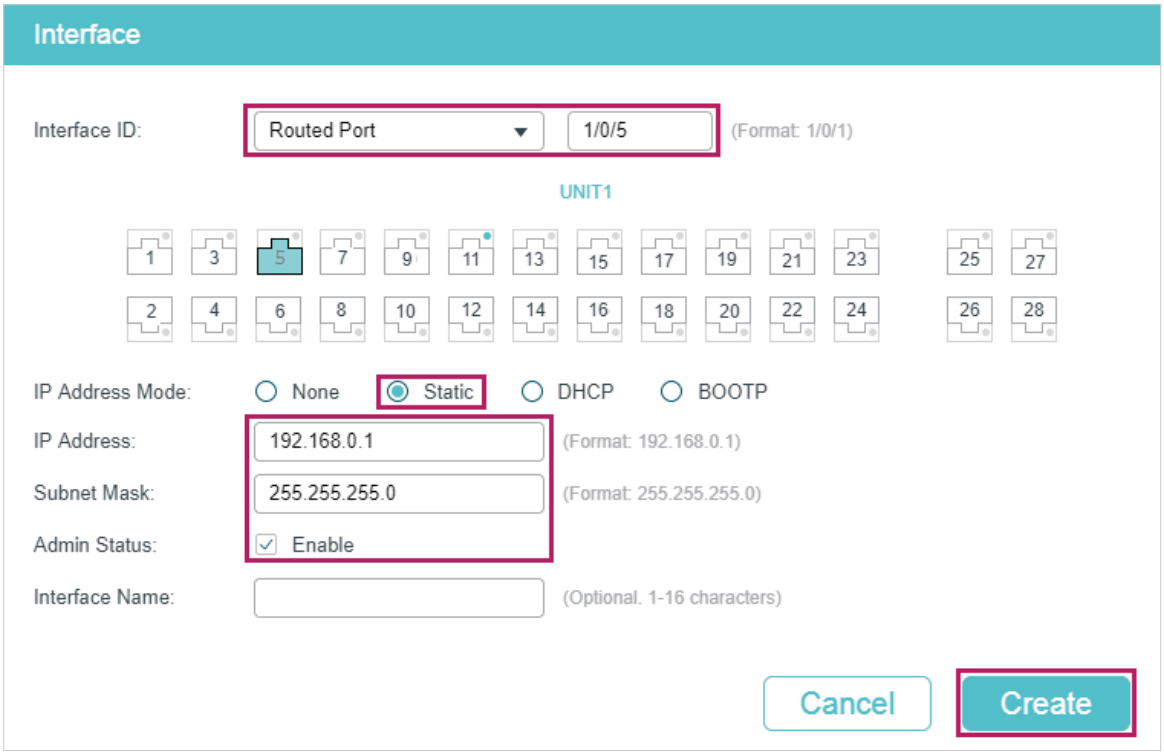


Figure 5-14 Creating VLAN Interface 20



2) On the same page, click Add again to configure port 1/0/5 as the routed port.

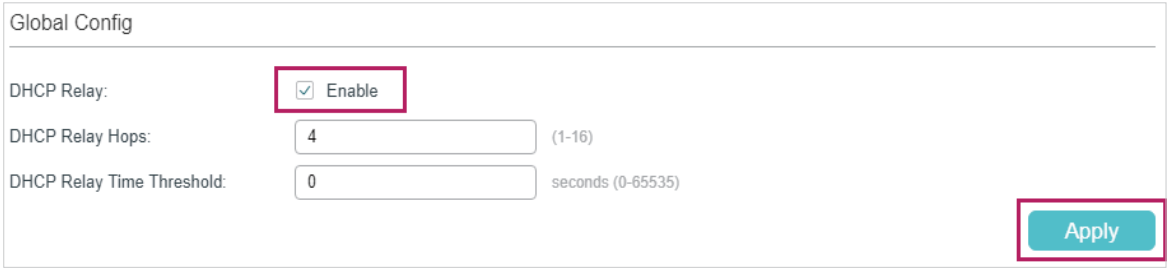
Figure 5-15 Configuring the Routed Port



Configuring DHCP Interface Relay on the Relay Agent

1) Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Relay Config** to load the following page. In the **Global Config** section, enable DHCP Relay, and click **Apply**.

Figure 5-16 Enable DHCP Relay



2) Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Interface Relay** and click Add to load the following page. Specify the DHCP server for the clients in VLAN 10 and VLAN 20.

Figure 5-17 Specify DHCP Server for Interface VLAN 10

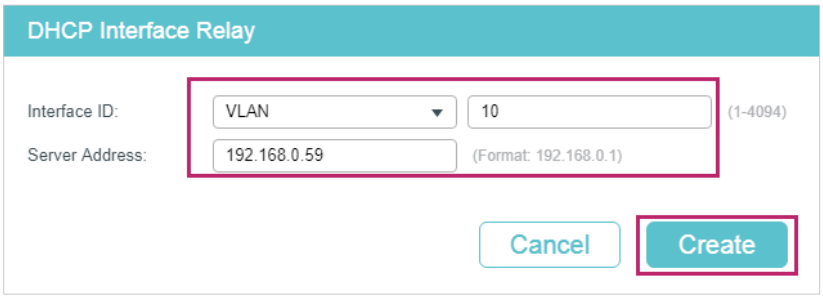
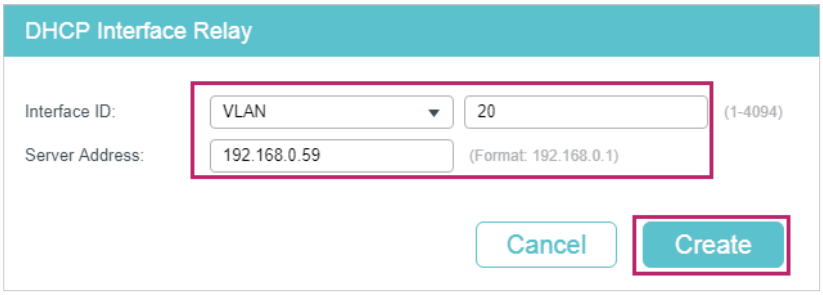


Figure 5-18 Specify DHCP Server for Interface VLAN 20



3) Click Save to save the settings.

5.2.4 Using the CLI

- Configurting the DHCP Server

1) Enable DHCP service globally.

Switch#configure

Switch(config)#service dhcp server

2) Create DHCP pool 1 and configure its network address as 192.168.2.0, subnet mask as 255.255.255.0, lease time as 120 minutes, default gateway as 192.168.2.1; Create DHCP pool 2 and configure its network address as 192.168.3.0, subnet mask as 255.255.255.0, lease time as 120 minutes, default gateway as 192.168.3.1.

Switch(config)#ip dhcp server pool pool1

Switch(dhcp-config)#network 192.168.2.0 255.255.255.0

Switch(dhcp-config)#lease 120

Switch(dhcp-config)#default-gateway 192.168.2.1

Switch(dhcp-config)#exit

Switch(config)#ip dhcp server pool pool2

Switch(dhcp-config)#network 192.168.2.0 255.255.255.0

Switch(dhcp-config)#lease 120

Switch(dhcp-config)#default-gateway 192.168.3.1

Switch(dhcp-config)#exit

3) Create two static routing entries to make sure that the DHCP server can reach the clients in the two VLANs.

Switch(config)# ip route 192.168.2.0 255.255.255.0 192.168.0.1

Switch(config)# ip route 192.168.3.0 255.255.255.0 192.168.0.1

Switch(config)#end

Switch#copy running-config startup-config

- Configuring the VLAN on the Relay Agent

Switch(config)# vlan 10

Switch(config-vlan)#name Marketing

Switch(config-vlan)#exit

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#switchport general allowed vlan 10 untagged

Switch(config-if)#exit

Switch(config)# vlan 20

Switch(config-vlan)#name RD

Switch(config-vlan)#exit

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#switchport general allowed vlan 20 untagged

Switch(config-if)#exit

- Configuring the VLAN Interfaces Routed Port on the Relay Agent

Switch(config)#interface vlan 10

Switch(config-if)#ip address 192.168.2.1 255.255.255.0

Switch(config-if)#exit

Switch(config)#interface vlan 20

Switch(config-if)#ip address 192.168.3.1 255.255.255.0

Switch(config-if)#exit

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#ip address 192.168.0.1 255.255.255.0

Switch(config-if)#exit

- Configuring DHCP Interface Relay on the Relay Agent

1) Enable DHCP Relay.

Switch#configure

Switch(config)#service dhcp relay

2) Specify the DHCP server for the interface VLAN 10.

```
Switch(config)#interface vlan 10
Switch(config-if)#ip helper-address 192.168.0.59
Switch(config-if)#exit
```

3) Specify the DHCP server for interface VLAN 20

```
Switch(config)#interface vlan 20
Switch(config-if)#ip helper-address 192.168.0.59
Switch(config-if)#end
Switch#copy running-config startup-config
```

Verify the Configurations of the DHCP Relay Agent

```
Switch#show ip dhcp relay
DHCP relay is enabled
...
DHCP relay helper address is configured on the following interfaces:
Interface            Helper address
-------------------- ------------------------
VLAN10               192.168.0.59
VLAN20               192.168.0.59
...
```

5.3 Example for DHCP VLAN Relay

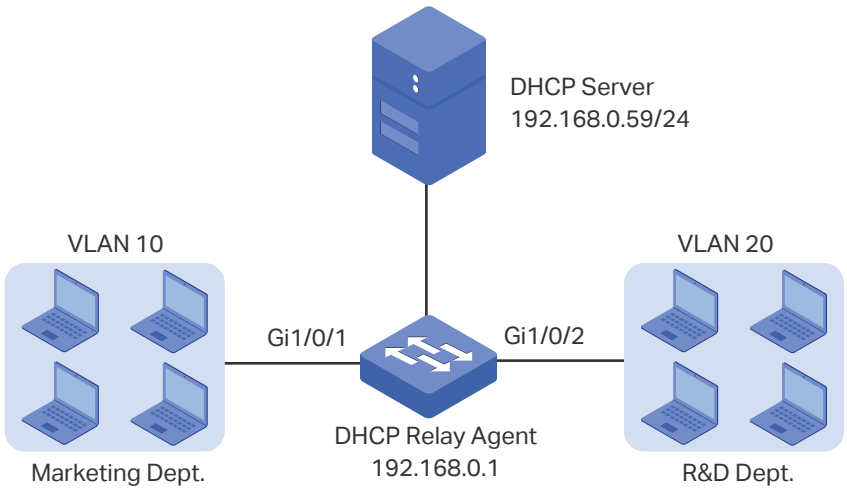
5.3.1 Network Requirements

The administrator needs to deploy the office network for the Marketing department and the R&D department. The detailed requirements are listed below:

- The Marketing department and the R&D department belong to VLAN 10 and VLAN 20, respectively. Both of the VLANs have no Layer 3 gateways.
- Computers in the two departments need to obtain IP addresses from the same DHCP server.

The network topology designed by the administrator is shown below.

Figure 5-19 Network Topology for DHCP VLAN Relay



5.3.2 Configuration Scheme

In the given situation, the DHCP server and the computers are isolated by VLANs, so the DHCP request from the clients cannot be directly forwarded to the DHCP server. Considering that the two VLANs have no Layer 3 gateways, we recommend you to configure DHCP VLAN Relay to satisfy the requirement.

The overview of the configurations are as follows:

1) Create one DHCP IP pool on the DHCP server, which is on 192.168.0.0/24 network segment.
2) Configure 802.1Q VLAN on the DHCP relay agent. Add all computers in the marketing department to VLAN 10, and add all computers in the R&D department to VLAN 20.
3) Configure DHCP VLAN Relay on the DHCP relay agent. Enable DHCP Relay globally, choose the VLAN interface 1 (the default management VLAN interface) as the default relay agent interface, and specify the DHCP server address for VLAN 10 and VLAN 20.

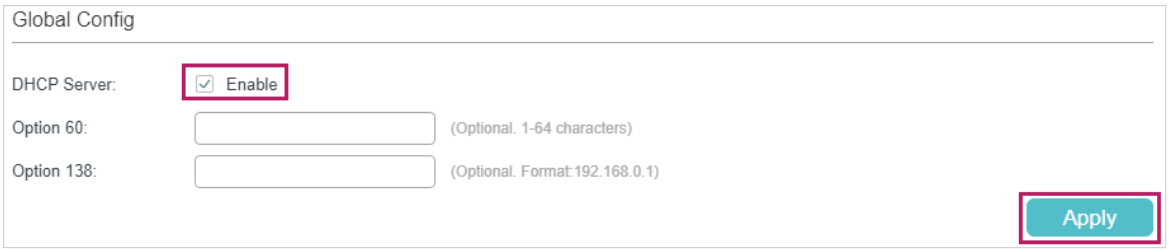
In this example, the DHCP server is demonstrated with T1600G-52TS and the DHCP relay agent is demonstrated with T1600G-28TS. The following sections provide configuration procedures in two ways: using the GUI and using the CLI.

5.3.3 Using the GUI

Configuring the DHCP Server

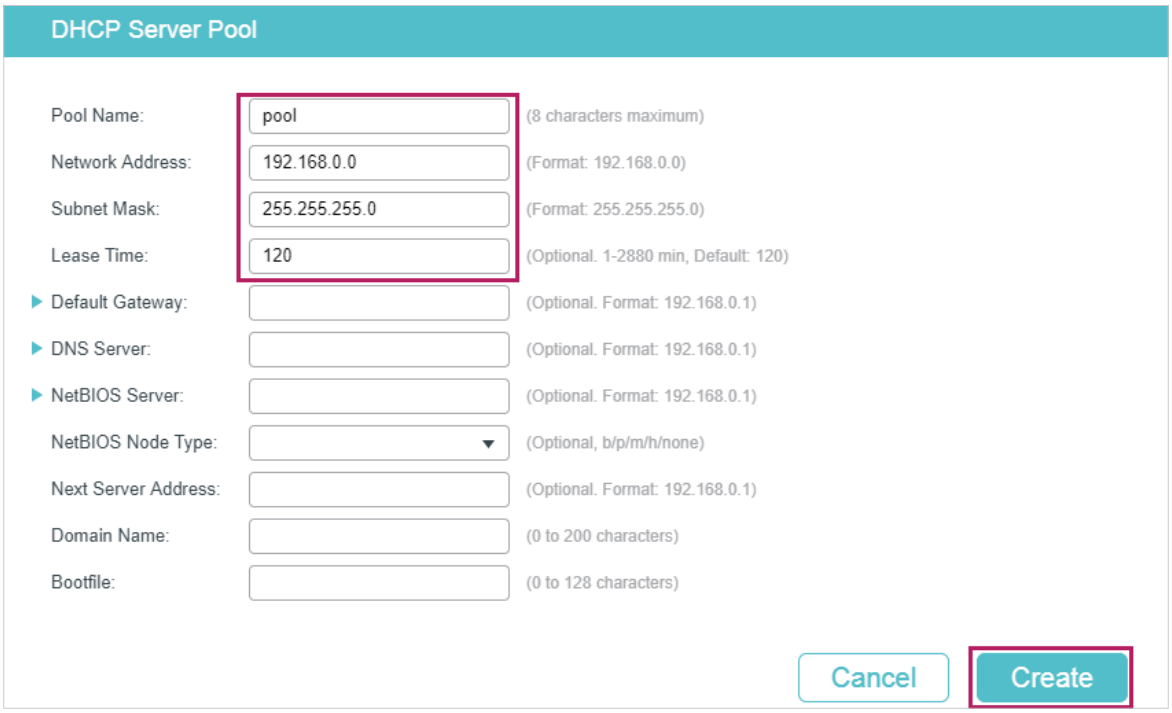
1) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > DHCP Server** to load the following page. In the **Global Config** section, enable DHCP Server globally.

Figure 5-20 Configuring DHCP Server



2) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > Pool Setting** and click Add to load the following page. Create a DHCP pool for the clients. Configure the corresponding parameters as the following picture shows.

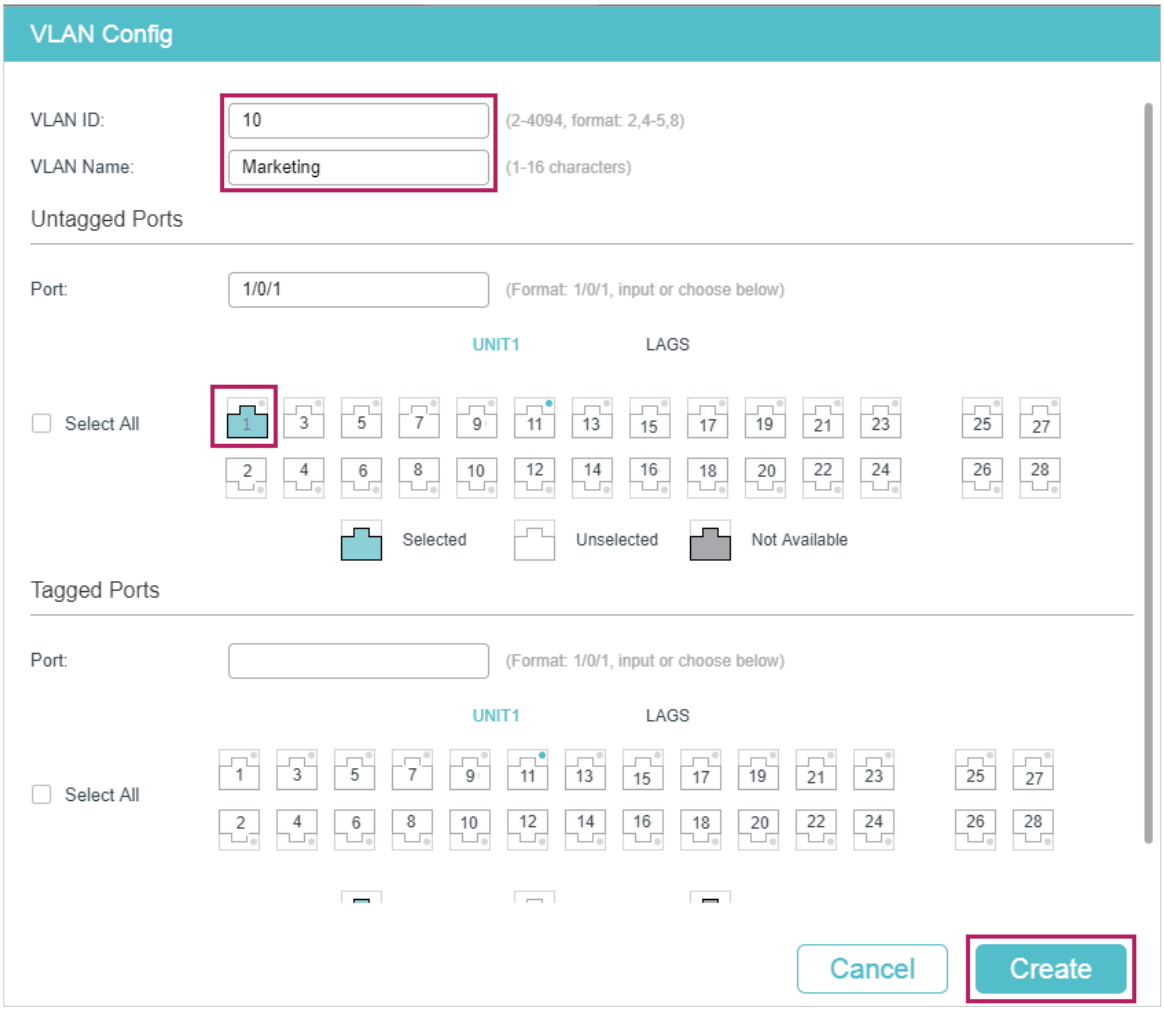
Figure 5-21 Configuring DHCP Pool 1 for VLAN 10



Configuring the VLANs on the Relay Agent

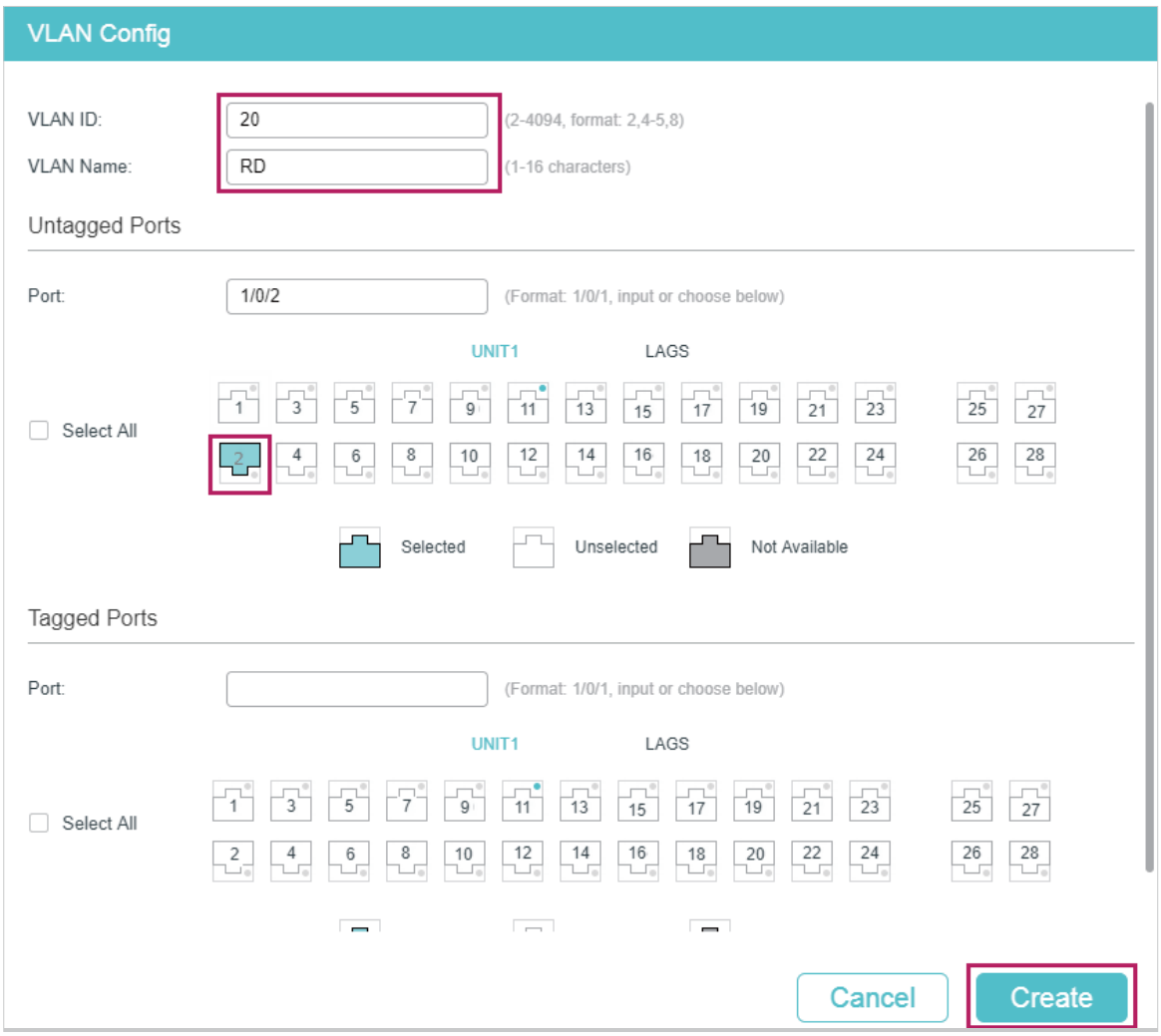
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 10 for the Marketing department and add port 1/0/1 as untagged port to the VLAN.

Figure 5-22 Creating VLAN 10



2) On the same page, click Add again to create VLAN 20 for the R&D department and add port 1/0/2 as untagged port to the VLAN.

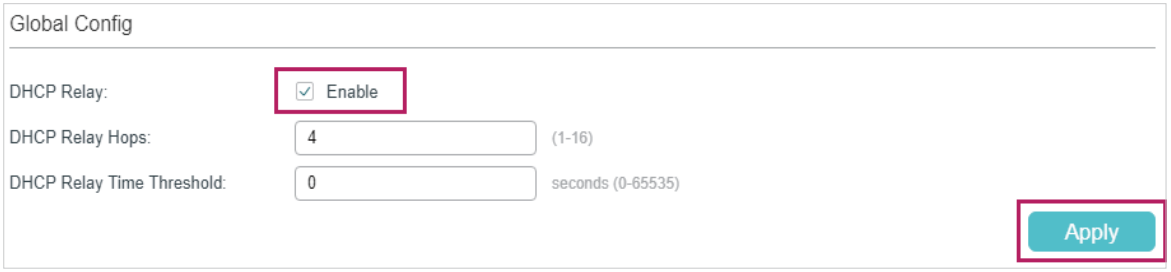
Figure 5-23 Creating VLAN 20



Configuring DHCP VLAN Relay on the Relay Agent

1) Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Relay Config** to load the following page. In the **Global Config** section, enable DHCP Relay, and click **Apply**.

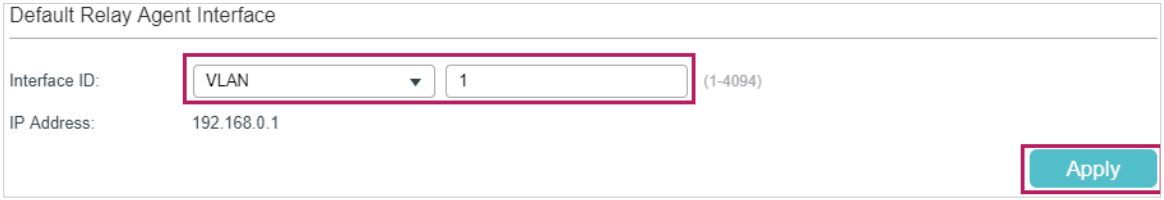
Figure 5-24 Enable DHCP Relay



2) Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP VLAN Relay** to load the following page. In the **Default Relay Agent Interface** section, specify

VLAN interface 1 (the default management VLAN interface) as the default relay-agent interface. Click **Apply**.

Figure 5-25 Specify the Default Relay Agent Interface



3) Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP VLAN Relay** and click Add to load the following page. Specify the DHCP server address for the clients in VLAN 10 and VLAN 20.

Figure 5-26 Specify DHCP Server for Interface VLAN 10

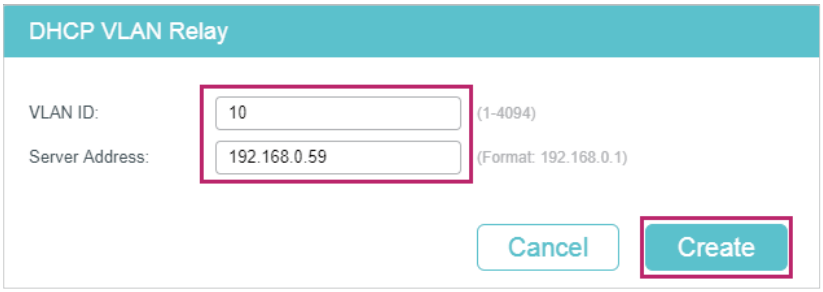
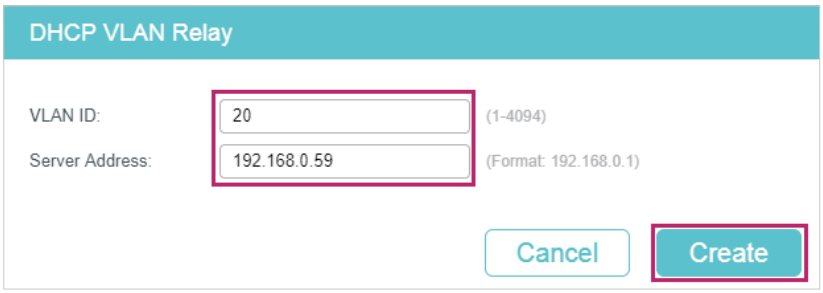


Figure 5-27 Specify DHCP Server for Interface VLAN 20



4) Click Save to save the settings.

5.3.4 Using the CLI

- Configurting the DHCP Server

1) Enable DHCP service globally.

Switch#configure

Switch(config)#service dhcp server

2) Create a DHCP pool and name it as “pool” and configure its network address as 192.168.0.0, subnet mask as 255.255.255.0, lease time as 120 minutes, default gateway as 192.168.0.1.

Switch(config)#ip dhcp server pool pool

Switch(dhcp-config)#network 192.168.0.0 255.255.255.0

```
Switch(dhcp-config)#lease 120
Switch(dhcp-config)#default-gateway 192.168.0.1
Switch(dhcp-config)#dns-server 192.168.0.2
Switch(dhcp-config)#end
Switch#copy running-config startup-config
```

- Configuring the VLAN on the Relay Agent

```
Switch#configure
Switch(config)# vlan 10
Switch(config-vlan)#name Marketing
Switch(config-vlan)#exit
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#switchport general allowed vlan 10 untagged
Switch(config-if)#exit
Switch(config)# vlan 20
Switch(config-vlan)#name RD
Switch(config-vlan)#exit
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#switchport general allowed vlan 20 untagged
Switch(config-if)#exit
```

- Configuring DHCP VLAN Relay on the Relay Agent

1) Enable DHCP Relay.

```
Switch(config)#service dhcp relay
```

2) Specify the routed port 1/0/5 as the default relay agent interface.

```
Switch(config)#interface vlan 1
Switch(config-if)#ip dhcp relay default-interface
Switch(config-if)#exit
```

3) Specify the DHCP server for VLAN 10 and VLAN 20

```
Switch(config)#ip dhcp relay vlan 10 helper-address 192.168.0.59
Switch(config)#ip dhcp relay vlan 20 helper-address 192.168.0.59
Switch(config)#exit
```

Verify the Configurations of the DHCP Relay Agent

Switch#show ip dhcp relay

Switch#show ip dhcp relay

DHCP relay state: enabled

...

DHCP relay default relay agent interface:

Interface: VLAN 1

IP address: 192.168.0.1

DHCP vlan relay helper address is configured on the following vlan:

vlan Helper address

---------- ----------

VLAN 10 192.168.0.59

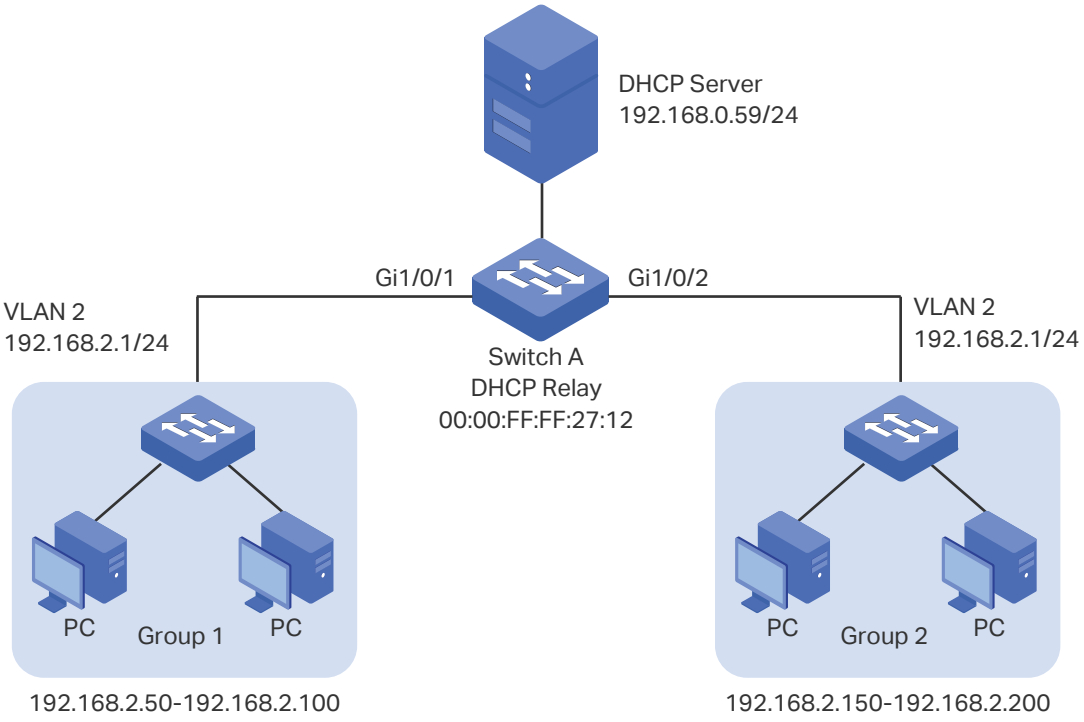
VLAN 20 192.168.0.59

5.4 Example for Option 82 in DHCP Relay

5.4.1 Network Requirements

As the following figure shows, there are two groups of computers. Group 1 is connected to Switch A via port 1/0/1, and Group 2 is connected via port 1/0/2. All computers are in the same VLAN, but the computers and the DHCP server are in different subnets. For management convenience, the administrator wants to allocate separate address spaces for the two groups of computers.

Figure 5-28 Network Topology for Option 82 in DHCP Relay



5.4.2 Configuration Scheme

To meet the requirements, you can configure Option 82 in DHCP Relay on Switch A. With DHCP Relay enabled, the switch can forward DHCP requests and replies between clients and the server. With Option 82 enabled, Switch A informs the DHCP server of the group information of each computer, so that the DHCP server can assign IP addresses of different address pools to the computers in different groups.

The overview of the configurations are as follows:

1) Configuring Switch A

   a. Configure 802.1Q VLAN. Add all computers to VLAN 2. For details, refer to Configuring 802.1Q VLAN.

   b. Configure the interface address of VLAN 2. For details, refer to Configuring Layer 3 Interfaces.

   c. Configure DHCP relay and enable Option 82 in DHCP Relay. In this example, both DHCP Interface Relay and DHCP VLAN Relay can implement the requirements. Demonstrated with T1600G-28TS, 5.4.3 Configuring the DHCP Relay Switch provides configuration procedures to configure DHCP Interface Relay in two ways: using the GUI and using the CLI.

2) Configuring the DHCP Server

   The detailed configurations on the DHCP server may be different among different devices. You can refer to the related document that is for the DHCP server you use. Demonstrated with a Linux ISC DHCP Server, 5.4.4 Configuring the DHCP Server provides information about how to set its DHCP configuration file.

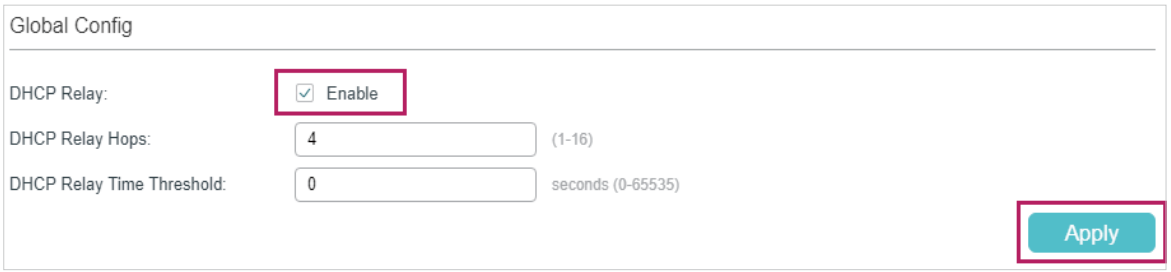
5.4.3 Configuring the DHCP Relay Switch

Using the GUI

Follow these steps to configure DHCP relay and enable Option 82 in DHCP Relay on Switch A:

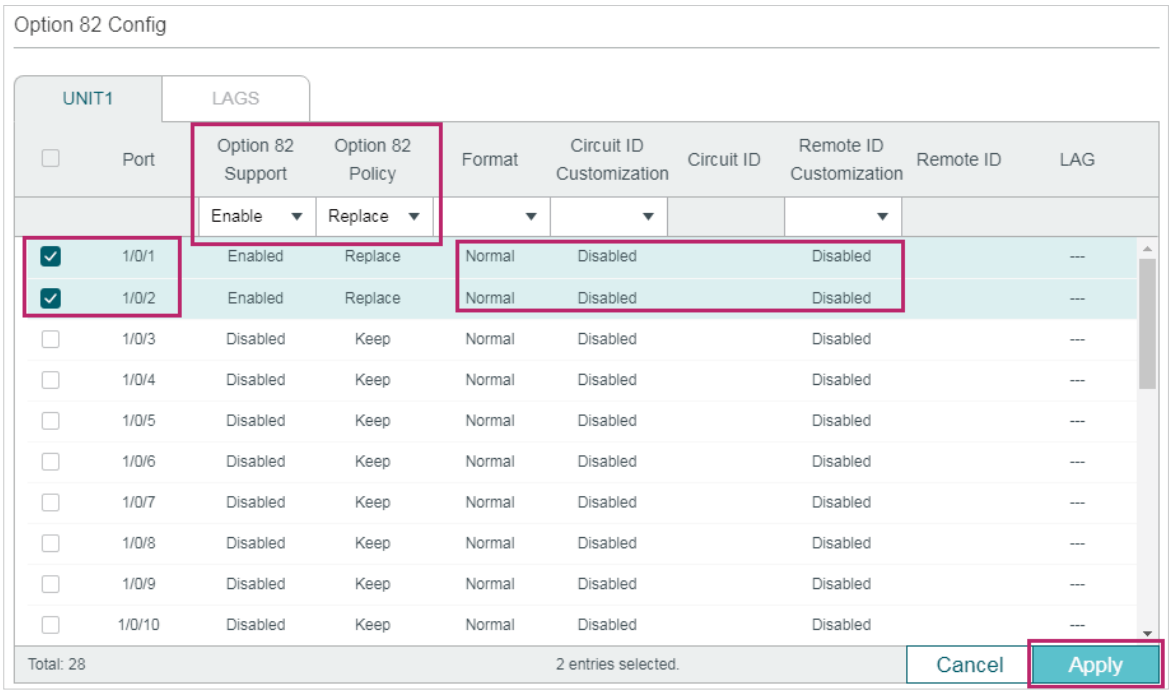
1) Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Relay Config** to load the following page. In the **Global Config** section, enable DHCP Relay, and click **Apply**.

Figure 5-29 Enable DHCP Relay



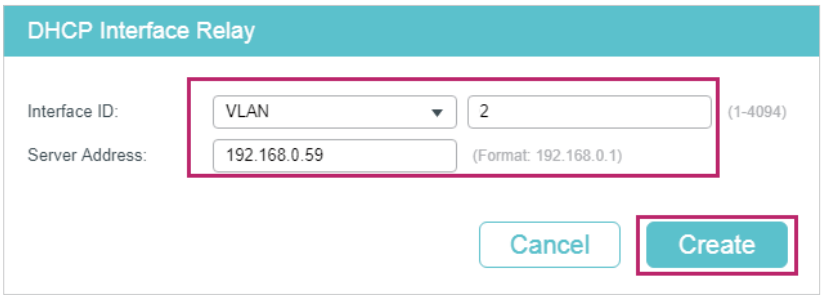
2) In the **Option 82 Config** section, select port 1/0/1 and port 1/0/2, enable Option 82 Support and set Option 82 Policy as Replace. You can configure other parameters according to your needs. In this example, the Format is set as Normal, and Circuit ID Customization and Remote ID Customization as Disabled. Click **Apply**.

Figure 5-30 Configure Option 82



3) Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Interface Relay** and click Add to load the following page. Specify the DHCP server address to assign IP addresses for clients in VLAN 2. Click **Create**.

Figure 5-31 Specify DHCP Server for Interface VLAN 2



4) Click Save to save the settings.

Using the CLI

Follow these steps to configure DHCP relay and enable Option 82 in DHCP Relay on Switch A:

1) Enable DHCP Relay.

Switch#configure

Switch(config)#service dhcp relay

2) Enable Option 82 for port 1/0/1 and port 1/0/2. Set Option 82 policy as **Replace**. You can configure other parameters according to your needs. In this example, the Format is set as Normal, and Circuit ID Customization and Remote ID Customization as Disabled.

Switch#(config)#interface range gigabitEthernet 1/0/1-2

Switch(config-if)#ip dhcp relay information option

Switch(config-if)#ip dhcp relay information strategy replace

Switch(config-if)#ip dhcp relay information format normal

Switch(config-if)#exit

3) Specify the DHCP server for the interface VLAN 2.

Switch(config)#interface vlan 2

Switch(config-if)#ip helper-address 192.168.0.59

Switch(config-if)#end

Switch#copy running-config startup-config

4) Verify the Configurations

View global settings:

Switch#show ip dhcp relay

DHCP relay state: enabled

...

DHCP relay helper address is configured on the following interfaces:

Interface Helper address

---------- ----------

VLAN2 192.168.0.59

...

View port settings:

Switch#show ip dhcp relay information interface

Interface	Option 82 Status	Operation Strategy	Format	Circuit ID	...
---	---	---	---	---	...
Gi1/0/1	Enable	Replace	Normal	Default:VLAN-PORT	...
Gi1/0/2	Enable	Replace	Normal	Default:VLAN-PORT	...

...

5.4.4 Configuring the DHCP Server

Note:

- Make sure the DHCP server supports Option 82 and more than one DHCP address pool.
- To make sure the DHCP server can reach the computers, you can create static routes or enable dynamic routing protocol like RIP on the DHCP server.
- In this section, we use different notations to distinguish ASCII strings from hexadecimal numbers. An ASCII string is enclosed with quotation marks, such as "123", while a hexadecimal number is divided by colon into parts of two digits, such as **31:32:33**.

On the DHCP server, you need to create two DHCP classes to identify the Option 82 payloads of DHCP request packets from Group 1 and Group 2, respectively.

In this example, the DHCP relay agent uses the default circuit ID and remote ID in TLV format. According to packet formats described in Table 1-1 and Table 1-2, the sub-options of the two groups are as shown in the following table.

Table 5-1 Sub-options of Group1 and Group 2

Group	Sub-option	Type (Hex)	Length (Hex)	Value (Hex)
1	Circuit ID	00	04	00:02:00:01
	Remote ID	00	06	00:00:FF:FF:27:12

Group	Sub-option	Type (Hex)	Length (Hex)	Value (Hex)
2	Circuit ID	00	04	00:02:00:02
	Remote ID	00	06	00:00:FF:FF:27:12

The configuration file **/etc/dhcpd.conf** of the Linux ISC DHCP Server is:

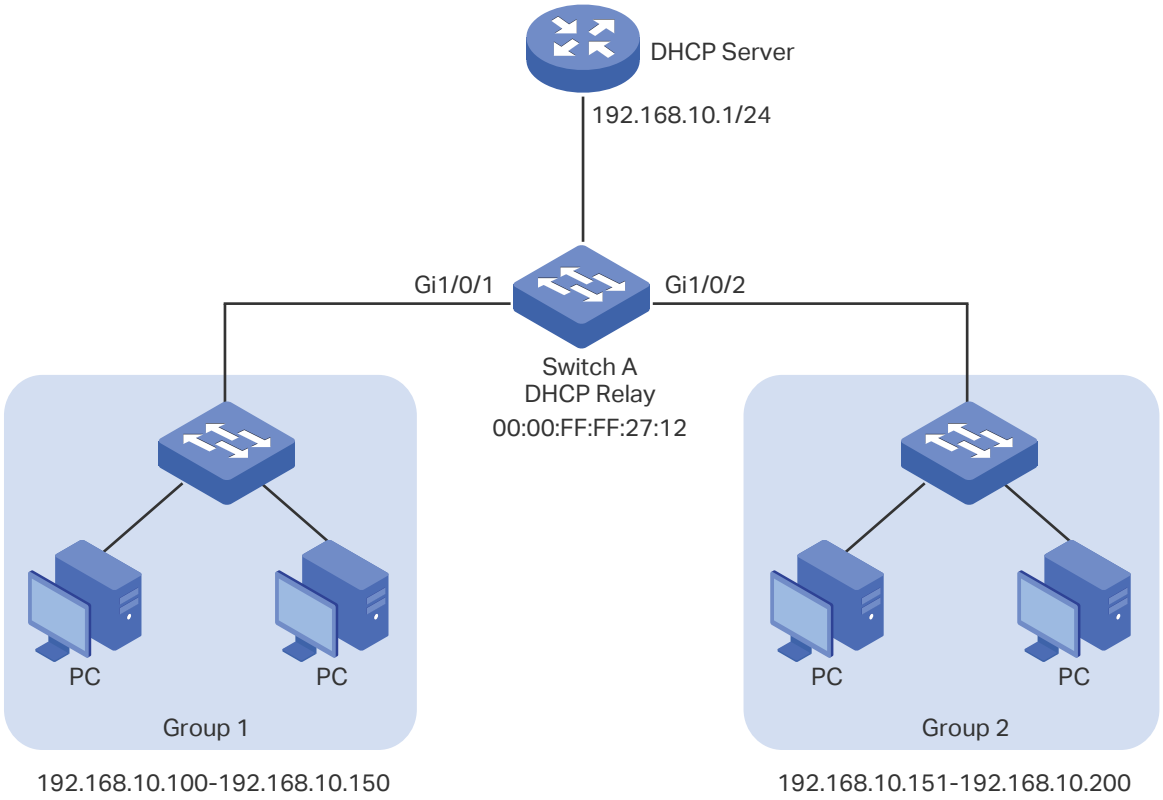
```
ddns-update-style interim;
ignore client-updates;

# Create two classes to match the pattern of Option 82 in DHCP request packets from
# Group 1 and Group 2, respectively.
# The agent circuit ID inserted by the DHCP relay switch is 6 bytes long in TLV format, one
# byte for Type, one byte for Length, and 4 bytes for Value. Therefore, the offset is 2 and the
length is 4.
# Similarly, the offset of the agent remote ID is 2 and the length is 6.
class “VLAN2Port1“ {
   match if substring (option agent.circuit-id, 2, 4) = 00:02:00:01
            and substring (option agent.remote-id, 2, 6) = 00:00:ff:ff:27:12;
}

class “VLAN2Port2“ {
  match if substring (option agent.circuit-id, 2, 4) = 00:02:00:02
            and substring (option agent.remote-id, 2, 6) = 00:00:ff:ff:27:12;
}

# Create two IP Address pools in the same subnet.
# Assign different IP addresses to the DHCP clients in different groups.
subnet 192.168.2.0 netmask 255.255.255.0 {
  option routers 192.168.2.1;
  option subnet-mask 255.255.255.0;
  option domain-name-servers 192.168.0.59;
  option domain-name “example.com“;
  default-lease-time 600;
  max-lease-time 7200;
  authoritative;

pool {
  range 192.168.2.50 192.168.2.100;
  allow members of “VLAN2Port1“;
}

pool {
  range 192.168.2.150 192.168.2.200;
  allow members of “VLAN2Port2“;
}
```

5.5 Example for DHCP L2 Relay

5.5.1 Network Requirements

As the following figure shows, two groups of computers are connected to Switch A, and Switch A is connected to the DHCP server. All devices on the network are in the default VLAN 1. All computers get dynamic IP addresses from the DHCP server. For management convenience, the administrator wants to allocate separate address spaces for the two groups of computers.

Figure 5-32 Network Topology for DHCP L2 Relay



5.5.2 Configuration Scheme

To meet the requirements, you can configure DHCP L2 Relay on Switch A to inform the DHCP server of the group information of each PC, so that the DHCP server can assign IP addresses of different address pools to the PCs in different groups.

The overview of the configurations are as follows:

1) Configuring Switch A

   a. Enable DHCP L2 Relay globally and on VLAN 1.

   b. Configure Option 82 on ports 1/0/1 and 1/0/2.

   Demonstrated with T1600G-28TS, 5.5.3 Configuring the DHCP Relay Switch provides configuration procedures in two ways: using the GUI and using the CLI.

2) Configuring the DHCP Server

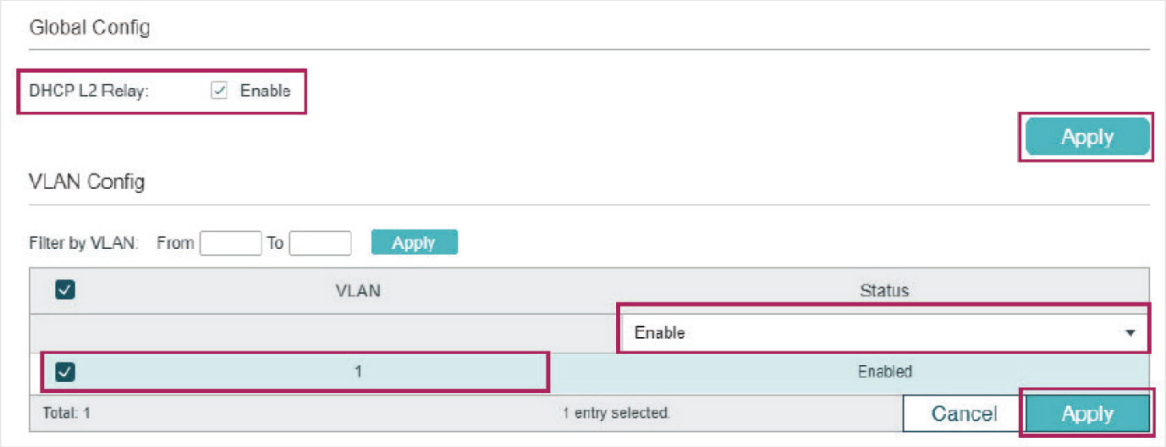
The detailed configurations on the DHCP server may be different among different devices. You can refer to the related document that is for the DHCP server you use. Demonstrated with a Linux ISC DHCP Server, 5.5.4 Configuring the DHCP Server provides information about how to set its DHCP configuration file.

5.5.3 Configuring the DHCP Relay Switch

Using the GUI

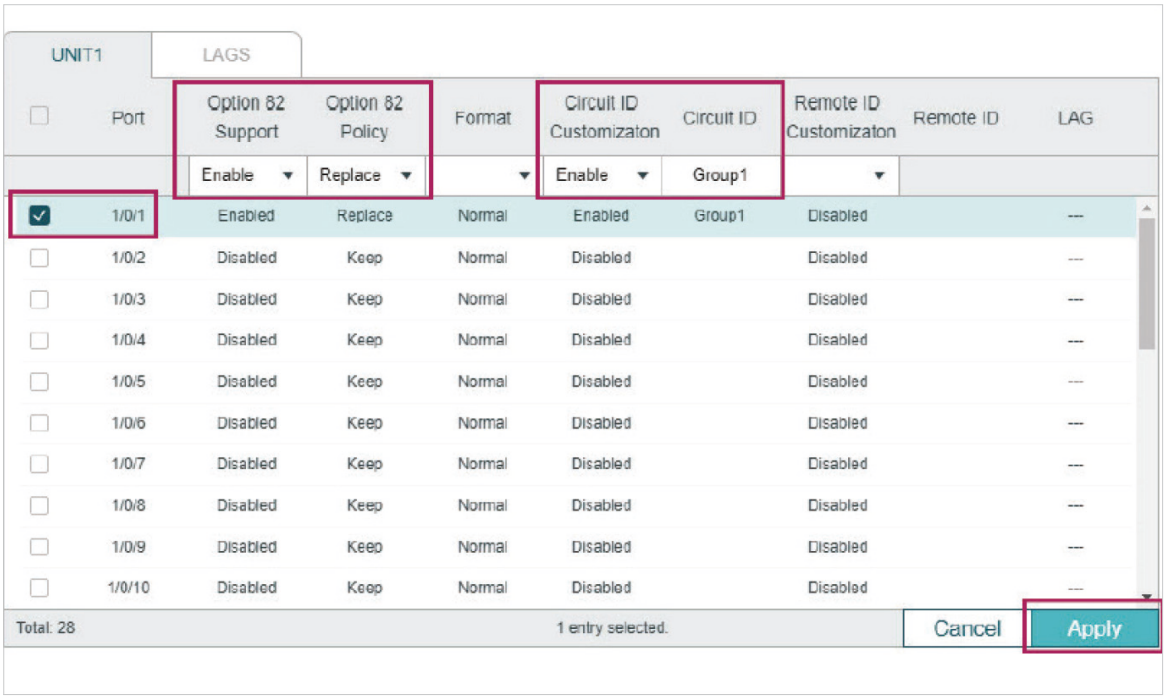
1) Choose the menu **L3 FEATURES** > **DHCP Service** > **DHCP L2 Relay** > **Global Config** to load the following page. In the **Global Config** section, enable DHCP L2 Relay globally and click **Apply**. Enable DHCP L2 Relay on VLAN 1 and click **Apply**.

Figure 5-33 Enabling DHCP L2 Relay



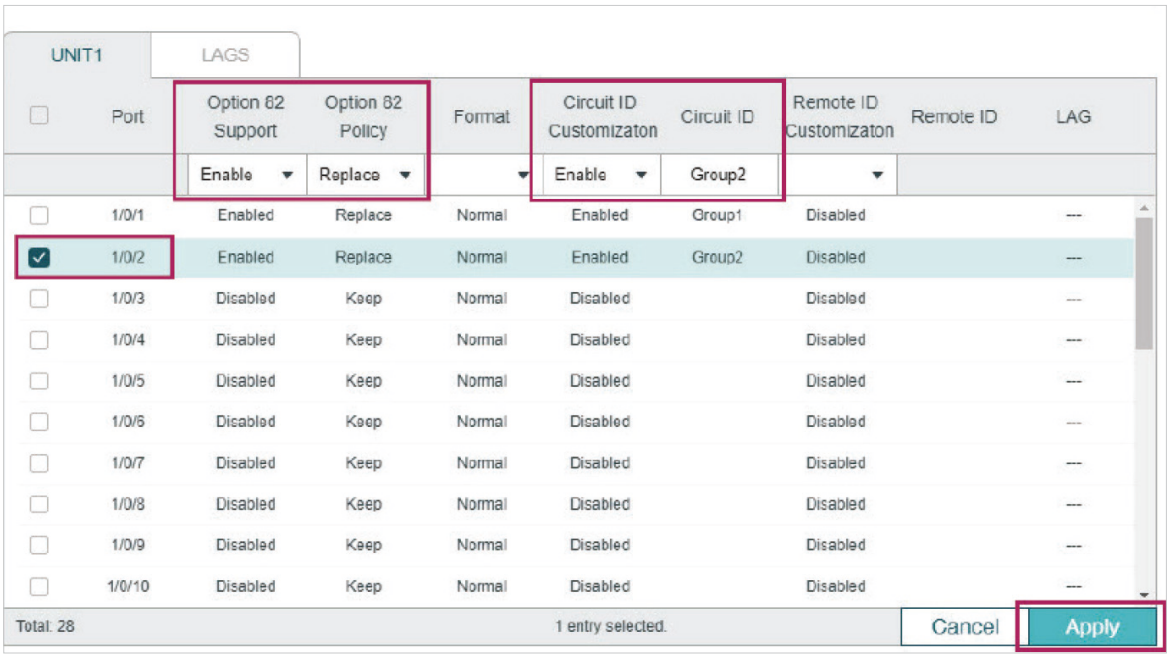
2) Choose the menu **L3 FEATURES** > **DHCP Service** > **DHCP L2 Relay** > **Port Config** to load the following page. Select port 1/0/1, enable Option 82 Support and select Option 82 Policy as Replace. You can configure other parameters according to your needs. In this example, keep Format as Normal and Remote ID Customization as Disabled. Enable Circuit ID Customization and specify the Circuit ID as Group1. Click **Apply**.

Figure 5-34 Configuring Port 1/0/1



3) On the same page, select port 1/0/2, enable Option 82 Support and select Option 82 Policy as Replace. You can configure other parameters according to your needs. In this example, keep Format as Normal and Remote ID Customization as Disabled. Enable Circuit ID Customization and specify the Circuit ID as Group2. Click **Apply**.

Figure 5-35 Configuring Port 1/0/2



4) Click Save to save the settings.

Using the CLI

1) Enable DHCP L2 Relay globally and on VLAN1.

Switch#configure

Switch(config)#ip dhcp l2relay

Switch(config)#ip dhcp l2relay vlan 1

2) On port 1/0/1, enable Option 82 and select Option 82 Policy as Replace. You can configure other parameters according to your needs. In this example, keep Format as Normal and Remote ID Customization as Disabled. Enable Circuit ID Customization and specify the Circuit ID as Group1.

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip dhcp l2relay information option

Switch(config-if)#ip dhcp l2relay information strategy replace

Switch(config-if)#ip dhcp l2relay information circuit-id Group1

Switch(config-if)#exit

3) On port 1/0/2, enable Option 82 and select Option 82 Policy as Replace. You can configure other parameters according to your needs. In this example, keep Format as Normal and Remote ID Customization as Disabled. Enable Circuit ID Customization and specify the Circuit ID as Group2.

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ip dhcp l2relay information

Switch(config-if)#ip dhcp l2relay information strategy replace

Switch(config-if)#ip dhcp l2relay information circuit-id Group2

Switch(config-if)#end

Switch#copy running-config startup-config

Verify the Configurations

View global settings:

Switch#show ip dhcp l2relay

Global Status: Enable

VLAN ID: 1

View port settings:

Switch#show ip dhcp l2relay information interface gigabitEthernet 1/0/1

Interface	Option 82 Status	Operation Strategy	Format	Circuit ID	...
---	---	---	---	---	---
Gi1/0/1	Enable	Replace	Normal	Group1	...

```
Switch#show ip dhcp l2relay information interface gigabitEthernet 1/0/1
Interface Option 82 Status   Operation Strategy   Format   Circuit ID   ...
---------  ----------------   ------------------   -------  ---------   ...
Gi1/0/2    Enable             Replace              Normal   Group2      ...
```

5.5.4 Configuring the DHCP Server

Note:

- Make sure the DHCP server supports Option 82 and more than one DHCP address pool.
- To make sure the DHCP server can reach the computers, you can create static routes or enable dynamic routing protocol like RIP on the DHCP server.
- In this section, we use different notations to distinguish ASCII strings from hexadecimal numbers. An ASCII string is enclosed with quotation marks, such as "123", while a hexadecimal number is divided by colon into parts of two digits, such as **31:32:33**.

On the DHCP server, you need to create two DHCP classes to identify the Option 82 payloads of DHCP request packets from Group 1 and Group 2, respectively.

In this example, the DHCP relay agent uses the customized circuit ID and default remote ID in TLV format. According to packet format described in Table 1-1 and Table 1-2, the sub-options of the two groups are as shown in the following table.

Table 5-2 Sub-options of Group1 and Group 2

Group	Sub-option	Type (Hex)	Length (Hex)	Value
1	Circuit ID	00	06	"Group1" as an ASCII string (or **47:72:6F:75:70:31** in hexadecimal)
	Remote ID	00	06	00:00:FF:FF:27:12
2	Circuit ID	00	06	"Group2" as an ASCII string (or **47:72:6F:75:70:32** in hexadecimal)
	Remote ID	00	06	00:00:FF:FF:27:12

The configuration file **/etc/dhcpd.conf** of the Linux ISC DHCP Server is:

```
ddns-update-style interim;
ignore client-updates;

# Create two classes to match the pattern of Option 82 in DHCP request packets from
# Group 1 and Group 2, respectively.
# The agent circuit ID inserted by the DHCP relay switch is 8 byte long in TLV format, one
# byte for Type, one byte for Length, and 6 bytes for Value. Therefore, the offset is 2 and the
length is 6.
```

```
# Similarly, the offset of the agent remote ID is 2 and the length is 6.

class “Group1“ {
   match if substring (option agent.circuit-id, 2, 6) = “Group1”
            and substring (option agent.remote-id, 2, 6) = 00:00:ff:ff:27:12;
}

class “Group2“ {
  match if substring (option agent.circuit-id, 2, 6) = “Group2”
            and substring (option agent.remote-id, 2, 6) = 00:00:ff:ff:27:12;
}

# Create two IP Address pools in the same subnet.
# Assign different IP addresses to the DHCP clients in different groups.
subnet 192.168.10.0 netmask 255.255.255.0 {
  option routers 192.168.10.1;
  option subnet-mask 255.255.255.0;
  option domain-name-servers 192.168.10.1;
  option domain-name “example.com“;
  default-lease-time 600;
  max-lease-time 7200;
  authoritative;

pool {
  range 192.168.10.100 192.168.10.150;
  allow members of “Group1“;
}

pool {
  range 192.168.10.151 192.168.10.200;
  allow members of “Group2“;
}
```

6 Appendix: Default Parameters

Default settings of DHCP Server are listed in the following table.

Table 6-1 Default Settings of DHCP Server

Parameter	Default Setting
Global Config	
DHCP Server	Disabled
Option 60	None
Option 138	None
Ping Time Config	
Ping Packets	1
Ping Timeout	100 ms
Excluded IP Address	
Start IP Address	None
End IP Address	None
Pool Setting	
Pool Name	None
Network Address	None
Subnet Mask	None
Lease Time	120 min
Default Gateway	None
DNS Server	None
NetBIOS Server	None
NetBIOS Node Type	None
Next Server Address	None
Domain Name	None
Bootfile	None

Parameter	Default Setting
Manual Binding	
Pool Name	None
IP Address	None
Binding Mode	Client ID
Client Id	None
Hardware Address	None
Hardware Type	Ethernet

Default settings of DHCP Relay are listed in the following table.

Table 6-2 Default Settings of DHCP Relay

Parameter	Default Setting
DHCP Relay	
DHCP Relay	Disabled
DHCP Relay Hops	4
DHCP Relay Time Threshold	0
Option 82 Configuration	
Option 82 Support	Disabled
Option 82 Policy	Keep
Format	Normal
Circuit ID Customization	Disabled
Circuit ID	None
Remote ID Customization	Disabled
Remote ID	None
DHCP Interface Relay	
Interface ID	None
Server Address	None

Parameter	Default Setting
DHCP VLAN Relay	
Interface ID	None
VLAN ID	None
Server Address	None

Default settings of DHCP L2 Relay are listed in the following table.

Table 6-3 Default Settings of DHCP L2 Relay

Parameter	Default Setting
Global Config	
DHCP Relay	Disabled
VLAN Status	Disabled
Port Config	
Option 82 Support	Disabled
Option 82 Policy	Keep
Format	Normal
Circuit ID Customization	Disabled
Circuit ID	None
Remote ID Customization	Disabled
Remote ID	None

Part 21

Configuring ARP

CHAPTERS

1. Overview
2. ARP Configurations
3. Appendix: Default Parameters

1 Overview

ARP (Address Resolution Protocol) is used to map IP addresses to MAC addresses. Taking an IP address as input, ARP learns the associated MAC address, and stores the IP-MAC address association in an ARP entry for rapid retrieval.

1.1 Supported Features

ARP Table

The ARP table displays all the ARP entries, including dynamic entries and static entries.

Dynamic Entry: Automatically learned and will be deleted after aging time.

Static Entry: Added manually and will be remained unless modified or deleted manually.

Static ARP

You can manually add ARP entries by specifying the IP addresses and MAC addresses.

Gratuitous ARP

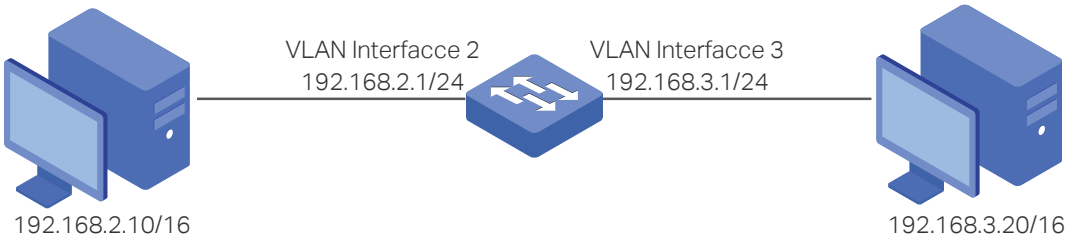
Gratuitous ARP is a special kind of ARP. Both the source and destination addresses of the gratuitous ARP packet are the sender its own IP address. It is used to detect duplicate IP address. If an interface sends a gratuitous ARP packet and no replies are received, then the sender knows its IP address is not used by other devices.

Proxy ARP

Normally, the ARP packets can only be transmitted in one broadcast domain, which means if two devices in the same network segment are connected to different Layer 3 interfaces, they cannot communicate with each other because they cannot learn each other's MAC address using ARP packets.

Proxy ARP solves this problem. As shown below, when a host sends an ARP request to another device that is not in the same broadcast domain but on the same network segment, the Layer 3 interface with Proxy ARP enabled will respond the ARP request with its own MAC address if the destination IP is reachable. After that, the ARP request sender sends packets to the switch, and the switch forwards the packets to the intended device.

Figure 1-1 Proxy ARP Application

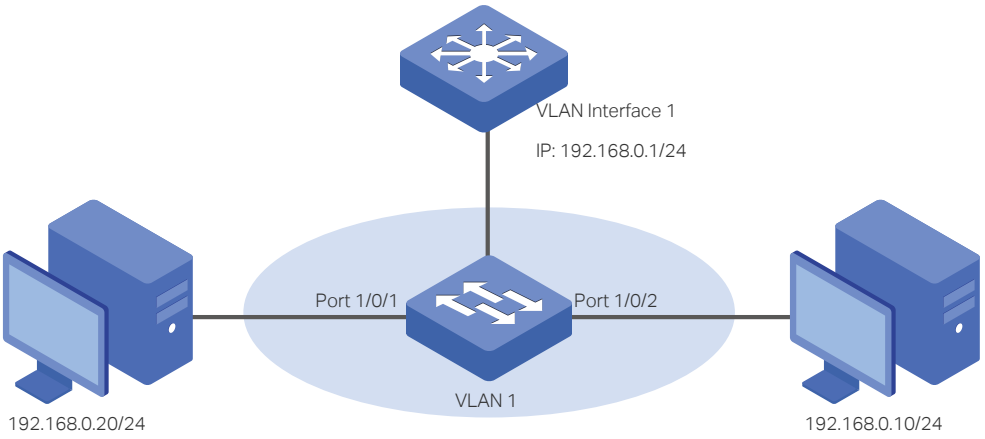


Local Proxy ARP

Local Proxy ARP is similar with Proxy ARP. As shown below, two hosts are in the same VLAN and connected to VLAN interface 1, but port 1/0/1 and port 1/0/2 are isolated on Layer 2. In this case, both of the hosts cannot receive each other's ARP request. So they cannot communicate with each other because they cannot learn each other's MAC address using ARP packets.

To solve this problem, you can enable Local Proxy ARP on the Layer 3 interface and the interface will respond the ARP request sender with its own MAC address. After that, the ARP request sender sends packets to the Layer 3 interface, and the interface forwards the packets to the intended device.

Figure 1-2 Local Proxy ARP Application



2 ARP Configurations

With ARP configurations, you can:

- View dynamic and static ARP entries.
- Add or delete static ARP entries.

To configure the Gratuitous ARP feature:

- Configure the Gratuitous ARP globally and set the Gratuitous ARP sending interval

To configure the Proxy ARP feature:

- Enable Proxy function for VLAN interfaces or routed ports.

To configure the Local Proxy ARP feature:

- Enable Local Proxy function for VLAN interfaces or routed ports.

2.1 Using the GUI

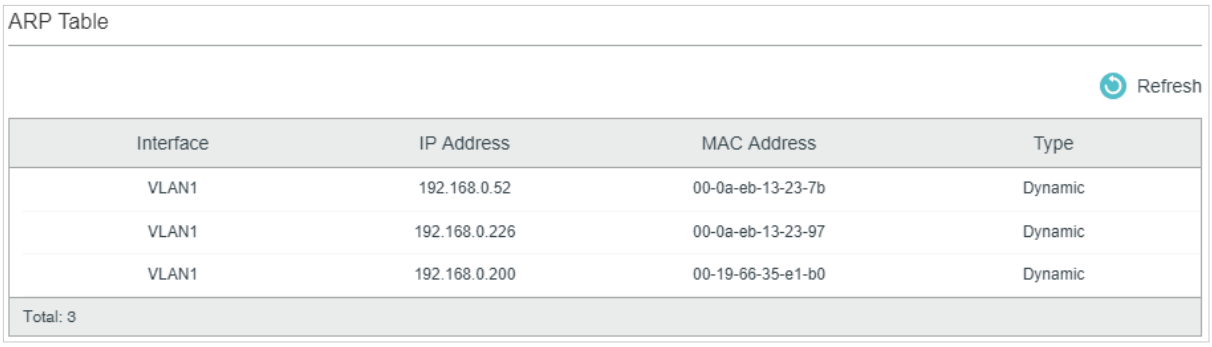
2.1.1 Viewing the ARP Entries

The ARP table consists of two kinds of ARP entries: dynamic and static.

- Dynamic Entry: Automatically learned and will be deleted after aging time.
- Static Entry: Added manually and will be remained unless modified or deleted manually.

Choose the menu **L3 FEATURES > ARP > ARP Table > ARP Table** to load the following page.

Figure 2-1 Viewing the ARP Entries



Interface	Displays the network interface of an ARP entry.
IP Address	Displays the IP address of an ARP entry.
MAC Address	Displays the MAC address of an ARP entry.

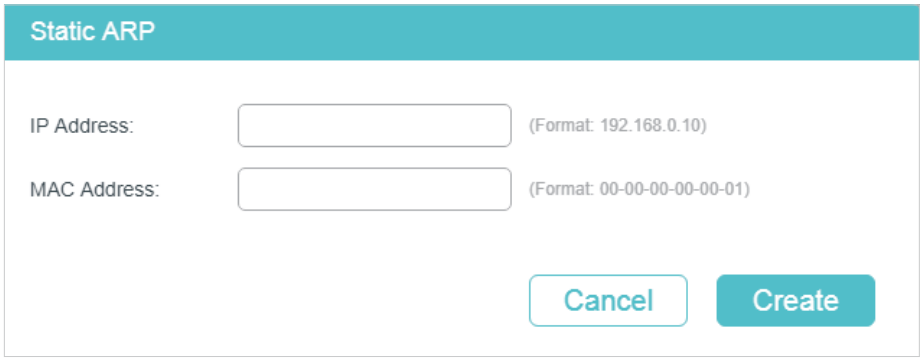
Type	Displays the type of an ARP entry. **Static**: The entry is added manually and will always remain the same. **Dynamic**: The entry that will be deleted after the aging time leased. The default aging time value is 600 seconds. If you want to change the aging time, you can use the CLI to configure it.

2.1.2 Adding Static ARP Entries Manually

You can add desired static ARP entries by mannually specifying the IP addresses and MAC addresses.

Choose the menu **L3 FEATURES > ARP > Static ARP** and click Add to load the following page.

Figure 2-2 Adding Static ARP Entries



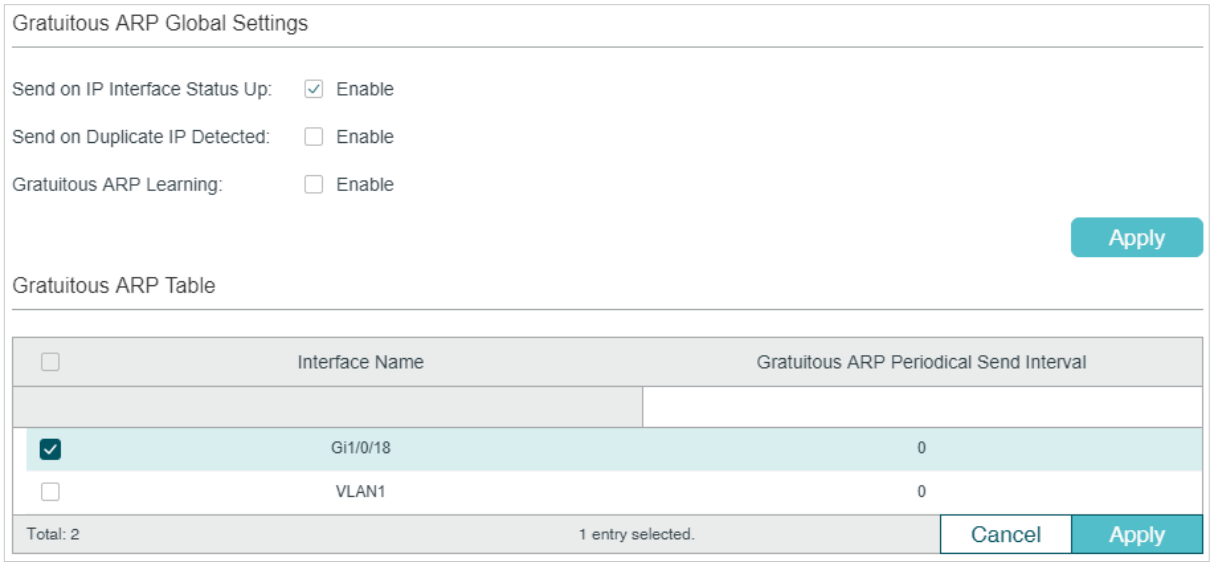
Enter the IP address and MAC address, then click **Create**.

IP address	Specify the IP address of the static ARP entry.
MAC address	Specify the MAC address.of the static ARP entry.

2.1.3 Configuring Gratuitous ARP

Choose the menu **L3 FEATURES > ARP > Gratuitous ARP** to load the following page.

Figure 2-3 Configuring Gratuitous ARP



Follow these steps to configure the Gratuitous feature for the interface.

1) In the **Gratuitous ARP Global Settings** section, configure the global parameters for gratuitous ARP. Then click **Apply**.

Send on IP Interface Status Up	With this option enabled, the interface will send gratuitous ARP request packets when its status becomes up. This is used to announce the interface's IP address to the other hosts. It is enabled by default.
Send on Duplicate IP Detected	With this option enabled, the interface will send gratuitous ARP request packets when a gratuitous ARP request packet is received for which the IP address is the same as the interface's. In this case, the switch knows that another host is using the same IP address as its own. To claim the IP address for the correct owner, the interface sends gratuitous ARP packets. It is disabled by default.
Gratuitous ARP Learning	Normally, the switch only updates the MAC address table by learning from the ARP reply packet or normal ARP request packet. With this option enabled, the switch will also update the MAC address table by learning from the received gratuitous ARP packets. It is disabled by default.

2) In the **Gratuitous ARP Table** section, configure the interval of sending gratuitous ARP request packets for the interface. Then click **Apply**.

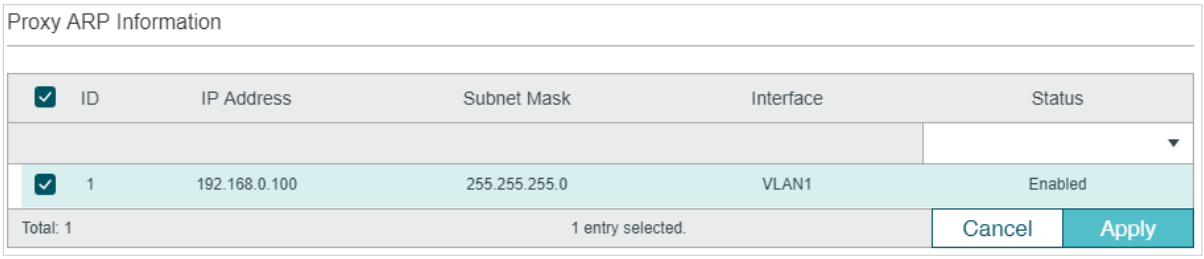
Interface Name	Displays the Interface ID of the Layer 3 interface.
Gratuitous ARP Periodical Send Interval	Enter the interval of sending gratuitous ARP request packets for the interface. A value of 0 means the interface will not send gratuitous ARP request packets periodically.

2.1.4 Configuring Proxy ARP

Proxy ARP is used in the situation that two devices are in the same network segment but connected to different Layer 3 interfaces.

Choose the menu **L3 FEATURES> ARP > Proxy ARP > Proxy ARP** to load the following page.

Figure 2-4 Configuring Proxy ARP



Select the desired interface and enable proxy ARP. Then click **Apply**.

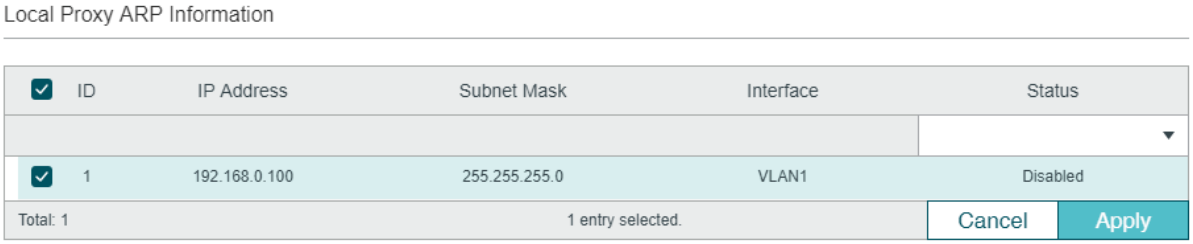
IP Address	Displays the IP address of the Layer 3 interface
Subnet Mask	Displays the subnet mask of the IP address.
Status	Enable proxy ARP feature on the interface. The interface will respond the ARP request sender with its own MAC address.

2.1.5 Configuring Local Proxy ARP

Local Proxy ARP is used in the situation that two devices are in the same VLAN but isolated on the layer 2 ports.

Choose the menu **L3 FEATURES > ARP > Proxy ARP > Local Proxy ARP** to load the following page.

Figure 2-5 Configuring Local Proxy ARP



Select the desired interface and enable local proxy ARP. Then click **Apply**.

IP Address	Displays the IP address of the Layer 3 interface
Subnet Mask	Displays the subnet mask of the IP address.
Status	Enable local proxy ARP feature on the interface. The interface will respond the ARP request sender with its own MAC address.

2.2 Using the CLI

2.2.1 Configuring the ARP Entry

■ Adding Static ARP Entries

Follow these steps to add static ARP entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**arp** *ip mac type* Add a static ARP entry. *ip*: Enter the IP address of the static ARP entry. *mac:* Enter the MAC address of the static ARP entry. *type:* Enter the ARP type. Configure it as 'arpa'.
Step 3	**show arp** [*ip*] [*mac*] *ip*: Specify the IP address of your desired ARP entry. *mac:* Specify the MAC address of your desired ARP entry.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to create a static ARP entry with the IP as 192.168.0.1 and the MAC as 00:11:22:33:44:55:

Switch#configure

Switch(config)#arp 192.168.0.1 00:11:22:33:44:55 **arpa**

Switch(config)#show arp 192.168.0.1

Interface	Address	Hardware Addr	Type
Vlan1	192.168.0.1	00:11:22:33:44:55	STATIC

Switch(config)#end

Switch#copy running-config startup-config

■ Configuring the Aging Time of Dynamic ARP Entries

Follow these steps to configure the aging time of dynamic ARP entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**arp timeout** *timeout* Configure the ARP aging time of the VLAN interface or routed port . *timeout*: Specify the value of aging time, which ranges from 1 to 3000 in seconds. The default value is 1200 seconds.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to configure the aging time of dynamic ARP entries as 1000 seconds:

Switch#configure

Switch(config)#arp timeout 1000

Switch(config)#end

Switch#copy running-config startup-config

■ Clearing Dynamic Entries

Step 1	**configure** Enter global configuration mode.
Step 2	**clear arp-cache** Clear all the dynamic ARP entries.
Step 3	**copy running-config startup-config** Save the settings in the configuration file.

■ Renewing Dynamic ARP Entries Automatically

Step 1	**configure** Enter global configuration mode.
Step 2	**arp dunamicrenew** Enable the switch to automatically renew dynamic ARP entries. By default, it is enabled..
Step 3	**copy running-config startup-config** Save the settings in the configuration file.

■ Viewing ARP Entries

On privileged EXEC mode or any other configuration mode, you can use the following command to view ARP entries:

show arp [*ip*] [*mac*]

ip: Specify the IP address of your desired ARP entry.

mac: Specify the MAC address of your desired ARP entry.

show ip arp { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *lagid* **| vlan** *vid* **}**

Verify the active ARP entries associated with a Layer 3 interface.

port: Specify the number of the routed port.

lagid: Specify the ID of the LAG.

vid: Specify the VLAN interface ID.

2.2.2 Configuring the Gratuitous ARP

■ Configuring Gratuitous ARP Globally

Follow these steps to add static ARP entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**gratuitous-arp intf-status-up enable** Enable the Layer 3 interface to send a gratuitous ARP packet to detect if its IP address is used by other devices. It is enabled by default
Step 3	**gratuitous-arp dup-ip-detected enable** (Optional) Enable the Layer 3 interface to send a gratuitous packet when the interface received a gratuitous ARP packet with the same IP address with its own. It is disabled by default.
Step 4	**gratuitous-arp learning enable** (Optional) Enable the switch to learn MAC address entries from gratuitous ARP packets. Generally, the switch only learn MAC address entries form normal ARP packets. With this option enabled, the switch will also learn MAC address entries from gratuitous ARP packets. By default, it is disabled.
Step 5	**show gratuitous-arp** Show the gratuitous ARP configuration.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to enable Send on IP Interface Status Up, Send on Duplicate IP Detected and Gratuitous ARP Learning features:

Switch#configure

Switch(config)#gratuitous-arp dup-ip-detected enable

Switch(config)#gratuitous-arp intf-status-up enable

Switch(config)#gratuitous-arp learning enable

Switch(config)#show gratuitous-arp

Send on IP interface Status up : Enabled

Send on Duplicate IP Detected : Enabled

Gratuitous ARP Learning : Enabled

Interface Gratuitous ARP Periodical Send Interval

--- ---

Gi1/0/18 0

VLAN1 0

Switch(config)#end

Switch#copy running-config startup-config

■ Configuring Interval of Sending Gratuitous ARP Packets

Follow these steps to configure gratuitous ARP packets for Layer 3 interfaces:

Step 1	**configure** Enter global configuration mode.
Step 2	There are three types of Layer 3 interface that are able to send gratuitous ARP packets: routed port, port-channel and VLAN interface. **interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** **no switch port** Enter interface configuration mode and change the port or port-channel to be a Layer 3 interface.
	Interface vlan *vlan-id* Enter the vlan interface configuration mode. *vlan-id:* Enter the interface VLAN ID.
Step 3	**gratuitous-arp send-interval** *interval* Specify the periodical interval at which the interface sends the gratuitous ARP packet. *interval:* Specify the interval in seconds. The valid value ranges from 0 to 65535. Value 0 means the interface does not periodically send gratuitous ARP packets.

Step 4	**show gratuitous-arp** Show the gratuitous ARP configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to configure the interval of sending gratuitous ARP packets for VLAN interface 1 as 10 seconds:

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#gratuitous-arp send-interval 10

Switch(config-if)#show gratuitous-arp

...

Interface Gratuitous ARP Periodical Send Interval

--- ---

VLAN1 10

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Configuring Proxy ARP

You can configure proxy ARP and local proxy ARP.

- Configuring Proxy ARP

Follow these steps to Proxy ARP on the VLAN interface, routed port or port channel.

Step 1	**configure** Enter global configuration mode.

Step 2	There are three types of Layer 3 interface can be enabled with Proxy ARP: routed port, port-channel and VLAN interface. **interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** **no switch port** Enter interface configuration mode and change the port or port-channel to be a Layer 3 interface.
	Interface vlan *vlan-id* Enter the vlan interface configuration mode. *vlan-id:* Enter the interface VLAN ID.
Step 3	**ip proxy-arp** Enable Proxy ARP function on the specified Layer 3 interface..
Step 4	**show ip proxy-arp** Show the Proxy ARP configuration..
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to enable Proxy ARP function for VLAN interface 1:

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ip proxy-arp

Switch(config-if)#show ip proxy-arp

Interface	IP Address	IP Mask	Status
---	---	---	---
vlan 1	192.168.0.1	255.255.255.0	Enabled

Switch(config-if)#end

Switch#copy running-config startup-config

Configuring Local Proxy ARP

Follow these steps to Local Proxy ARP on the VLAN interface, routed port or port channel.

Step 1	**configure** Enter global configuration mode.

Step 2	There are three types of Layer 3 interface can be enabled with Local Proxy ARP: routed port, port-channel and VLAN interface. **interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** **no switch port** Enter interface configuration mode and change the port or port-channel to be a Layer 3 interface.
	Interface vlan *vlan-id* Enter the vlan interface configuration mode. *vlan-id:* Enter the interface VLAN ID.
Step 3	**ip local-proxy-arp** Enable Local Proxy ARP function on the specified Layer 3 interface..
Step 4	**show ip local-proxy-arp** Show the Local Proxy ARP configuration..
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to enable Local Proxy ARP function for VLAN interface 1:

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ip local-proxy-arp

Switch(config-if)#show ip local-proxy-arp

Interface	IP Address	IP Mask	Status
---	---	---	---
vlan 1	192.168.0.1	255.255.255.0	Enabled

Switch(config-if)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

Default ARP settings are listed in the following tables.

Table 3-1 Default Gratuitous Settings

Parameter	Default Setting
Send on IP Interface Status Up	Enabled
Send on Duplicate IP Detected	Disabled
Gratuitous ARP Learning	Disabled
Gratuitous ARP Periodical Send Interval	0 second

Part 22

Configuring QoS

CHAPTERS

1. QoS
2. Class of Service Configuration
3. Bandwidth Control Configuration
4. Voice VLAN Configuration
5. Auto VoIP Configuration
6. Configuration Examples
7. Appendix: Default Parameters

1 QoS

1.1 Overview

With network scale expanding and applications developing, internet traffic is dramatically increased, thus resulting in network congestion, packet drops and long transmission delay. Typically, networks treat all traffic equally on FIFO (First In First Out) delivery basis, but nowadays many special applications like VoD, video conferences, VoIP, etc, require more bandwidth or shorter transmission delay to guarantee the performance.

With QoS (Quality of Service) technology, you can classify and prioritize network traffic to provide differentiated services to certain types of traffic.

1.2 Supported Features

You can configure the class of service, bandwidth control, Voice VLAN and Auto VoIP features on the switch to maximize the network performance and bandwidth utilization.

Class of Service

The switch classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduler settings to implement QoS function.

- Priority Mode: Three modes are supported, Port Priority, 802.1p Priority and DSCP Priority.
- Scheduler Mode: Two scheduler types are supported, Strict and Weighted.

Bandwidth Control

Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance.

- Rate limit functions to limit the ingress/egress traffic rate on each port. In this way, the network bandwidth can be reasonably distributed and utilized.
- Storm Control function allows the switch to monitor broadcast packets, multicast packets and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the packets exceeds the set rate, the packets will be automatically discarded to avoid network broadcast storm.

Voice VLAN and Auto VoIP

The voice VLAN and Auto VoIP features are used to prioritize the transmission of voice traffic. Voice traffic is typically more time-sensitive than data traffic, and the voice quality

can deteriorate a lot because of packet loss and delay. To ensure the high voice quality, you can configure Voice VLAN or Auto VoIP.

These two features can be enabled on the ports that transmit voice traffic only or transmit both voice traffic and data traffic. Voice VLAN can change the voice packets' 802.1p priority and transmit the packets in desired VLAN. Auto VoIP can inform the voice devices of send the packets with specific configuration by working with the LLDP-MED feature.

2 Class of Service Configuration

With class of service configurations, you can:

- Configure port priority
- Configure 802.1p priority
- Configure DSCP priority
- Specify the scheduler settings

Configuration Guidelines

- Select the priority mode that the ports trust according to your network requirements.

  A port can use only one priority to classify the ingress packets. Three priority modes are supported on the switch: Port Priority, 802.1P Priority and DSCP Priority.

  - Port Priority

  In this mode, the switch prioritizes packets according to their ingress ports, regardless of the packet field or type.

  - 802.1P Priority

  802.1P defines the first three bits in 802.1Q Tag as PRI field. The PRI values are from 0 to 7. 802.1P priority determines the priority of packets based on the PRI value.

  In this mode, the switch only prioritizes packets with VLAN tag, regardless of the IP header of the packets.

  - DSCP Priority

  DSCP priority determines the priority of packets based on the ToS (Type of Service) field in their IP header. RFC2474 re-defines the ToS field in the IP packet header as DS field. The first six bits (bit 0-bit 5) of the DS field is used to represent DSCP priority. The DSCP values are from 0 to 63.

  In this mode, the switch only prioritizes IP packets.

- Specify the 802.1p to queue mapping according to your needs.

  For 802.1p Priority, the packets will be forwarded according to the 802.1p to queue mapping directly.

  For Port Priority and DSCP Priority, the port priority and DSCP priority will first be mapped to the 802.1p priority, and then mapped to the queue according to the 802.1p to queue mapping.

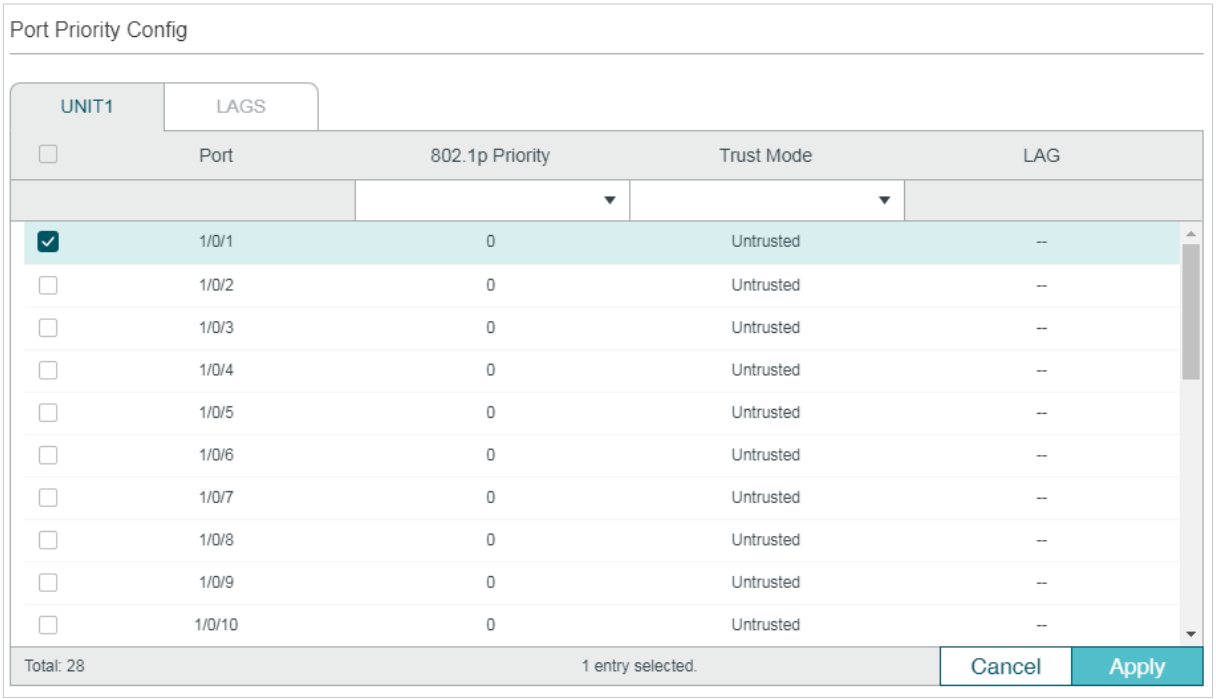
2.1 Using the GUI

2.1.1 Configuring Port Priority

■ Configuring the Trust Mode and Port to 802.1p Mapping

Choose the menu **QoS > Class of Service > Port Priority** to load the following page.

Figure 2-1 Configuring the Trust Mode and Port to 802.1p Mapping



Follow these steps to configure the parameters of the port priority:

1) Select the desired ports, specify the 802.1p priority and set the trust mode as Untrusted.

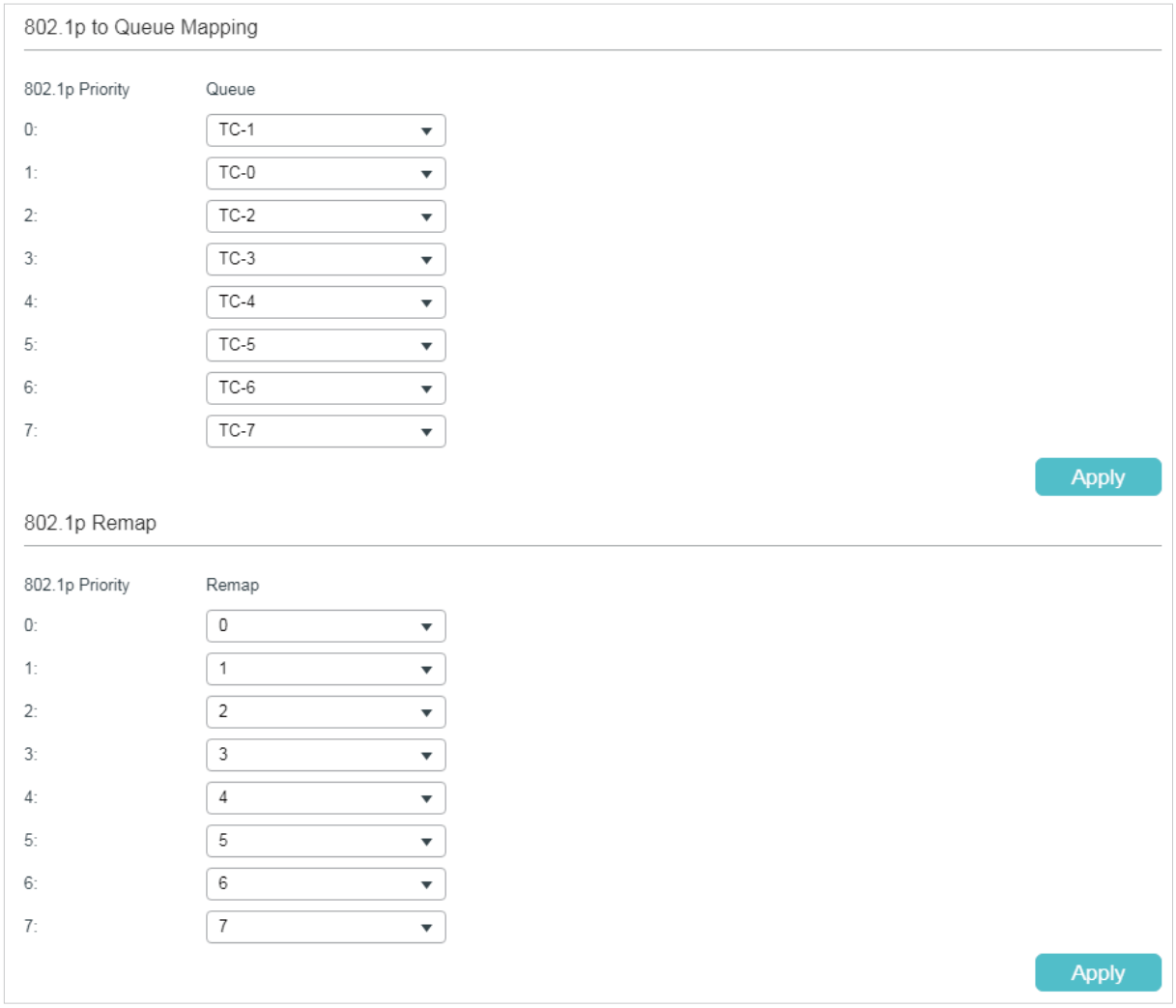
802.1p Priority	Specify the port to 802.1p mapping for the desired port. The ingress packets from one port are first mapped to 802.1p priority based on the port to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. The untagged packets from one port will be added an 802.1p priority value according to the port to 802.1p priority mapping.
Trust Mode	Select the Trust mode as Untrusted. In this mode, the packets will be processed according to the port priority configuration.

2) Click **Apply**.

Configuring the 802.1p to Queue Mapping

Choose the menu **QoS > Class of Service > 802.1p Priority** to load the following page.

Figure 2-2 Configuring the 802.1p to Queue Mapping



In the **802.1p to Queue Mapping** section, configure the mappings and click **Apply**.

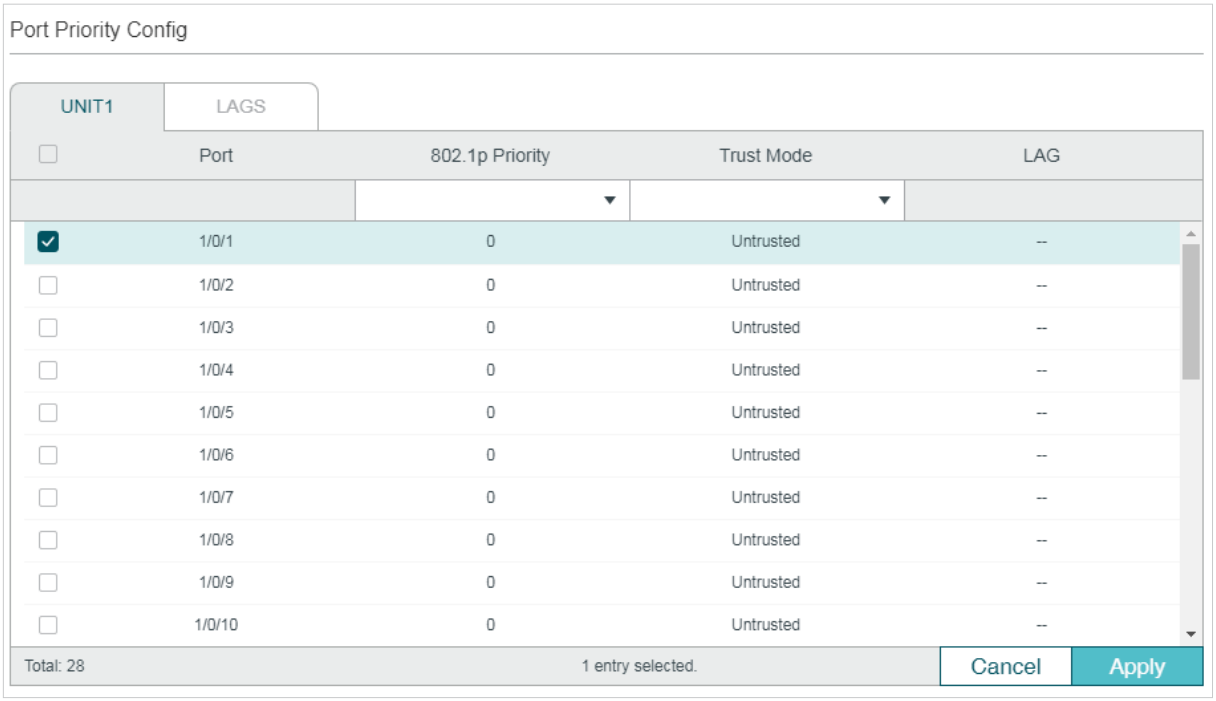
802.1p Priority	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service.
Queue	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

2.1.2 Configuring 802.1p Priority

■ Configuring the Trust Mode

Choose the menu **QoS > Class of Service > Port Priority** to load the following page.

Figure 2-3 Configuring the Trust Mode



Follow these steps to configure the trust mode:

1) Select the desired ports and set the trust mode as Trust 802.1p.

Trust Mode	Select the Trust mode as Trust 802.1p. In this mode, the tagged packets will be processed according to the 802.1p priority configuration and the untagged packets will be processed according to the port priority configuration.

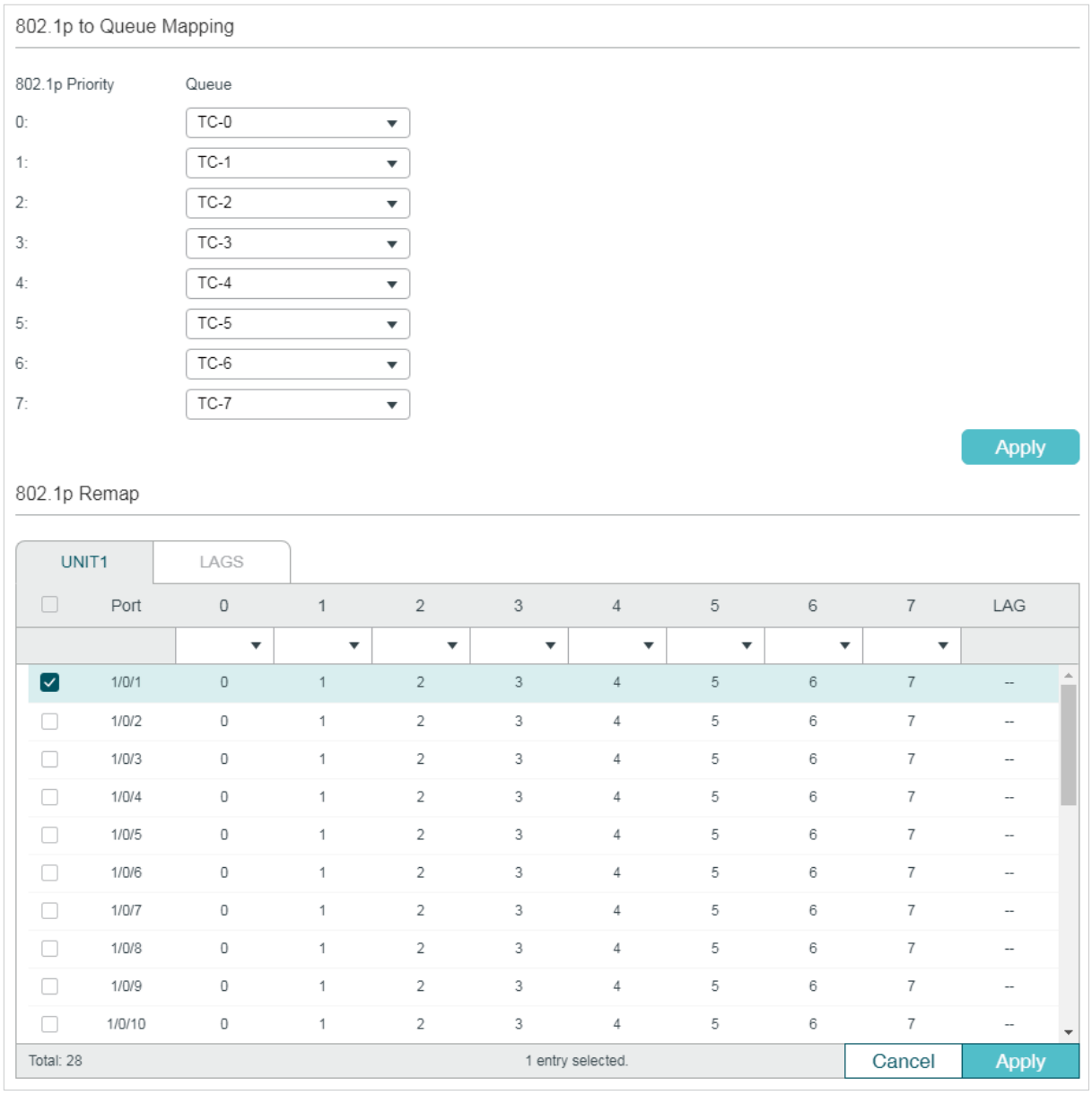
2) Click **Apply**.

■ Configuring the 802.1p to Queue Mapping and 802.1p Remap

For Certain Devices:

Choose the menu **QoS > Class of Service > 802.1p Priority** to load the following page.

Figure 2-4 Configuring the 802.1p to Queue Mapping and 802.1p Remap



Follow these steps to configure the parameters of the 802.1p priority:

1) In the **802.1p to Queue Mapping** section, configure the mappings and click **Apply**.

802.1p Priority	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service. IEEE 802.1p standard defines three bits in 802.1Q tag as PRI filed. The PRI values are called 802.1p priority and used to represent the priority of the layer 2 packets. This function requires packets with VLAN tags.
Queue	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

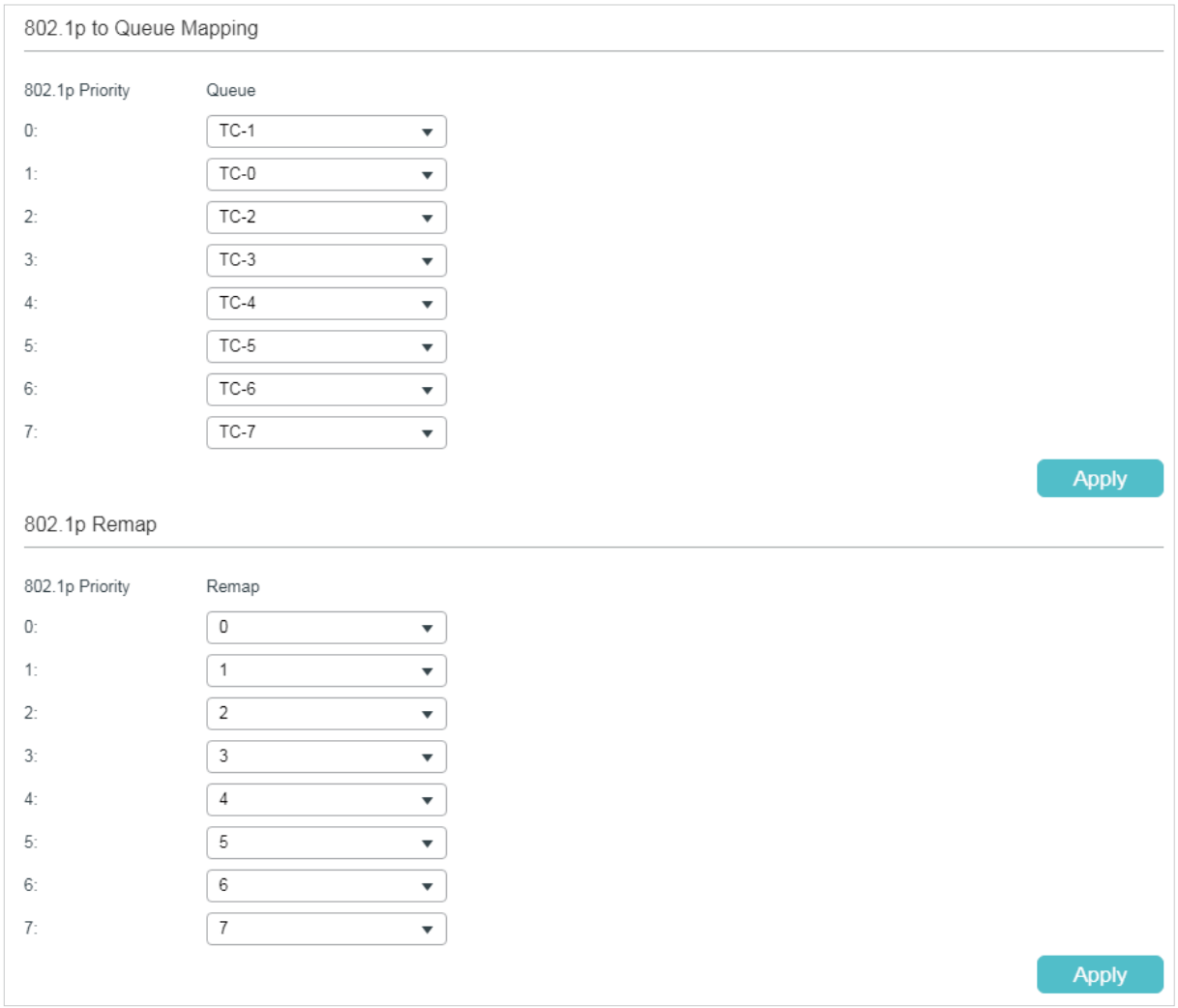
2) (Optional) In the **802.1p Remap** section, configure the 802.1p to 802.1p mappings for ports and click **Apply**.

0 - 7	Select the number of 802.1p priority to which the desired 802.1p priority will be remapped. 802.1p Remap is used to modify the 802.1p priority of the ingress packets. When the switch detects the packets with desired 802.1p priority, it will modify the value of 802.1p priority according to the map.

For Certain Devices:

Choose the menu **QoS > Class of Service > 802.1p Priority** to load the following page.

Figure 2-5 Configuring the 802.1p to Queue Mapping and 802.1p Remap



Follow these steps to configure the parameters of the 802.1p priority:

1) In the **802.1p to Queue Mapping** section, configure the mappings and click **Apply**.

802.1p Priority	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service. IEEE 802.1p standard defines three bits in 802.1Q tag as PRI filed. The PRI values are called 802.1p priority and used to represent the priority of the layer 2 packets. This function requires packets with VLAN tags.

Queue	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

2) (Optional) In the **802.1p Remap** section, configure the 802.1p to 802.1p mappings and click **Apply**.

802.1p Priority	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service. IEEE 802.1p standard defines three bits in 802.1Q tag as PRI filed. The PRI values are called 802.1p priority and used to represent the priority of the layer 2 packets. This function requires packets with VLAN tags.
Remap	Select the number of 802.1p priority to which the original 802.1p priority will be remapped. 802.1p Remap is used to modify the 802.1p priority of the ingress packets. When the switch detects the packets with desired 802.1p priority, it will modify the value of 802.1p priority according to the map.

Note:

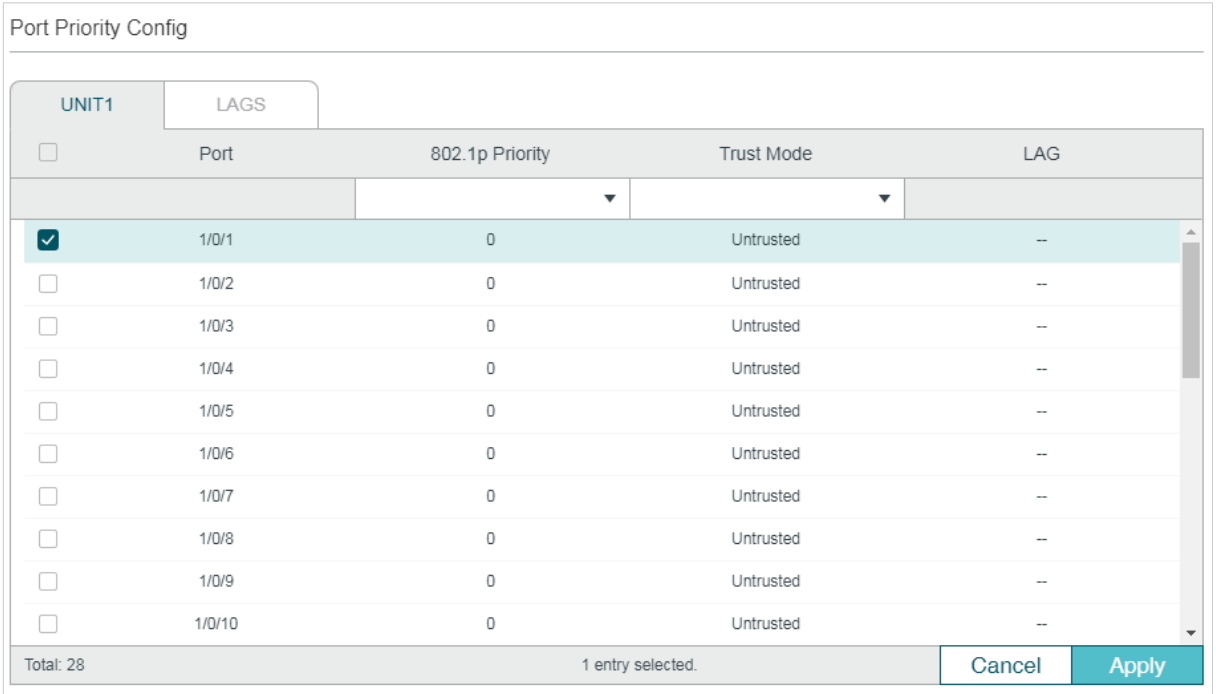
In Trust 802.1p mode, the untagged packets will be added an 802.1p priority based on the port to 802.1p mapping and will be forwarded according to the 802.1p to queue mapping.

2.1.3 Configuring DSCP Priority

Configuring the Trust Mode

Choose the menu **QoS > Class of Service > Port Priority** to load the following page.

Figure 2-6 Configuring the Trust Mode



Follow these steps to configure the trust mode:

1) Select the desired ports and set the trust mode as Trust DSCP.

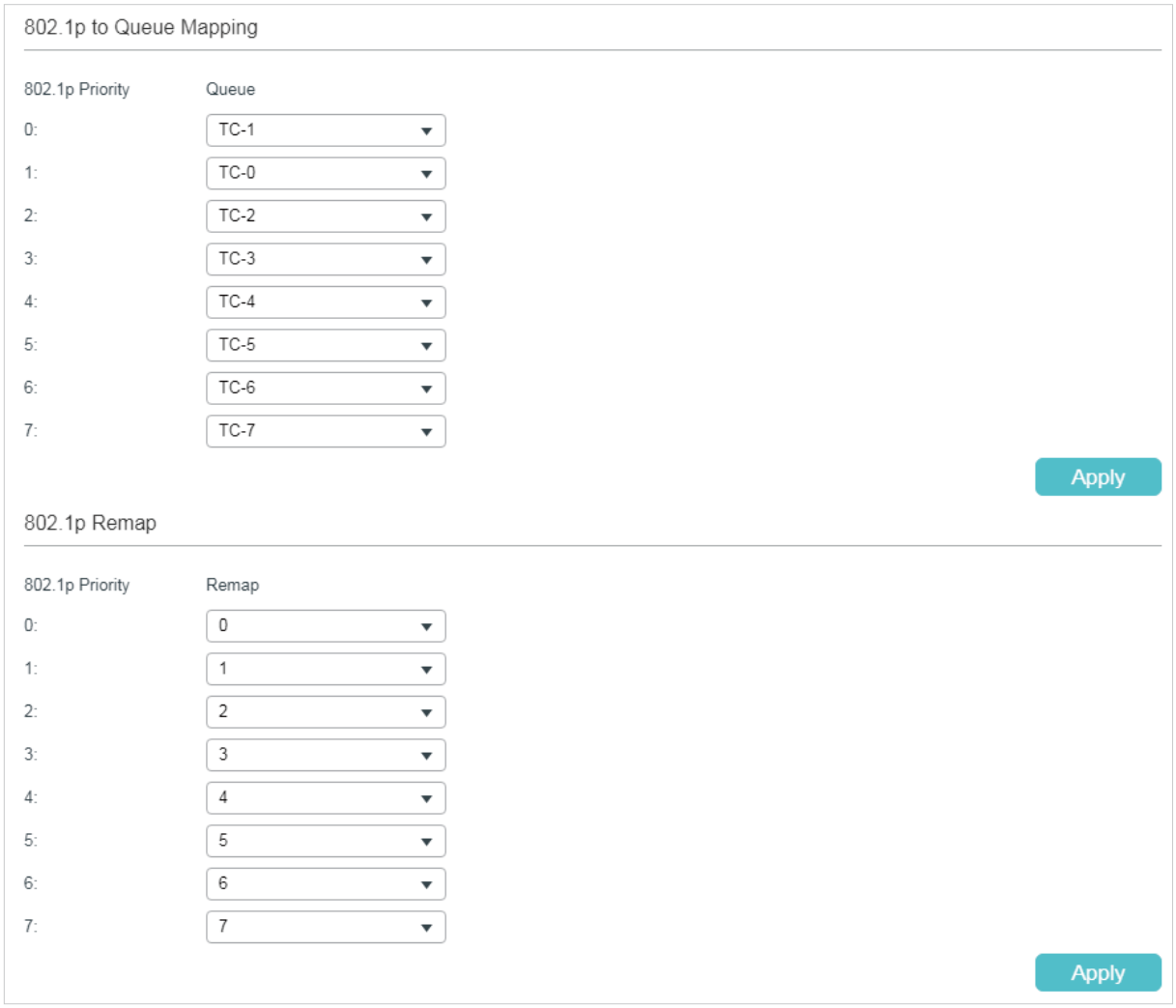
Trust Mode	Select the Trust mode as Trust DSCP. In this mode, the IP packets will be processed according to the DSCP priority configuration and the non-IP packets will be processed according to the port priority configuration.

2) Click **Apply**.

Configuring the 802.1p to Queue Mapping

Choose the menu **QoS > Class of Service > 802.1p Priority** to load the following page.

Figure 2-7 Configuring the 802.1p to Queue Mapping



In the **802.1p to Queue Mapping** section, configure the mappings and click **Apply**.

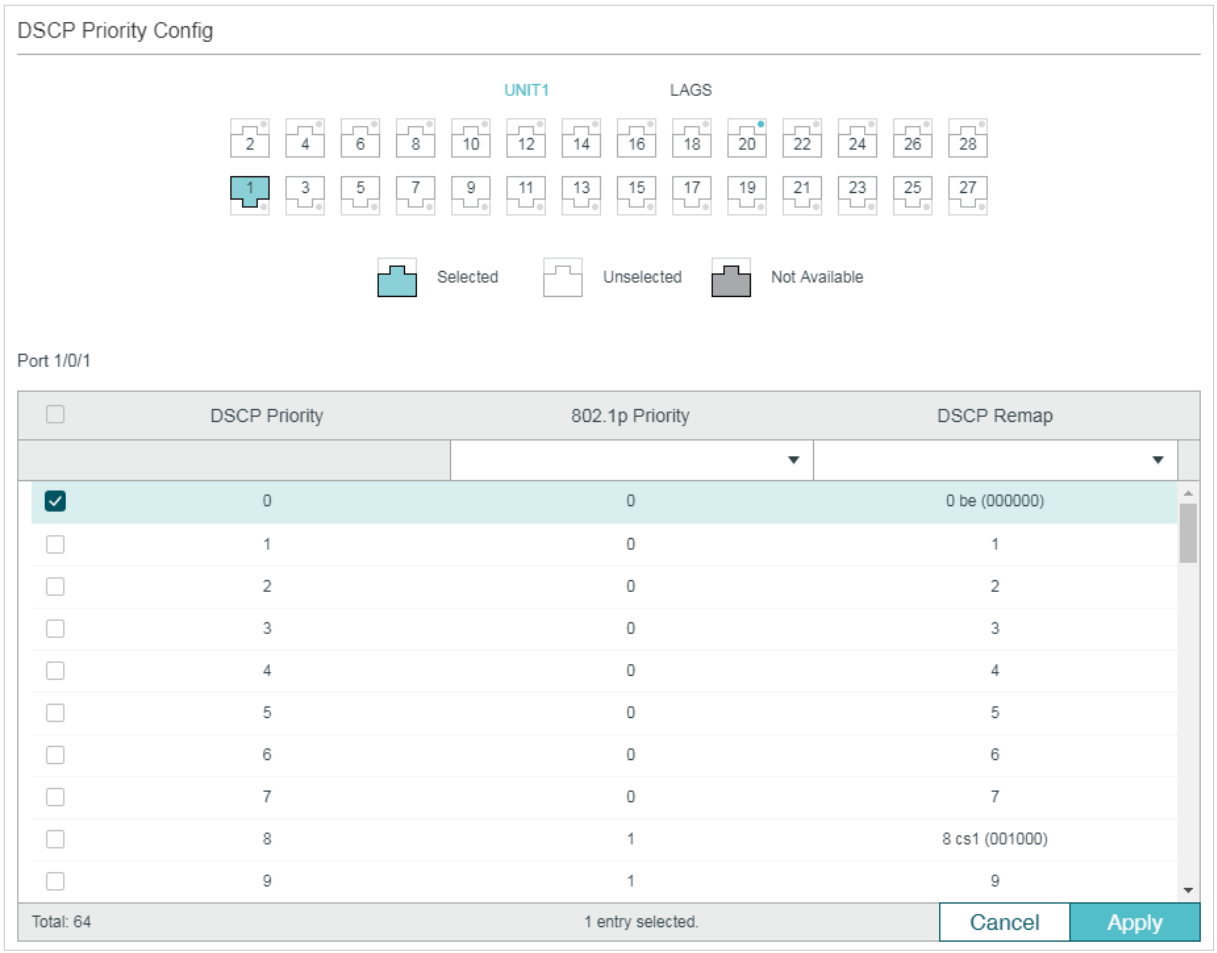
802.1p Priority	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service.
Queue	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

■ Configuring the DSCP to 802.1p Mapping and the DSCP Remap

For Certain Devices:

Choose the menu **QoS > Class of Service >DSCP Priority** to load the following page.

Figure 2-8 Configuring the DSCP to 802.1p Mapping and the DSCP Remap



Follow these steps to configure the DSCP Priority:

1) Select the desired port, configure the DSCP to 802.1p mapping and the DSCP remap.

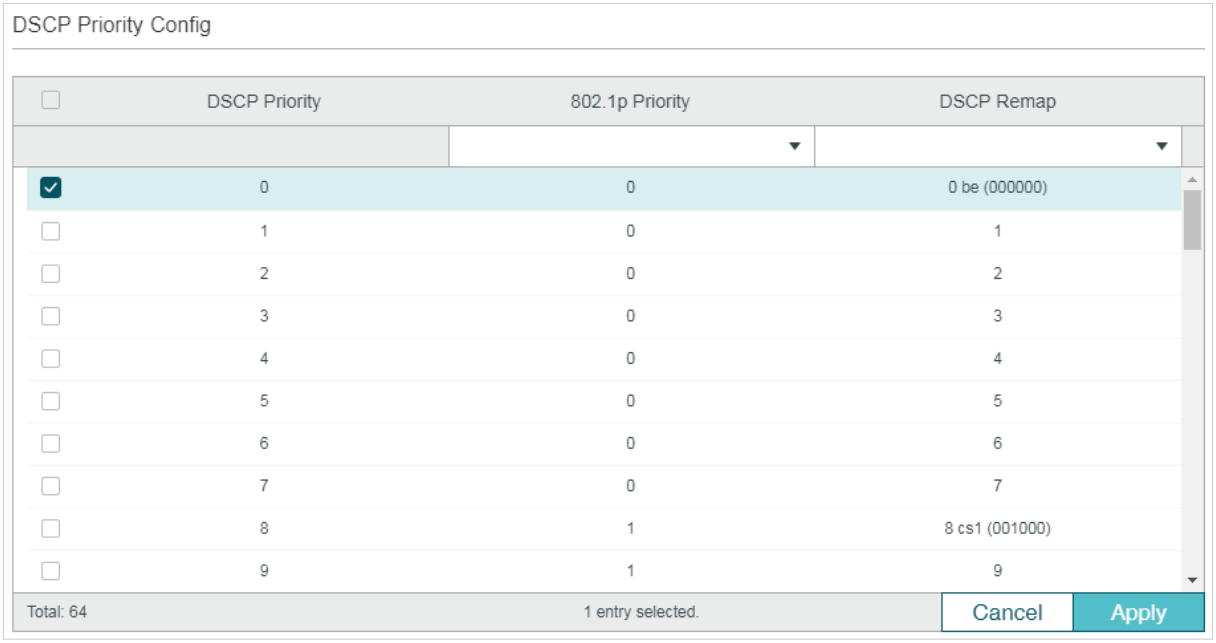
DSCP Priority	Displays the number of DSCP priority. DSCP Priority is used to classify the packets based on the value of DSCP, and map them to different queues. ToS (Type of Service) is a part of IP header, and DSCP uses the first six bits of ToS to represent the priority of IP packets. The DSCP values range from 0 to 63.
802.1p Priority	Specify the DSCP to 802.1p mapping for the desired port. The ingress packets are first mapped to 802.1p priority, then to TC queues according to the 802.1p to queue mappings.
DSCP Remap	(Optional) Select the DSCP priority to which the desired DSCP priority will be remapped for the port. When the switch detects the packets with desired DSCP value, it will modify the packets' DSCP value according to the map.

2) Click **Apply**.

For Certain Devices:

Choose the menu **QoS > Class of Service >DSCP Priority** to load the following page.

Figure 2-9 Configuring the DSCP to 802.1p Mapping and the DSCP Remap



Follow these steps to configure the DSCP Priority:

1) In the **DSCP Priority Config** section, configure the DSCP to 802.1p mapping and the DSCP remap.

DSCP Priority	Displays the number of DSCP priority. DSCP Priority is used to classify the packets based on the value of DSCP, and map them to different queues. ToS (Type of Service) is a part of IP header, and DSCP uses the first six bits of ToS to represent the priority of IP packets. The DSCP values range from 0 to 63.
802.1p Priority	Specify the DSCP to 802.1p mapping. The ingress packets are first mapped to 802.1p priority based on the DSCP to 802.1p mappings, then to TC queues according to the 802.1p to queue mappings. The untagged IP packets with the desired DSCP value will be added an 802.1p priority value according to the DSCP to 802.1p mapping.
DSCP Remap	(Optional) Select the DSCP priority to which the original DSCP priority will be remapped. When the switch detects the packets with desired DSCP value, it will modify the packets' DSCP value according to the map.

2) Click **Apply**.

Note:

In Trust DSCP mode, non-IP packets will be added an 802.1p priority based on the port to 802.1p mapping and will be forwarded according to the 802.1p to queue mapping.

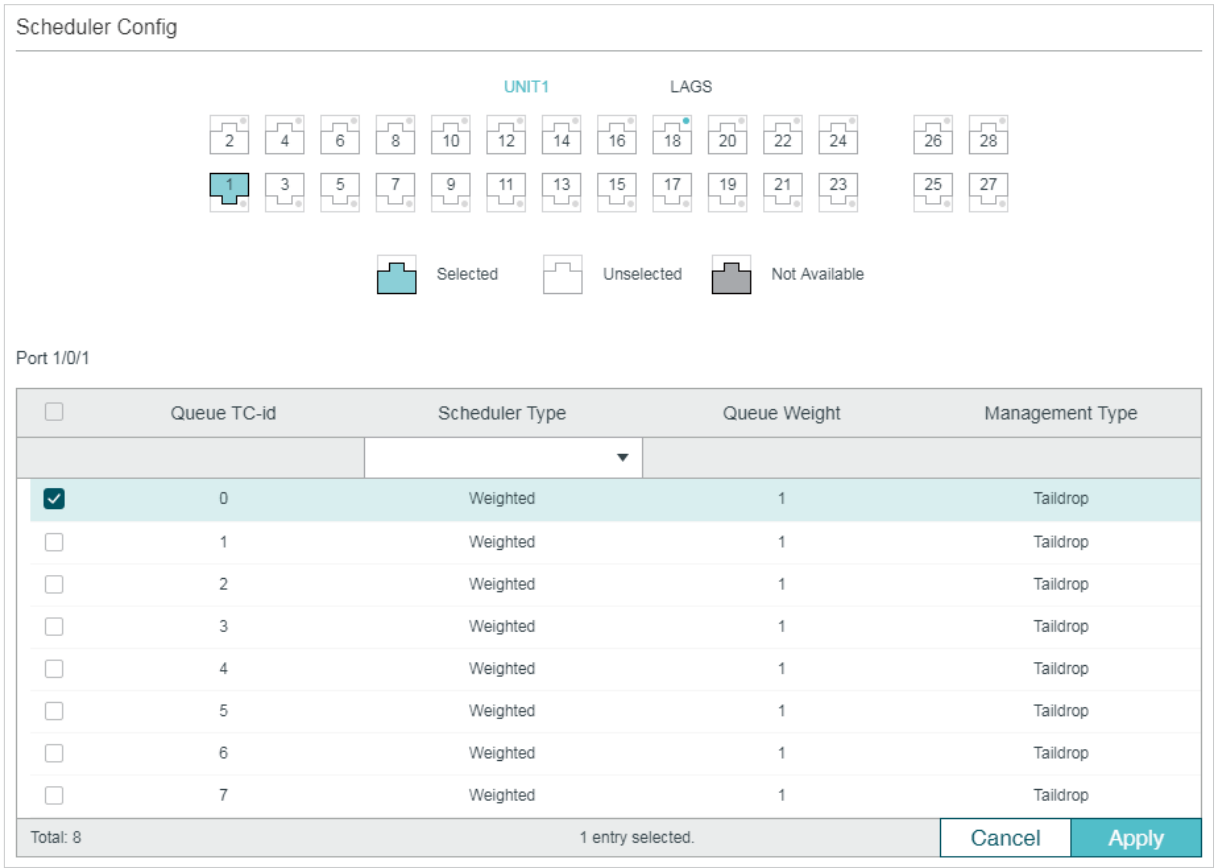
2.1.4 Specifying the Scheduler Settings

Specify the scheduler settings to control the forwarding sequence of different TC queues when congestion occurs.

For Certain Devices:

Choose the menu **QoS > Class of Service > Scheduler Settings** to load the following page.

Figure 2-10 Specifying the Scheduler Settings



Follow these steps to configure the schedule mode:

1) In the **Scheduler Config** section, select the desired port.
2) Select the desired queue and configure the parameters.

Queue TC-id	Displays the ID number of priority Queue.

Scheduler Type	Select the type of scheduling used for corresponding queue. When the network congestion occurs, the egress queue will determine the forwarding sequence of the packets according to the type. **Strict:** In this mode, the egress queue will use SP (Strict Priority) to process the traffic in different queues. When congestion occurs, the traffic will be transmitted according to its queue priority strictly. The queue with higher priority occupies the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. **Weighted:** In this mode, the egress queue will use WRR (Weighted Round Robin) to process the traffic in different queues. When congestion occurs, all the traffic will be transmitted, but the bandwidth that each traffic queue occupies will be allocated based on the queue weight.
Queue Weight	Specify the queue weight for the desired queue. This value can be set only in the Weighted mode. The valid values are from 1 to 127.
Minimum Bandwidth	Specify the minimum guaranteed bandwidth for the desired queue. The valid values are from 0 to 100 and 0 means Minimum Bandwidth is disabled. If the queue bandwidth calculated according to the weight is smaller than the minimum bandwidth, the switch will be forced to allocated the minimum bandwidth to the queue, and the other queue will share the rest bandwidth based on the weight. **Note:** Minimum Bandwidth is only available on certain devices.
Management Type	Displays the Management Type for the queues. The switch supports Taildrop mode. When the traffic exceeds the limit, the additional traffic will be dropped.

3) Click **Apply**.

For Certain Devices:

Choose the menu **QoS > Class of Service > Scheduler Settings** to load the following page.

Figure 2-11 Specifying the Scheduler Settings

Scheduler Config

Queue TC-id	Scheduler Type	Queue Weight	Management Type
0	Weighted	1	Taildrop
1	Weighted	1	Taildrop
2	Weighted	1	Taildrop
3	Weighted	1	Taildrop
4	Weighted	1	Taildrop
5	Weighted	1	Taildrop
6	Weighted	1	Taildrop
7	Weighted	1	Taildrop

Total: 8

Follow these steps to configure the schedule mode:

1) In the **Scheduler Config** section, select the desired queue and configure the parameters.

Queue TC-id	Displays the ID number of priority Queue.
Scheduler Type	Select the type of scheduling used for corresponding queue. When the network congestion occurs, the egress queue will determine the forwarding sequence of the packets according to the type. **Strict:** In this mode, the egress queue will use SP (Strict Priority) to process the traffic in different queues. When congestion occurs, the traffic will be transmitted according to its queue priority strictly. The queue with higher priority occupies the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. **Weighted:** In this mode, the egress queue will use WRR (Weighted Round Robin) to process the traffic in different queues. When congestion occurs, all the traffic will be transmitted, but the bandwidth that each traffic queue occupies will be allocated based on the queue weight.
Queue Weight	Specify the queue weight for the desired queue. This value can be set only in the Weighted mode. The valid values are from 1 to 127.
Minimum Bandwidth	Specify the minimum guaranteed bandwidth for the desired queue. The valid values are from 0 to 100 and 0 means Minimum Bandwidth is disabled. If the queue bandwidth calculated according to the weight is smaller than the minimum bandwidth, the switch will be forced to allocated the minimum bandwidth to the queue, and the other queue will share the rest bandwidth based on the weight. **Note:** Minimum Bandwidth is only available on certain devices.
Management Type	Displays the Management Type for the queues. The switch supports Taildrop mode. When the traffic exceeds the limit, the additional traffic will be dropped.

2) Click **Apply**.

Note:

With ACL Redirect feature, the switch maps all the packets that meet the configured ACL rules to the new TC queue, regardless of the mapping relations configured in this section.

2.2 Using CLI

2.2.1 Configuring Port Priority

- Configuring the Trust Mode and the port to 802.1p Mapping

Follow these steps to configure the trust mode and the port to 802.1p mapping:

Step 1	**configure** Enter global configuration mode
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**qos trust mode {***untrust* **|** *dot1p* **|** *dscp***}** Select the trust mode for the port. By default, it is untrust. Here we set the trust mode as untrust. *untrust:* Specify the ports' trust mode as untrust. In this mode, the packets will be processed according to the port priority configuration.
Step 4	**qos port-priority {***dot1p-priority***}** Specify the port to 802.1p priority mapping for the desired port. The ingress packets from one port are first mapped to 802.1p priority based on the port to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. The untagged packets from one port will be added an 802.1p priority value according to the port to 802.1p mapping. *dot1p-priority:* Specify the 802.1p priority ranging from 0 to 7. The default value is 0.
Step 5	**show qos trust interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the trust mode of the ports.
Step 6	**show qos port-priority interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the port to 802.1p mappings.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

■ Configuring the 802.1p to Queue Mapping

Follow these steps to configure the 802.1p to queue mapping:

Step 1	**configure** Enter global configuration mode

Step 2	**qos cos-map {***dot1p-priority***} {***tc-queue***}** Specify the 802.1p to queue mapping. The packets with the desired 802.1p priority will be put in the corresponding queues. By default, the 802.1p priority 0 to 7 is respectively mapped to TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7. *dot1p-priority*: Specify the 802.1p priority. The valid values are from 0 to 7. *tc-queue*: Specify the ID number of the TC queue. The valid values are from 0 to 7.
Step 3	**show qos cos-map** Verify the 802.1p to queue mappings.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the trust mode of port 1/0/1 as untrust, map the port 1/0/1 to 802.1p priority 1 and map 802.1p priority 1 to TC3:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#qos trust mode untrust

Switch(config-if)#qos port-priority 1

Switch(config-if)#exit

Switch(config)#qos cos-map 1 3

Switch(config)#show qos trust interface gigabitEthernet 1/0/1

```
Port       Trust Mode      LAG
--------   ---------       --------
Gi1/0/1    untrust         N/A
```

Switch(config)#show qos port-priority interface gigabitEthernet 1/0/1

```
Port       CoS Value       LAG
--------   ---------       --------
Gi1/0/1    CoS  1          N/A
```

Switch(config)#show qos cos-map

```
---------------+-----+-----+-----+-----+-----+-----+----+----
Dot1p Value |0     |1    |2     |3     |4     |5     |6    |7
---------------+-----+-----+-----+-----+-----+-----+----+----
TC             |TC0  |TC3  |TC2  |TC3  |TC4 |TC5  |TC6 |TC7
---------------+-----+-----+-----+-----+-----+-----+----+----
```

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring 802.1p Priority

■ Configuring the Trust Mode

Follow these steps to configure the trust mode:

Step 1	**configure** Enter global configuration mode

Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**qos trust mode {***untrust* **|** *dot1p* **|** *dscp***}** Select the trust mode for the port. By default, it is untrust. Here we set the trust mode as dot1p. *dot1p:* Specify the ports' trust mode as dot1p. In this mode, the tagged packets will be processed according to the 802.1p priority configuration and the untagged packets will be processed according to the port priority configuration.
Step 4	**show qos trust interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the trust mode of the ports.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

Configuring the 802.1p to Queue Mapping and 802.1p Remap

Follow these steps to configure the 802.1p to queue mapping and 802.1p remap:

Step 1	**configure** Enter global configuration mode
Step 2	**qos cos-map {***dot1p-priority***} {***tc-queue***}** Specify the 802.1p to queue mapping. The packets with the desired 802.1p priority will be put in the corresponding queues. By default, the 802.1p priority 0 to 7 is respectively mapped to TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7. *dot1p-priority:* Specify the 802.1p priority. The valid values are from 0 to 7. *tc-queue:* Specify the ID number of the TC queue. The valid values are from 0 to 7.

Step 3	For Certain Devices: **interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode. **qos dot1p-remap {***dot1p-priority***} {***new-dot1p-priority***}** (Optional) Specify the 802.1p to 802.1p mappings for the desired port. 802.1p Remap is used to modify the 802.1p priority of the ingress packets. When the switch detects the packets with desired 802.1p priority, it will modify the value of 802.1p priority according to the map. By default, the original 802.1p priority 0 is mapped to the 802.1p priority 0, the original 802.1p priority 1 is mapped to the 802.1p priority 1 and so on. *dot1p-priority*: Specify the original 802.1p priority. The valid values are from 0 to 7. *new-dot1p-priority*: Specify the new 802.1p priority. The valid values are from 0 to 7. For Certain Devices: **qos dot1p-remap {***dot1p-priority***} {***new-dot1p-priority***}** (Optional) Specify the 802.1p to 802.1p mappings. 802.1p Remap is used to modify the 802.1p priority of the ingress packets. When the switch detects the packets with desired 802.1p priority, it will modify the value of 802.1p priority according to the map. By default, the original 802.1p priority 0 is mapped to the 802.1p priority 0, the original 802.1p priority 1 is mapped to the 802.1p priority 1 and so on. *dot1p-priority*: Specify the original 802.1p priority. The valid values are from 0 to 7. *new-dot1p-priority*: Specify the new 802.1p priority. The valid values are from 0 to 7.
Step 4	**show qos cos-map** Verify the 802.1p to queue mappings.
Step 5	For Certain Devices: **show qos dot1p-remap interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the 802.1p to 802.1p mappings of the ports. For Certain Devices: **show qos dot1p-remap** Verify the 802.1p to 802.1p mappings globally.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

Note:

In Trust 802.1p mode, the untagged packets will be added an 802.1p priority based on the port to 802.1p mapping and will be forwarded according to the 802.1p to queue mapping.

The following example shows how to configure the trust mode of port 1/0/1 as dot1p, map 802.1p priority 3 to TC4, and configure to map the original 802.1p 1 to 802.1p priority 3:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#qos trust mode dot1p

Switch(config-if)#exit

Switch(config)#qos cos-map 3 4

Switch(config)#qos dot1p-remap 1 3

Switch(config)#show qos trust interface gigabitEthernet 1/0/1

Port	Trust Mode	LAG
Gi1/0/1	trust 802.1P	N/A

Switch(config)#show qos cos-map

Dot1p Value	0	1	2	**3**	4	5	6	7
TC	TC0	TC1	TC2	**TC4**	TC4	TC5	TC6	TC7

Switch(config)#show qos dot1p-remap

Dot1p Value	0	**1**	2	3	4	5	6	7	LAG
Dot1p Remap	0	**3**	2	3	4	5	6	7	N/A

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring DSCP Priority

- Configuring the Trust Mode

Follow these steps to configure the trust mode:

Step 1	**configure** Enter global configuration mode
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**qos trust mode {***untrust* **|** *dot1p* **|** *dscp***}** Select the trust mode for the port. By default, it is untrust. Here we set the trust mode as dscp. *dscp:* Specify the ports' trust mode as dscp. In this mode, the IP packets will be processed according to the DSCP priority configuration and the non-IP packets will be processed according to the port priority configuration.
Step 4	**show qos trust interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the trust mode of the ports.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

■ Configuring the 802.1p to Queue Mapping

Follow these steps to configure the 802.1p to queue mapping:

Step 1	**configure** Enter global configuration mode
Step 2	**qos cos-map {***dot1p-priority***} {***tc-queue***}** Specify the 802.1p to queue mapping. The packets with the desired 802.1p priority will be put in the corresponding queues. By default, the 802.1p priority 0 to 7 is respectively mapped to TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7. *dot1p-priority:* Specify the 802.1p priority. The valid values are from 0 to 7. *tc-queue:* Specify the ID number of the TC queue. The valid values are from 0 to 7.
Step 3	**show qos cos-map** Verify the 802.1p to queue mappings.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

Configuring the DSCP to 802.1p Mapping and DSCP Remp

Follow these steps to configure the DSCP to 802.1p mapping and DSCP remap:

Step 1	**configure** Enter global configuration mode
Step 2	For Certain Devices: **interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode. **qos dscp-map {***dscp-value-list***} {***dot1p-priority***}** Specify the DSCP to 802.1p mapping for the desired port. The ingress packets with the desired DSCP priority are first mapped to 802.1p priority based on the DSCP to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. By default, the DSCP priorities 0-7 are mapped to the 802.1p priority 0, the DSCP priorities 8-15 are mapped to the 802.1p priority 1 and so on. *dscp-value-list:* Specify the DSCP value list in the format of "1-3,5,7". The valid values are from 0 to 63. *dot1p-priority:* Specify the 802.1p priority. The valid values are from 0 to 7. For Certain Devices: **qos dscp-map {***dscp-value-list***} {***dot1p-priority***}** Specify the DSCP to 802.1p mapping. The ingress packets with the desired DSCP priority are first mapped to 802.1p priority based on the DSCP to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. The untagged packets with the desired DSCP priority will be added an 802.1p priority value according to the DSCP to 802.1p mapping. by default, the DSCP priorities 0-7 are mapped to the 802.1p priority 0, the DSCP priorities 8-15 are mapped to the 802.1p priority 1 and so on. *dscp-value-list:* Specify the DSCP value list in the format of "1-3,5,7". The valid values are from 0 to 63. *dot1p-priority:* Specify the 802.1p priority. The valid values are from 0 to 7.
Step 3	**qos dscp-remap {***dscp-value-list***} {***dscp-remap-value***}** (Optional) Specify the DSCP to DSCP mappings. DSCP Remap is used to modify the DSCP priority of the ingress packets. When the switch detects the packets with the desired DSCP priority, it will modify the value of DSCP priority according to the map. By default, the original DSCP priority 0 is mapped to the DSCP priority 0, the original DSCP priority 1 is mapped to the DSCP priority 1 and so on. *dscp-value-list:* Specify the original DSCP priority list in the format of "1-3,5,7". The valid values are from 0 to 63. *dscp-remap-value:* Specify the new DSCP priority. The valid values are from 0 to 63.

Step 4	For Certain Devices: **show qos dscp-map interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the DSCP to queue mappings of ports. For Certain Devices: **show qos dscp-map** Verify the DSCP to queue mappings globally.
Step 5	For Certain Devices: **show qos dscp-remap interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the DSCP to DSCP mappings of the ports. For Certain Devices: **show qos dscp-remap** Verify the DSCP to DSCP mappings globally.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

Note:

In Trust DSCP mode, non-IP packets will be added an 802.1p priority based on the port to 802.1p mapping and will be forwarded according to the 802.1p to queue mapping.

The following example shows how to configure the trust mode of port 1/0/1 as dscp, map 802.1p priority 3 to TC4, map DSCP priority 1-3,5,7 to 802.1p priority 3, and configure to map the original DSCP priority 9 to DSCP priority 5:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#qos trust mode dscp

Switch(config-if)#exit

Switch(config)#qos cos-map 3 4

Switch(config)#qos dscp-map 1-3,5,7 3

Switch(config)#qos dscp-remap 9 5

Switch(config)#show qos trust interface gigabitEthernet 1/0/1

```
Port        Trust Mode      LAG
--------    ---------       ------
Gi1/0/1     trust DSCP      N/A
```

Switch(config)#show qos cos-map

```
---------------+-----+-----+-----+-----+-----+-----+----+----
Dot1p Value |0     |1    |2    |3    |4    |5    |6   |7
---------------+-----+-----+-----+-----+-----+-----+----+----
TC              |TC0 |TC1 |TC2 |TC4 |TC4 |TC5 |TC6 |TC7
---------------+-----+-----+-----+-----+-----+-----+----+----
```

Switch(config)#show qos dscp-map

```
DSCP:               0   1   2   3   4   5   6   7
DSCP to 802.1P      0   3   3   3   0   3   0   3
                    ---- ---- ---- ---- ---- ---- ---- ----
DSCP:               8   9   10  11  12  13  14  15
DSCP to 802.1P      1   1   1   1   1   1   1   1
                    ---- ---- ---- ---- ---- ---- ---- ----
DSCP:               16  17  18  19  20  21  22  23
DSCP to 802.1P      2   2   2   2   2   2   2   2
                    ---- ---- ---- ---- ---- ---- ---- ----
DSCP:               24  25  26  27  28  29  30  31
DSCP to 802.1P      3   3   3   3   3   3   3   3
                    ---- ---- ---- ---- ---- ---- ---- ----
DSCP:               32  33  34  35  36  37  38  39
DSCP to 802.1P      4   4   4   4   4   4   4   4
                    ---- ---- ---- ---- ---- ---- ---- ----
DSCP:               40  41  42  43  44  45  46  47
DSCP to 802.1P      5   5   5   5   5   5   5   5
                    ---- ---- ---- ---- ---- ---- ---- ---
DSCP:               48  49  50  51  52  53  54  55
```

DSCP to 802.1P 6 6 6 6 6 6 6 6

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 56 57 58 59 60 61 62 63

DSCP to 802.1P 7 7 7 7 7 7 7 7

---- ---- ---- ---- ---- ---- ---- ---

Switch(config)#show qos dscp-remap

DSCP: 0 1 2 3 4 5 6 7

DSCP remap value 0 1 2 3 4 5 6 7

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 8 **9** 10 11 12 13 14 15

DSCP remap value 8 **5** 10 11 12 13 14 15

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 16 17 18 19 20 21 22 23

DSCP remap value 16 17 18 19 20 21 22 23

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 24 25 26 27 28 29 30 31

DSCP remap value 24 25 26 27 28 29 30 31

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 32 33 34 35 36 37 38 39

DSCP remap value 32 33 34 35 36 37 38 39

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 40 41 42 43 44 45 46 47

DSCP remap value 40 41 42 43 44 45 46 47

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 48 49 50 51 52 53 54 55

DSCP remap value 48 49 50 51 52 53 54 55

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 56 57 58 59 60 61 62 63

DSCP remap value 56 57 58 59 60 61 62 63

---- ---- ---- ---- ---- ---- ---- ----

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Specifying the Scheduler Settings

Follow these steps to specify the scheduler settings to control the forwarding sequence of different TC queues when congestion occurs.

Step 1	**configure**	
	Enter global configuration mode.	

Step 2 For Certain Devices:

interface {fastEthernet *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}**

Enter interface configuration mode.

qos queue *tc-queue* **mode {**sp **|** wrr**} [weight** *weight***]**

Specify the type of scheduling used for corresponding queue. When the network congestion occurs, the egress queue will determine the forwarding sequence of the packets according to the type. By default, it is wrr mode and the all the queue weights are 1.

tc-queue: Specify the ID number of TC queue. The valid values are from 0 to 7.

sp: In sp mode, the egress queue will use SP (Strict Priority) to process the traffic in different queues. When congestion occurs, the traffic will be transmitted according to its queue priority strictly. The queue with higher priority occupies the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.

wrr: In wrr mode, the egress queue will use WRR (Weighted Round Robin) to process the traffic in different queues. When congestion occurs, all the traffic will be transmitted, but the bandwidth that each traffic queue occupies will be allocated based on the queue weight.

weight: Specify the queue weight for the desired queue. This value can be set only in the wrr mode. The valid values are from 1 to 127.

For Certain Devices:

qos queue *tc-queue* **mode {**sp **|** wrr**} [weight** *weight***]**

Specify the type of scheduling used for corresponding queue. When the network congestion occurs, the egress queue will determine the forwarding sequence of the packets according to the type. By default, it is wrr mode and the all the queue weights are 1.

tc-queue: Specify the ID number of TC queue. The valid values are from 0 to 7.

sp: In sp mode, the egress queue will use SP (Strict Priority) to process the traffic in different queues. When congestion occurs, the traffic will be transmitted according to its queue priority strictly. The queue with higher priority occupies the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.

wrr: In wrr mode, the egress queue will use WRR (Weighted Round Robin) to process the traffic in different queues. When congestion occurs, all the traffic will be transmitted, but the bandwidth that each traffic queue occupies will be allocated based on the queue weight.

weight: Specify the queue weight for the desired queue. This value can be set only in the wrr mode. The valid values are from 1 to 127.

Step 3	**qos queue** *tc-queue* **bandwidth** *rate* Specify the minimum guaranteed bandwidth for the desired queue. If the queue bandwidth calculated according to the weight is smaller than the minimum bandwidth, the switch will be forced to allocated the minimum bandwidth to the queue, and the other queue will share the rest bandwidth based on the weight. *tc-queue:* Specify the ID number of the TC queue. The valid values are from 0 to 7. *rate:* Specify the rate for the desired TC queue. The valid values are from 1 to 100. The default value is 0. **Note**: Minimum Bandwidth is only available on certain devices.
Step 4	**show qos queue interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the scheduler settings..
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

Note:

With ACL Redirect feature, the switch maps all the packets that meet the configured ACL rules to the new TC queue, regardless of the mapping relations configured in this section.

The following example shows how to specify the scheduler settings for port 1/0/1. Set the scheduler mode of TC1 as sp mode, set the scheduler mode of TC4 as wrr mode and set the queue weight as 5.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#qos queue 1 **mode** sp

Switch(config-if)#qos queue 4 **mode** wrr **weight** 5

Switch(config-if)#show qos queue interface gigabitEthernet 1/0/1

Gi1/0/1----LAG: N/A

Queue	Schedule Mode	Weight
TC0	WRR	1
TC1	Strict	N/A
TC2	WRR	1
TC3	WRR	1

TC4	WRR	5
TC5	WRR	1
TC6	WRR	1
TC7	WRR	1

Switch(config-if)#end

Switch#copy running-config startup-config

3 Bandwidth Control Configuration

With bandwidth control configurations, you can:

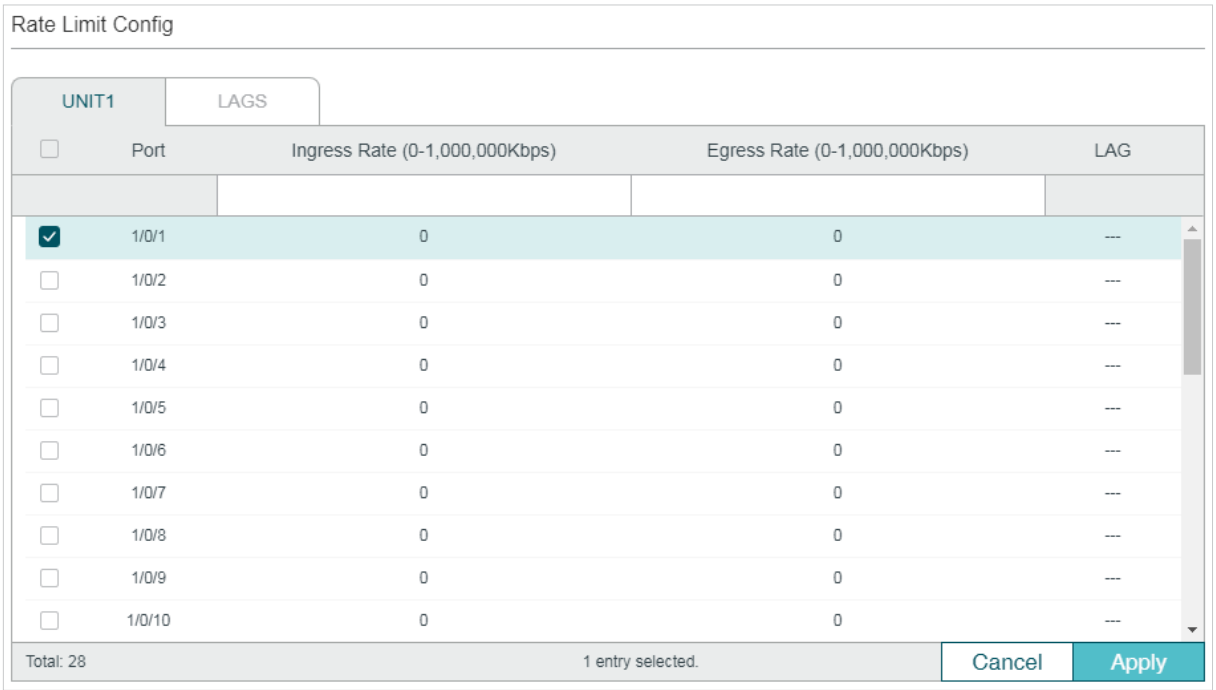
- Configure rate limit
- Configure storm control

3.1 Using the GUI

3.1.1 Configuring Rate Limit

Choose the menu **QoS > Bandwidth Control > Rate Limit** to load the following page.

Figure 3-1 Configuring Rate Limit



Follow these steps to configure the Rate Limit function:

1) Select the desired port and configure the upper rate limit to receive and send packets.

Ingress Rate (0-1,000,000Kbps)	Specify the upper rate limit for receiving packets on the port. The rate ranges from 1 to 1000000 kbps for the gigaport and 1 to 100000 kbps for the fast port, and is rounded off to the nearest multiple of 64. 0 means the ingress rate limit is disabled.

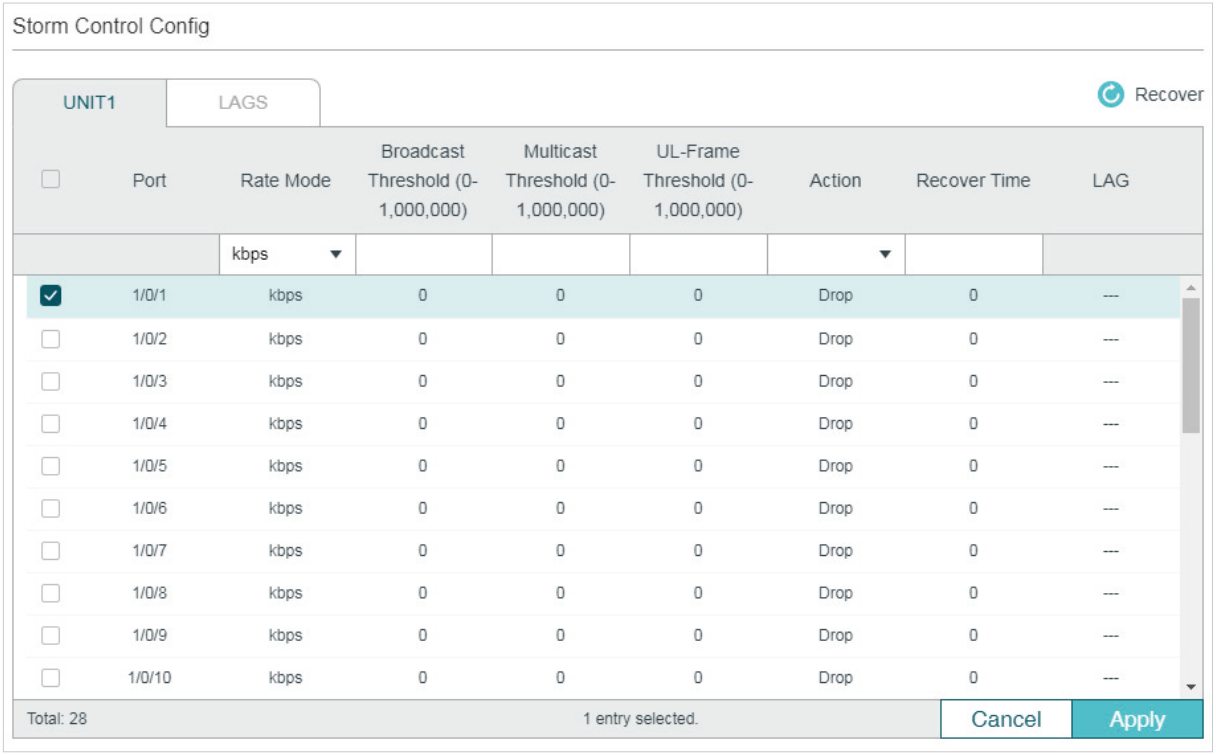
Egress Rate (0-1,000,000Kbps)	Specify the upper rate limit for sending packets on the port. The rate ranges from 1 to 1000000 kbps for the gigaport and 1 to 100000 kbps for the fast port, and is rounded off to the nearest multiple of 64. 0 means the egress rate limit is disabled.

2) Click **Apply**.

3.1.2 Configuring Storm Control

Choose the menu **QoS > Bandwidth Control > Storm Control** to load the following page.

Figure 3-2 Configuring Storm Control



Follow these steps to configure the Storm Control function:

1) Select the desired port and configure the upper rate limit for forwarding broadcast packets, multicast packets and UL-frames (Unknown unicast frames).

Rate Mode	Specify the Rate Mode for the broadcast threshold, multicast threshold and UL-Frame threshold on the desired port. **kbps:** The switch will limit the maximum speed of the specific kinds of traffic in kilo-bits per second. **ratio:** The switch will limit the percentage of bandwidth utilization for specific kinds of traffic. **pps:** The switch will limit the maximum number of packets per second for specific kinds of traffic. Note: **pps** is only available on certain devices.

Broadcast Threshold (0-1,000,000)	Specify the upper rate limit for receiving broadcast packets. The valid values differ among different rate modes. For kbps, the rate ranges from 1 to 1000000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate ranges from 1 to 1488000 packets per second. The value 0 means the broadcast threshold is disabled. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold (0-1,000,000)	Specify the upper rate limit for receiving multicast packets. The valid values differ among different rate modes. For kbps, the rate ranges from 1 to 1000000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate ranges from 1 to 1488000 packets per second. The value 0 means the multicast threshold is disabled. The multicast traffic exceeding the limit will be processed according to the Action configurations.
UL-Frame Threshold (0-1,000,000)	Specify the upper rate limit for receiving unknown unicast frames. The valid values differ among different rate modes. For kbps, the rate ranges from 1 to 1000000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate ranges from 1 to 1488000 packets per second. The value 0 means the unknown unicast threshold is disabled. The traffic exceeding the limit will be processed according to the Action configurations.
Action	Select the action that the switch will take when the traffic exceeds its corresponding limit. **Drop:** Set the Action as Drop. The port will drop the subsequent packets when the traffic exceeds the limit. **Shutdown:** Set the Action as Shutdown. The port will be shutdown when the traffic exceeds the limit.
Recover Time	Specify the recover time for the port. It takes effect only when the action is set as shutdown. The valid values are from 0 to 3600 seconds. When the port is shutdown, it can recover to its normal state after the recover time passed. If the recover time is specified as 0, which means the port will not recover to its normal state automatically and you can recover the port manually.

2) Click **Apply**.

Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and not its own. The configurations of the port can take effect only after it leaves the LAG.

3.2 Using the CLI

3.2.1 Configuring Rate Limit

Follow these steps to configure the upper rate limit for the port to receive and send packets:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**bandwidth {ingress** *ingress-rate* **| egress** *egress-rate***}** Configure the upper rate limit for the port to receive and send packets. *ingress-rate:* Specify the upper rate limit for receiving packets on the port. The rate ranges from 1 to 1000000 kbps for the gigaport and 1 to 100000 kbps for the fast port, and is rounded off to the nearest multiple of 64. *egress-rate:* Specify the upper rate limit for sending packets on the port. The rate ranges from 1 to 1000000 kbps for the gigaport and 1 to 100000 kbps for the fast port, and is rounded off to the nearest multiple of 64.
Step 4	**show bandwidth interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the ingress/egress rate limit for forwarding packets on the port or LAG. If no port or LAG is specified, it displays the upper ingress/egress rate limit for all ports or LAGs.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the ingress-rate as 5120 Kbps and egress-rate as 1024 Kbps for port 1/0/5:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#bandwidth ingress 5120 **egress** 1024

Switch(config-if)#show bandwidth interface gigabitEthernet 1/0/5

Port	IngressRate(Kbps)	EgressRate(Kbps)	LAG
---	---	---	---

Gi1/0/5	5120	1024	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.2 Configuring Storm Control

Follow these steps to configure the upper rate limit on the port for forwarding broadcast packets, multicast packets and unknown unicast frames:

Step 1	**configure** Enter global configuration mode
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**storm-control rate-mode {**kbps **|** ratio | pps**}** Specify the Rate Mode for the broadcast threshold, multicast threshold and UL-Frame threshold on the desired port. kbps: The switch will limit the maximum speed of the specific kinds of traffic in kilo-bits per second. ratio: The switch will limit the percentage of bandwidth utilization for specific kinds of traffic. pps: The switch will limit the maximum number of packets per second for specific kinds of traffic. Note: pps is only available on certain devices.
Step 4	**storm-control broadcast** *rate* Specify the upper rate limit for receiving broadcast packets. The broadcast traffic exceeding the limit will be processed according to the Action configurations. *rate*: Specify the upper rate limit for receiving broadcast packets. The valid values differ among different rate modes. For kbps, the rate ranges from 1 to 1000000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate ranges from 1 to 1488000 packets per second.
Step 5	**storm-control multicast** *rate* Specify the upper rate limit for receiving multicast packets. The multicast traffic exceeding the limit will be processed according to the Action configurations. *rate*: Specify the upper rate limit for receiving multicast packets. The valid values differ among different rate modes. For kbps, the rate ranges from 1 to 1000000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate ranges from 1 to 1488000 packets per second.

Step6	**storm-control unicast** *rate* Specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations. *rate*: Specify the upper rate limit for receiving unknown unicast frames. The valid values differ among different rate modes. For kbps, the rate ranges from 1 to 1000000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate ranges from 1 to 1488000 packets per second.
Step 7	**storm-control exceed {**drop **|** shutdown**} [recover-time** *time***]** Specify the action and the recover time. The switch will perform the action when the traffic exceeds its corresponding limit. By default, it is drop. drop**:** Set the Action as Drop. The port will drop the subsequent packets when the traffic exceeds the limit. shutdown**:** Set the Action as Shutdown. The port will be shutdown when the traffic exceeds the limit. *time*: Specify the recover time for the port. It takes effect only when the action is set as shutdown. The valid values are from 0 to 3600 and the default value is 0. When the port is shutdown, it can recover to its normal state after the recover time passed. If the recover time is specified as 0, which means the port will not recover to its normal state automatically and you can recover the port manually.
Step 8	**storm-control recover** (Optional) Recover the port manually. When the recover time is specified as 0, the port will not recover to its normal state automatically. In this condition, you need to use this command to recover the port manually.
Step 9	**show storm-control interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the storm control configurations of the port or LAG. If no port or LAG is specified, it displays the storm control configuration for all ports or LAGs.
Step 10	**end** Return to privileged EXEC mode.
Step 11	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the upper rate limit of broadcast packets as 1024 kbps, Specify the action as shutdown and set the recover time as 10 for port 1/0/5:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#storm-control rate-mode kbps

Switch(config-if)#storm-control broadcast 1024

Switch(config-if)#storm-control exceed shutdown **recover-time** 10

Switch(config-if)#show storm-control interface gigabitEthernet 1/0/5

Port	Rate Mode	BcRate	McRate	UlRate	Exceed	Recover Time	LAG
Gi1/0/5	kbps	1024	0	0	shutdown	10	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

4 Voice VLAN Configuration

To complete the voice VLAN configurations, follow these steps:

1) Create a 802.1Q VLAN
2) Configure OUI addresses
3) Configure Voice VLAN globally
4) Add ports to Voice VLAN

Configuration Guidelines

- Before configuring voice VLAN, you need to create a 802.1Q VLAN for voice traffic. For details about 802.1Q VLAN Configuration, please refer to Configuring 802.1Q VLAN.
- VLAN 1 is a default VLAN and cannot be configured as the voice VLAN.
- Only one VLAN can be set as the voice VLAN on the switch.

4.1 Using the GUI

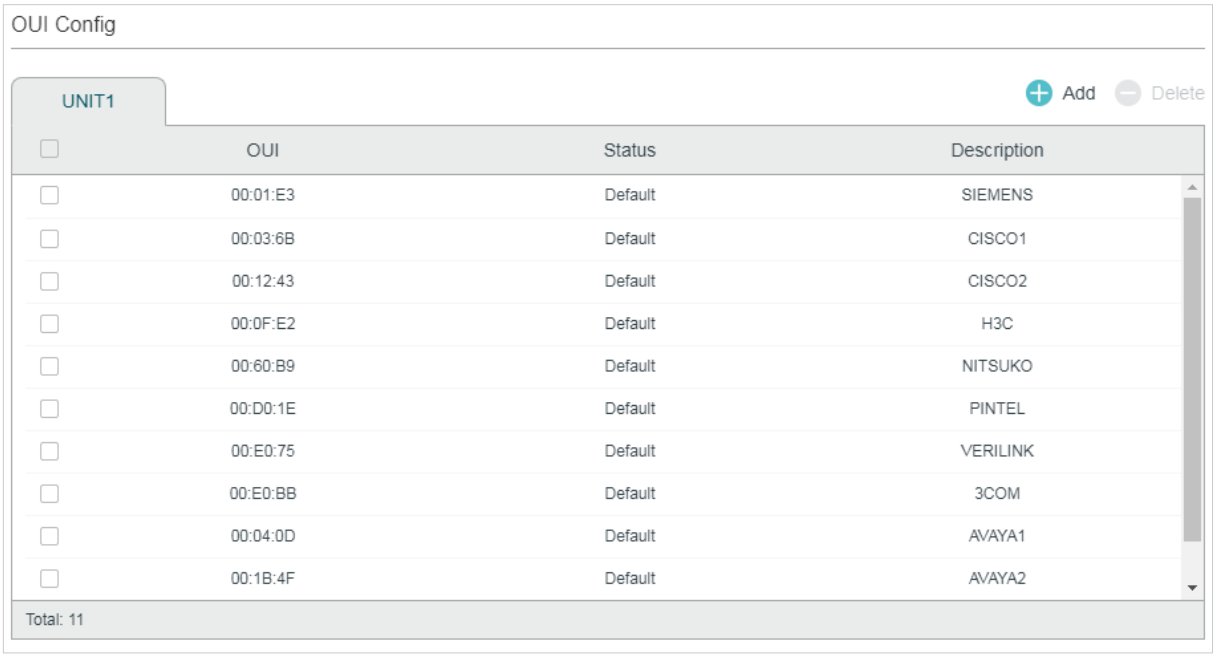
4.1.1 Configuring OUI Addresses

The OUI address is assigned as a unique identifier by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. It is used by the switch to determine whether a packet is a voice packet.

If the OUI address of your voice device is not in the OUI table, you need to add the OUI address to the table.

Choose the menu **QoS > Voice VLAN > OUI Config** to load the following page.

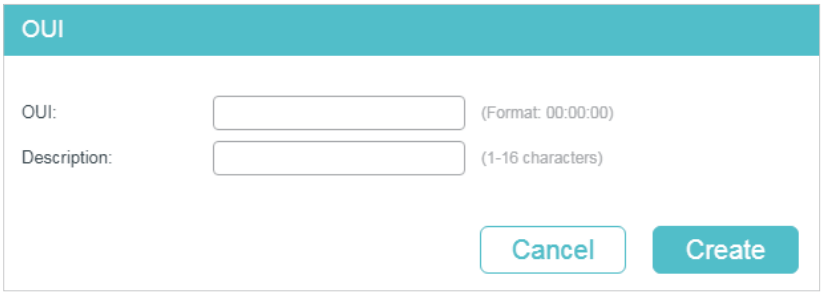
Figure 4-1 Configuring OUI Addresses



Follow these steps to configure the OUI addresses:

1) Click Add to load the following page.

Figure 4-2 Creating an OUI Entry



2) Specify the OUI and the Description.

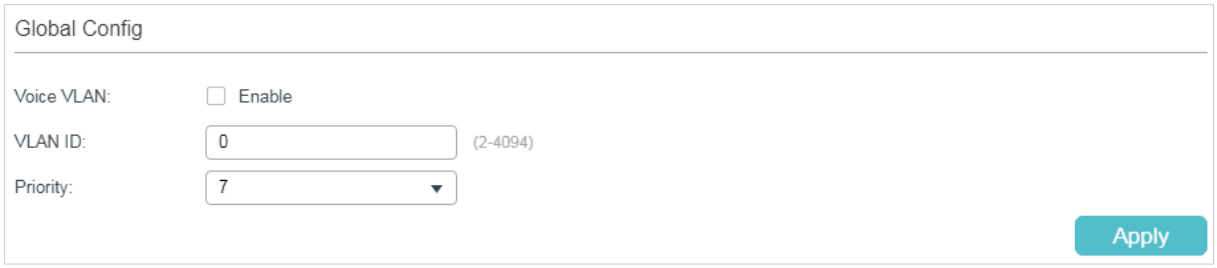
OUI	Enter the OUI address of your voice devices. The OUI address is used by the switch to determine whether a packet is a voice packet. An OUI address is the first 24 bits of a MAC address, and is assigned as a unique identifier by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. If the source MAC address of a packet matches the OUI addresses in the OUI list, the switch identifies the packet as a voice packet and prioritizes it in transmission.
Description	Give an OUI address description for identification.

3) Click **Create**.

4.1.1 Configuring Voice VLAN Globally

Choose the menu **QoS > Voice VLAN > Global Config** to load the following page.

Figure 4-3 Configuring Voice VLAN Globally



Follow these steps to configure voice VLAN globally:

1) Enable the voice VLAN feature and specify the parameters.

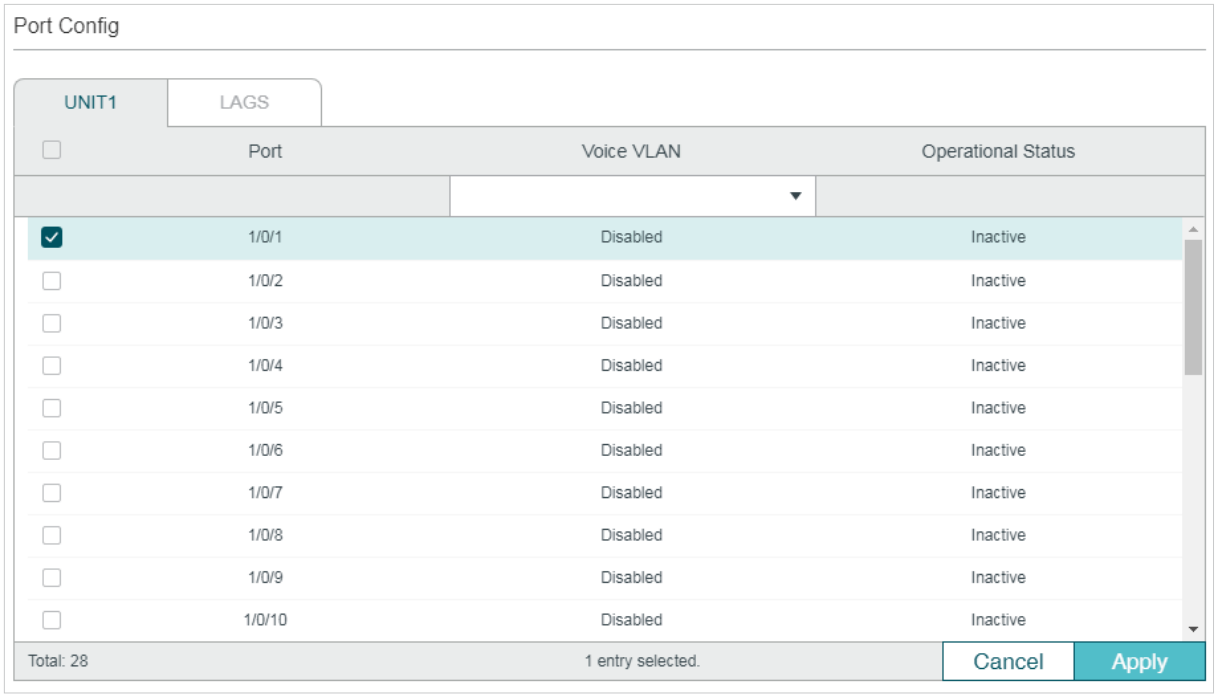
VLAN ID	Specify the 802.1Q VLAN ID to set the 802.1Q VLAN as the voice VLAN.
Priority	Select the priority that will be assigned to voice packets. A bigger value means a higher priority. This is an IEEE 802.1p priority, and you can further configure its scheduler mode in Class of Service if needed.

2) Click **Apply**.

4.1.1 Adding Ports to Voice VLAN

Choose the menu **QoS > Voice VLAN > Port Config** to load the following page.

Figure 4-4 Adding Ports to Voice VLAN



Follow these steps to configure voice VLAN globally:

1) Select the desired ports and choose Enable in Voice VLAN filed.

Voice VLAN	Select Enable to enable the voice VLAN feature on ports and add the desired ports to Voice VLAN.

Optional Status	Displays the state of the Voice VLAN on the corresponding port. **Active:** Indicates that Voive VLAN function is enabled on the port. **Inactive:** Indicates that Voive VLAN function is disabled on the port.

2) Click **Apply**.

4.2 Using the CLI

Follow these steps to configure voice VLAN:

Step 1	**configure** Enter global configuration mode.
Step 2	**show voice vlan oui-table** Check whether the OUI address of your voice device is in the OUI table. The OUI address is used by the switch to determine whether a packet is a voice packet. An OUI address is the first 24 bits of a MAC address, and is assigned as a unique identifier by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. If the source MAC address of a packet matches the OUI addresses in the OUI list, the switch identifies the packet as a voice packet and prioritizes it in transmission.
Step 3	**voice vlan oui** *oui-prefix* **oui-desc** *string* If the OUI address of your voice device is not in the OUI table, add the OUI address to the table. *oui-prefix*: Enter the OUI address for your voice device in the format of XX:XX:XX. *string*: Give an OUI address description for identification. It contains 16 characters at most.
Step 4	**voice vlan** *vid* Enable the voice VLAN feature and specify an existing 802.1Q VLAN as the voice VLAN. *vid:* Enter the 802.1Q VLAN ID to set the 802.1Q VLAN as the voice VLAN.
Step 5	**voice vlan priority** *pri* Specify the priority that will be assigned to voice packets. *pri:* Enter the priority that will be assigned to voice packets. A bigger value means a higher priority. The valid values are from 0 to 7 and the default value is 7. This is an IEEE 802.1p priority, and you can further configure its scheduler mode in Class of Service if needed.
Step 6	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 7	**voice vlan** Enable the voice VLAN feature on ports and add the desired ports to voice VLAN.
Step 8	**show voice vlan interface** Verify the voice VLAN configuration information.

Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to show the OUI table, set VLAN 8 as voice VLAN, set the priority as 6 and enable voice VLAN feature on port 1/0/3:

Switch#configure

Switch(config)#show voice vlan oui-table

00:01:E3 Default SIEMENS

00:03:6B Default CISCO1

00:12:43 Default CISCO2

00:0F:E2 Default H3C

00:60:B9 Default NITSUKO

00:D0:1E Default PINTEL

00:E0:75 Default VERILINK

00:E0:BB Default 3COM

00:04:0D Default AVAYA1

00:1B:4F Default AVAYA2

00:04:13 Default SNOM

Switch(config)#voice vlan 8

Switch(config)#voice vlan priority 6

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#voice vlan

Switch(config-if)#show voice vlan interface

Voice VLAN ID 8

Priority 6

Interface	Voice VLAN Mode	Operational Status	LAG
---	---	---	---
Gi1/0/1	disabled	Down	N/A
Gi1/0/2	disabled	Down	N/A

Gi1/0/3	enabled	Up	N/A
Gi1/0/4	disabled	Down	N/A
Gi1/0/5	disabled	Down	N/A

...

Switch(config-if)#end

Switch#copy running-config startup-config

5 Auto VoIP Configuration

Configuration Guidelines

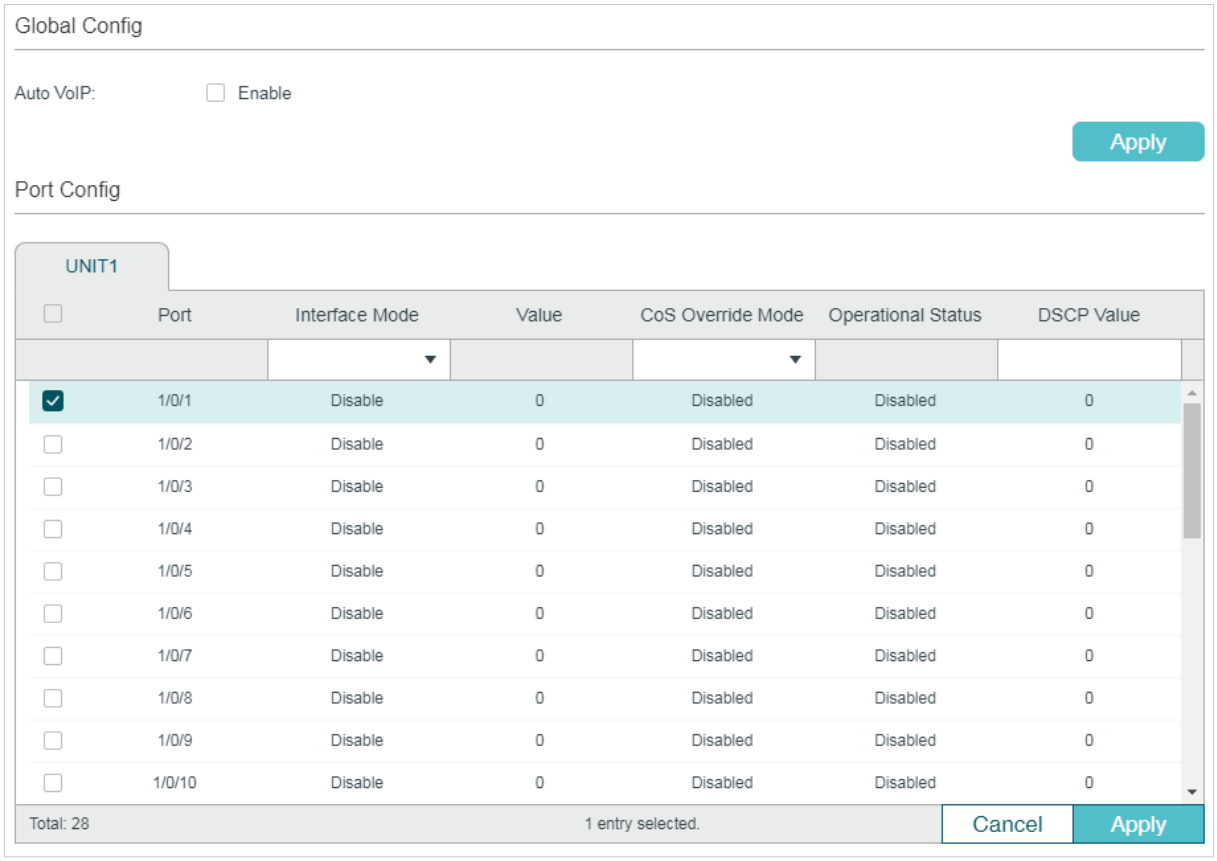
- Before configuring Auto VoIP, you need to enable LLDP-MED on ports and configure the relevant parameters. For details about LLDP-MED configuration, please refer to Configuring LLDP.

- Auto VoIP provide flexible solutions for optimizing the voice traffic. It can work with other features such as VLAN and Class of Service to process the voice packets with specific fields. You can choose and configure Auto VoIP and other features according to your needs.

5.1 Using the GUI

Choose the menu **QoS > Auto VoIP** to load the following page.

Figure 5-1 Configuring Auto VoIP



Follow these steps to configure the OUI addresses:

1) In the **Global Config** section, enable the Auto VoIP function gloablly.
2) In the **Port Config** section, select the desired and configure the parameters.

Interface Mode	Select the interface mode for the port. **Disable:** Disable the Auto VoIP function on the corresponding port. **None:** Allow the voice devices to use its own configuration to send voice traffic. **VLAN ID:** The voice devices will send voice packets with desired VLAN tag. If this mode is selected, it is necessary to specify the VLAN ID in the Value field. In addition, you need to configure the 802.1Q VLAN to ensure the corresponding ports can forward the packets normally. **Dot1p:** The voice devices will send voice packets with desired 802.1p priority. If this mode is selected, it is necessary to specify 802.1p priority in the Value field. In addition, you can configure the Class of Service to make the switch process the packets according to the 802.1p priority. **Untagged:** The voice devices will send untagged voice packets.
Value	Enter the value of VLAN ID or 802.1p priority for the port according to the Interface Mode configurations.
CoS Override Mode	Enable or disable the Class of Service override mode. **Enabled:** Enable CoS override. The switch will ignore Class of Service settings and put the packets in TC-5 directly. **Disabled:** Disable CoS override. The switch will then put the voice packets in the corresponding TC queue according to Class of Service settings.
Operational Status	Displays the operating status of the Voice VLAN feature on the interface. To make it enabled, you must enable the Voice VLAN both globally and on the interface.
DSCP Value	Enter the value of DSCP priority. The voice device will send the packets with the corresponding DSCP value. In addition, you can configure the Class of Service to make the switch process the packets according to the DSCP priority.

3) Click **Apply**.

5.2 Using the CLI

Follow these steps to configure Auto VoIP:

Step 1	**configure** Enter global configuration mode.
Step 2	**auto-voip** Enable Auto VoIP globally.

Step 3 **interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}**

Enter interface configuration mode.

Step 4 Select the interface mode for the port.

no auto-voip

Specify the interface mode as disabled, which means the Auto VoIP function is disabled on the corresponding port.

auto-voip none

Specify the interface mode as none. In this mode, the switch allows the voice devices to use its own configuration to send voice traffic.

auto-voip *vlan-id*

Specify the interface mode as VLAN ID. In this mode, the voice devices will send voice packets with desired VLAN tag. If this mode is selected, it is necessary to specify the 802.1Q VLAN ID. The valid values are from 1 to 4093.

In addition, you need to configure the 802.1Q VLAN to ensure the corresponding ports can forward the packets normally.

auto-voip dot1p *dot1p*

Specify the interface mode as dot1p. In this mode, the voice devices will send voice packets with desired 802.1p priority. If this mode is selected, it is necessary to specify 802.1p priority. The valid values are from 0 to 7.

In addition, you can configure the Class of Service to make the switch process the packets according to the 802.1p priority.

auto-voip untagged

Specify the interface mode as untagged. In this mode, the voice devices will send untagged voice packets.

Step 5 **auto-voip data priority {**trust **|** untrust**}**

Enable or disable the Class of Service override mode. By default, it is trust, which means the Class of Service override mode is disabled.

trust: In this mode, The switch will then put the voice packets in the corresponding TC queue according to Class of Service settings.

untrust: In this mode, The switch will ignore Class of Service settings and put the packets in TC-5 directly.

Step 6 **auto-voip dscp** *value*

Specify the value of DSCP priority. The voice device will send the packets with the corresponding DSCP value.

In addition, you can configure the Class of Service to make the switch process the packets according to the DSCP priority.

value: Enter the value of DSCP priority. The valid values are from 0 to 63 and the default value is 0.

Step 7	**show auto-voip** Verify the global state of Auto VoIP.
Step 8	**show auto-voip interface** Verify the Auto VoIP configuration information of ports.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the interface mode as dot1p, specify the 802.1p priority as 4, specify the DSCP priority as 10 and enable the CoS override mode for port 1/0/3:

Switch#configure

Switch(config)#auto-voip

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#auto-voip dot1p 4

Switch(config-if)#auto-voip dscp 10

Switch(config-if)#auto-voip data priority untrust

Switch(config-if)#show auto-voip

Administrative Mode: Enabled

Switch(config-if)#show auto-voip interface

Interface.Gi1/0/1

Auto-VoIP Interface Mode. Disabled

Auto-VoIP COS Override. False

Auto-VoIP DSCP Value. 0

Auto-VoIP Port Status. Disabled

Interface.Gi1/0/2

Auto-VoIP Interface Mode. Disabled

Auto-VoIP COS Override. False

Auto-VoIP DSCP Value. 0

Auto-VoIP Port Status. Disabled

Interface.Gi1/0/3

Auto-VoIP Interface Mode. Enabled

Auto-VoIP Priority. 4

Auto-VoIP COS Override. True

Auto-VoIP DSCP Value. 10

Auto-VoIP Port Status. Enabled

...

Switch(config-if)#end

Switch#copy running-config startup-config

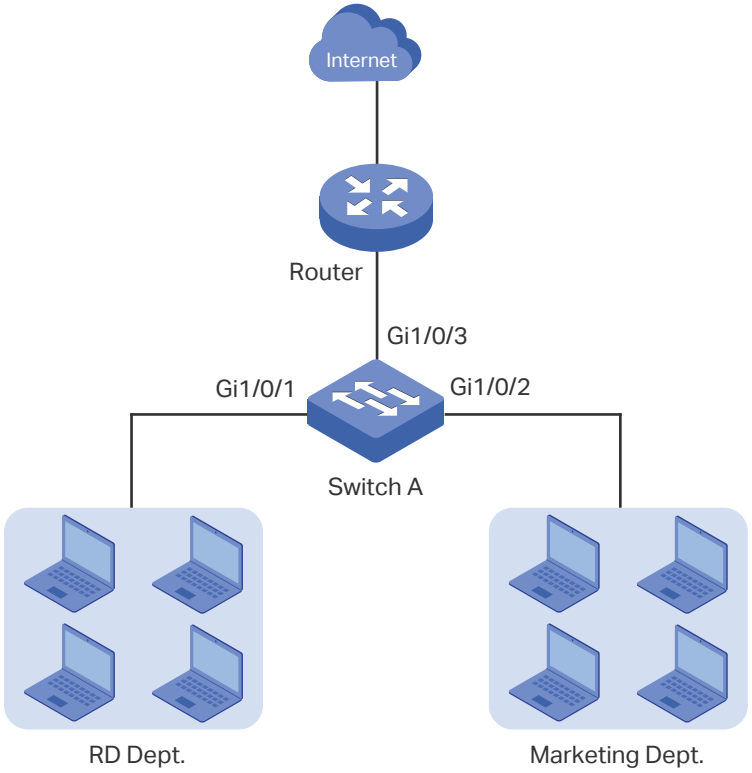
6 Configuration Examples

6.1 Example for Class of Service

6.1.1 Network Requirements

As shown below, both RD department and Marketing department can access the internet. When congestion occurs, the traffic from two departments can both be forwarded and the traffic from the Marketing department should take precedence.

Figure 6-1 QoS Application Topology



6.1.2 Configuration Scheme

To implement this requirement, you can configure Port Priority to put the packets from the Marketing department into the queue with the higher priority than the packets from the RD department.

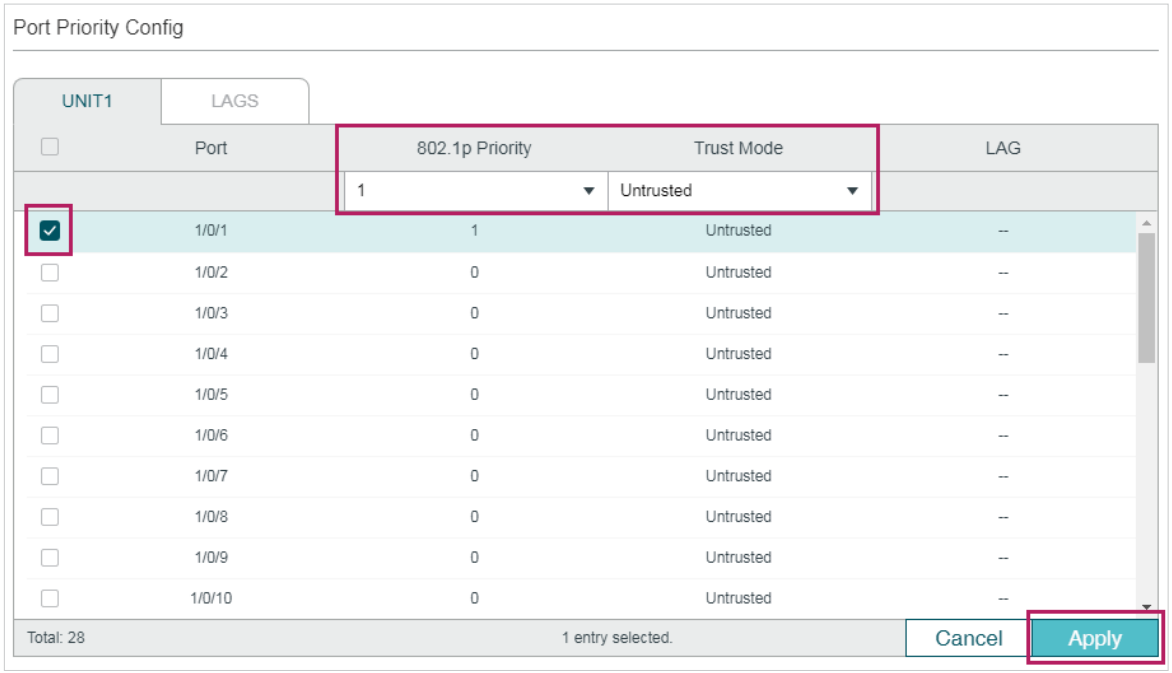
1) Configure the trust mode of port 1/0/1 and port 1/0/2 as untrusted and map the ports to different queues.
2) Set the scheduler type of the queues as weighted for port 1/0/3 and specify the queue weight to make the traffic from the Marketing department take precedence.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

6.1.3 Using the GUI

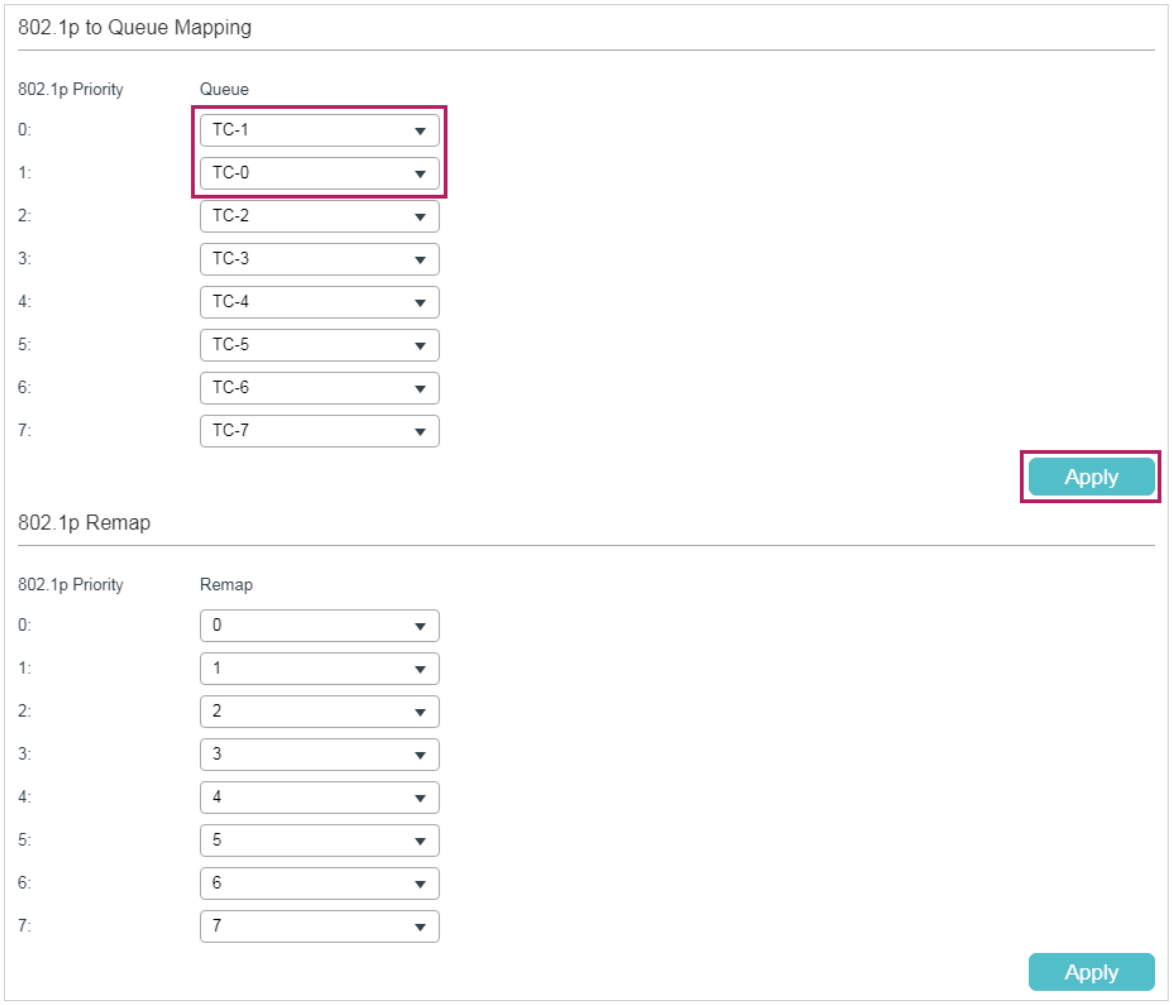
1) Choose the menu **QoS > Class of Service > Port Priority** to load the following page. Set the trust mode of port 1/0/1 and 1/0/2 as untrusted. Specify the 802.1p priority of port 1/0/1 as 1 and specify the 802.1p priority of port 1/0/2 as 0. Click **Apply**.

Figure 6-2 Configuring Port Priority



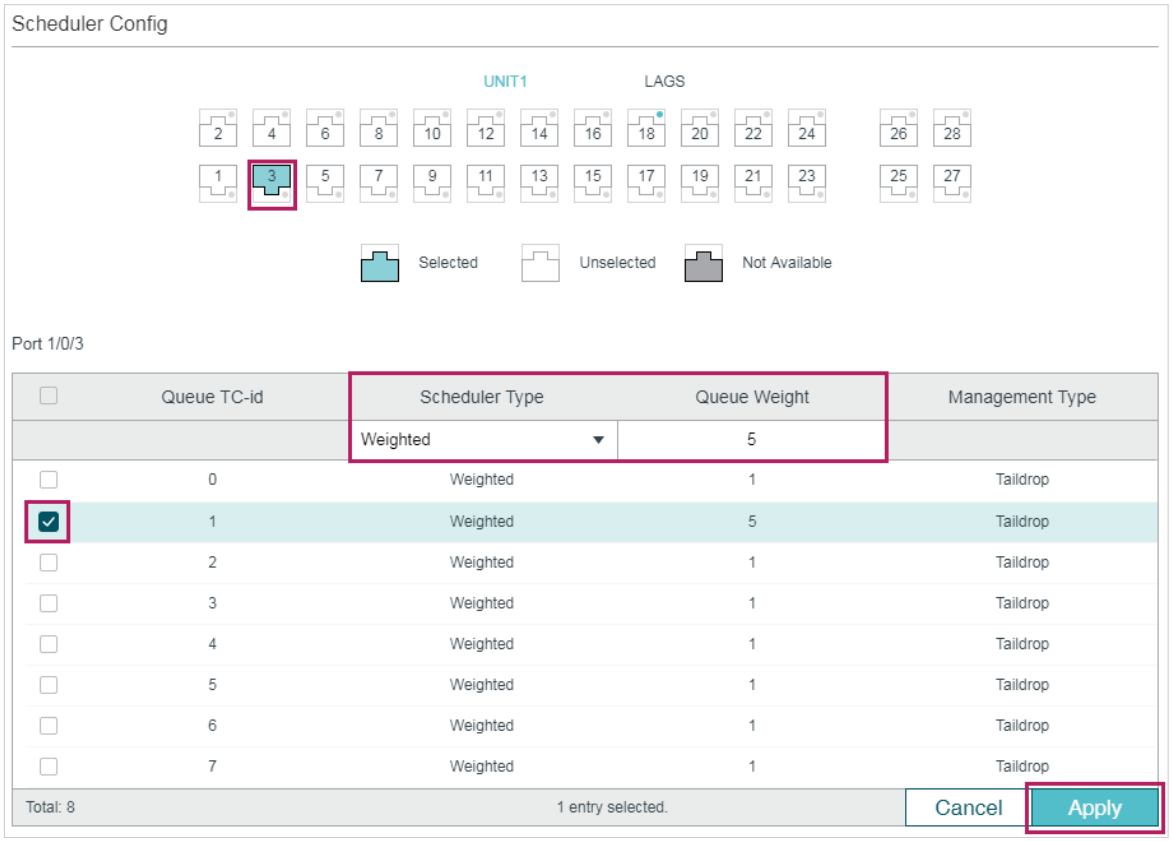
2) Choose the menu **QoS > Class of Service > 802.1p Priority** to load the following page. Map the 802.1p priority 0 to TC-1 and map the 802.1p priority 1 to TC-0. Click **Apply**.

Figure 6-3 Configuring the 802.1p to Queue Mappings



3) Choose the menu **QoS > Class of Service > Scheduler Settings** to load the following page. Select the port 1/0/3 and set the scheduler type of TC-0 and TC-1 as Weighted. Specify the queue weight of TC-0 as 1 and specify the queue weight of TC-1 as 5. Click **Apply**.

Figure 6-4 Configuring the Egress Queue



4) Click Save to save the settings.

6.1.4 Using the CLI

1) Set the trust mode of port 1/0/1 as untrusted and specify the 802.1p priority as 1.

   Switch_A#configure

   Switch_A(config)#interface gigabitEthernet 1/0/1

   Switch_A(config-if)#qos trust mode untrust

   Switch_A(config-if)#qos port-priority 1

   Switch_A(config-if)#exit

2) Set the trust mode of port 1/0/2 as untrusted and specify the 802.1p priority as 0.

   Switch_A(config)#interface gigabitEthernet 1/0/2

   Switch_A(config-if)#qos trust mode untrust

   Switch_A(config-if)#qos port-priority 0

   Switch_A(config-if)#exit

3) Map the 802.1p priority 0 to TC-1 and map the 802.1p priority 1 to TC-0.

   Switch_A(config)#qos cos-map 0 1

   Switch_A(config)#qos cos-map 1 0

4) Set the scheduler type of TC-0 and TC-1 as Weighted for egress port 1/0/3. Specify the queue weight of TC-0 as 1 and specify the queue weight of TC-1 as 5.

```
Switch_A(config)#interface gigabitEthernet 1/0/3
Switch_A(config-if)#qos queue 0 mode wrr weight 1
Switch_A(config-if)#qos queue 1 mode wrr weight 5
Switch_A(config-if)#end
Switch_A#copy running-config startup-config
```

Verify the configurations

Verify the trust mode of the port:

```
Switch_A#show qos trust interface
Port       Trust Mode      LAG
--------   ---------       --------
Gi1/0/1    untrust         N/A
Gi1/0/2    untrust         N/A
Gi1/0/3    untrust         N/A
Gi1/0/4    untrust         N/A
...
```

Verify the port to 802.1p mappings:

```
Switch_A#show qos port-priority interface
Port       CoS Value       LAG
--------   ---------       --------
Gi1/0/1    CoS  1          N/A
Gi1/0/2    CoS  0          N/A
Gi1/0/3    CoS  0          N/A
Gi1/0/4    CoS  0          N/A
...
```

Verify the 802.1p to queue mappings:

```
Switch_A#show qos cos-map
---------------+-----+-----+-----+-----+-----+-----+----+----
Dot1p Value  |0     |1     |2     |3     |4     |5     |6    |7
---------------+-----+-----+-----+-----+-----+-----+----+----
TC              |TC1  |TC0  |TC2  |TC4  |TC4 |TC5  |TC6 |TC7
---------------+-----+-----+-----+-----+-----+-----+----+----
```

Verify the scheduler mode of the egress port:

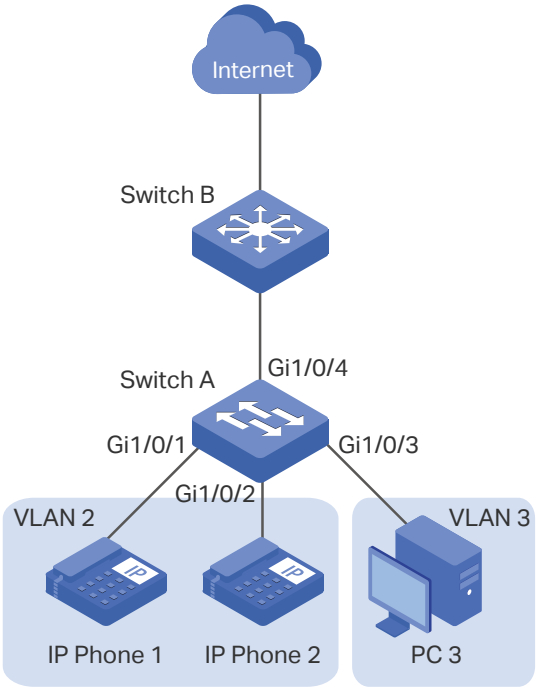
```
Switch _A#show qos queue interface gigabitEthernet 1/0/3
Gi1/0/3----LAG: N/A
Queue  Schedule Mode  Weight
-----     ----------          -----
TC0      WRR                 1
TC1      WRR                 5
TC2      WRR                 1
TC3      WRR                 1
TC4      WRR                 1
TC5      WRR                 1
TC6      WRR                 1
TC7      WRR                 1
```

6.2 Example for Voice VLAN

6.2.1 Network Requirements

As shown below, the company plans to install IP phones in the office area. To ensure the good voice quality, IP phones and the computers will be connected to the different ports of the switch, and the voice traffic requires a higher priority than the data traffic.

Figure 6-5 Voice VLAN Application Topology



6.2.2 Configuration Scheme

To implement this requirement, you can configure Voice VLAN to ensure that the voice traffic can be transmitted in the same VLAN and the data traffic is transmitted in another VLAN. In addition, specify the priority to make the voice traffic can take precedence when the congestion occurs.

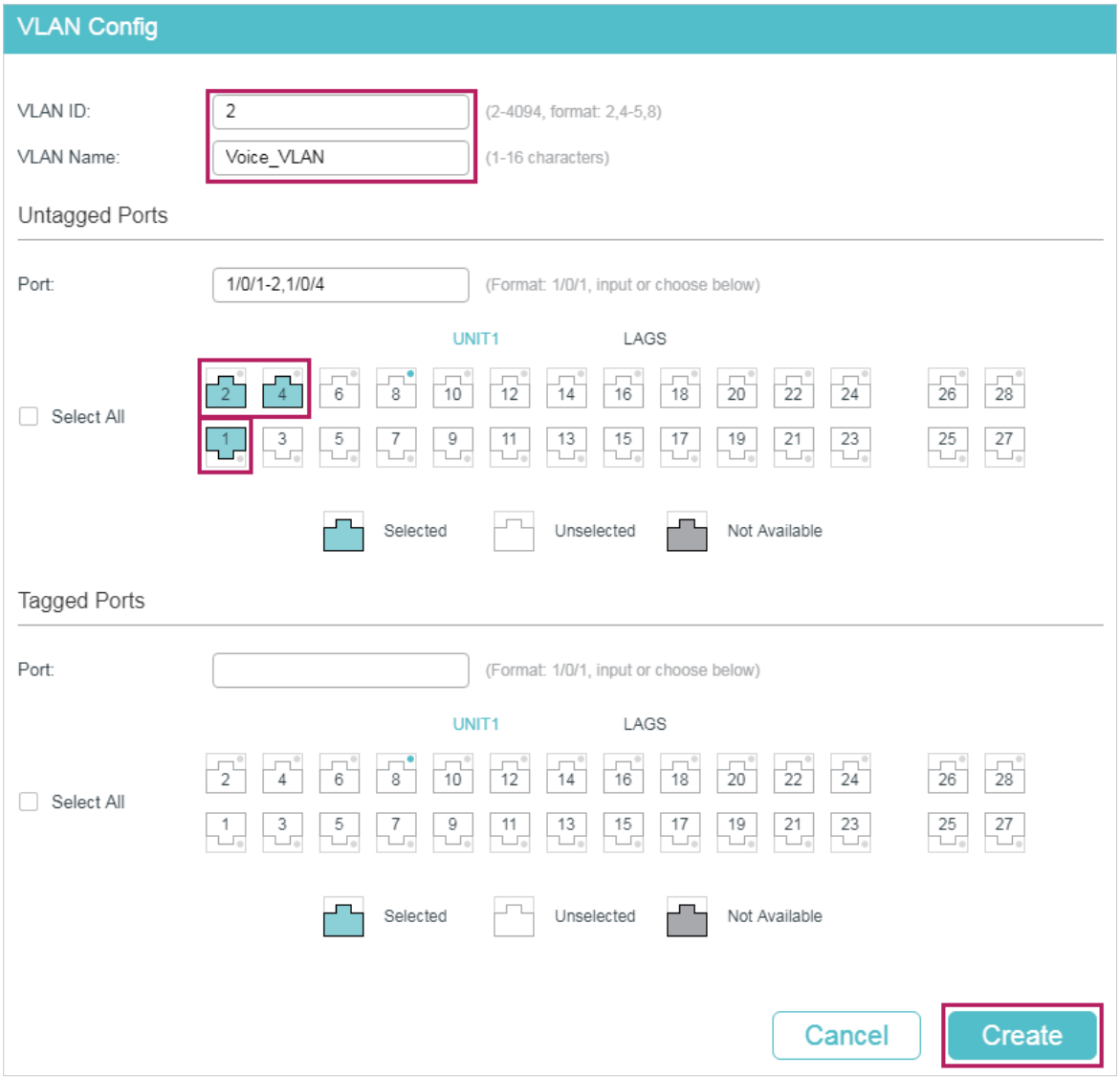
1) Configure 802.1Q VLAN for port 1/0/1, port 1/0/2. port 1/0/3 and port 1/0/4.
2) Configure Voice VLAN feature on port 1/0/1 and port 1/0/2.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

6.2.3 Using the GUI

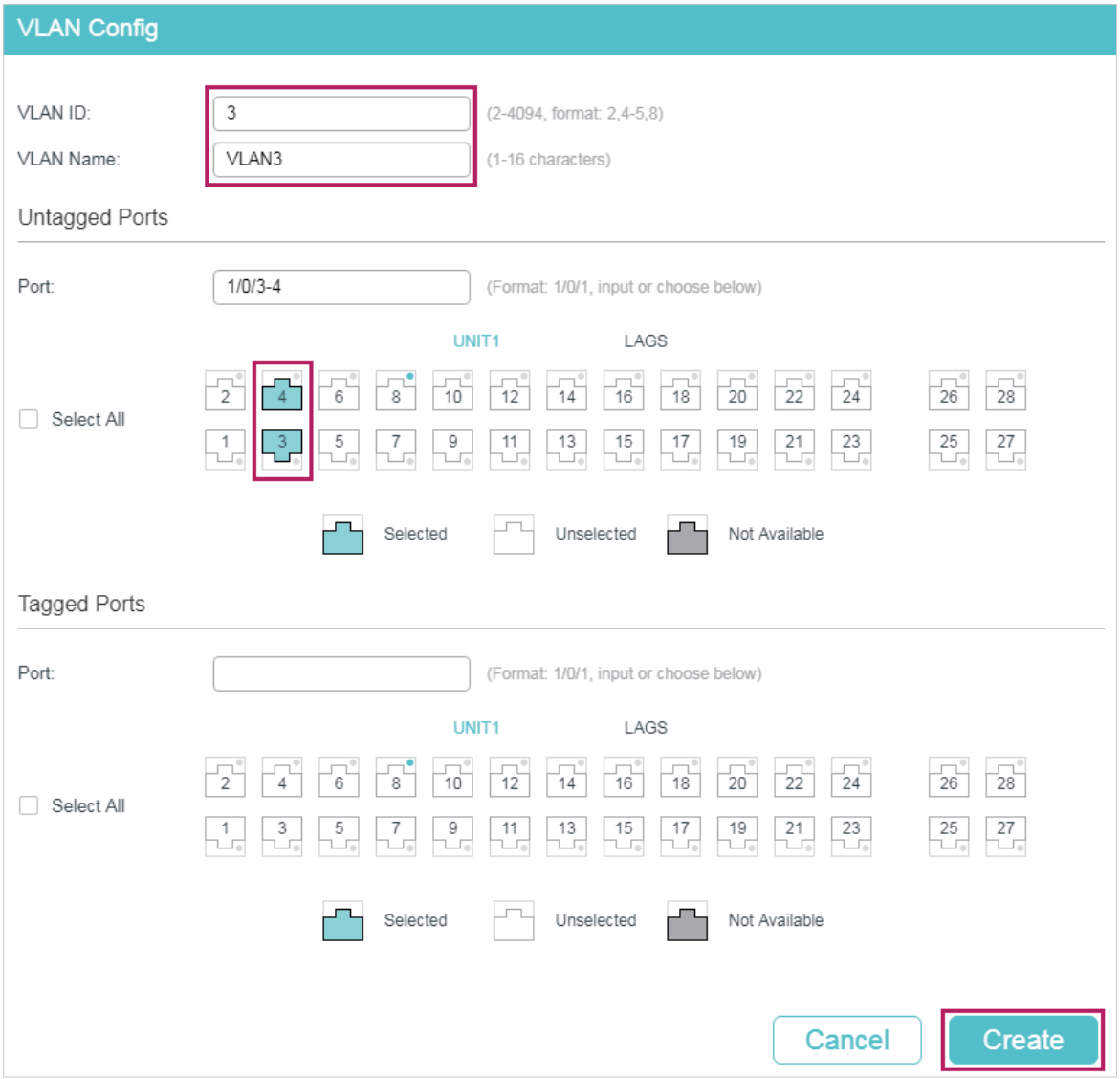
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 2 and add untagged port 1/0/1, port 1/0/2 and port 1/0/4 to VLAN 2. Click **Create**.

Figure 6-6 Configuring VLAN 2



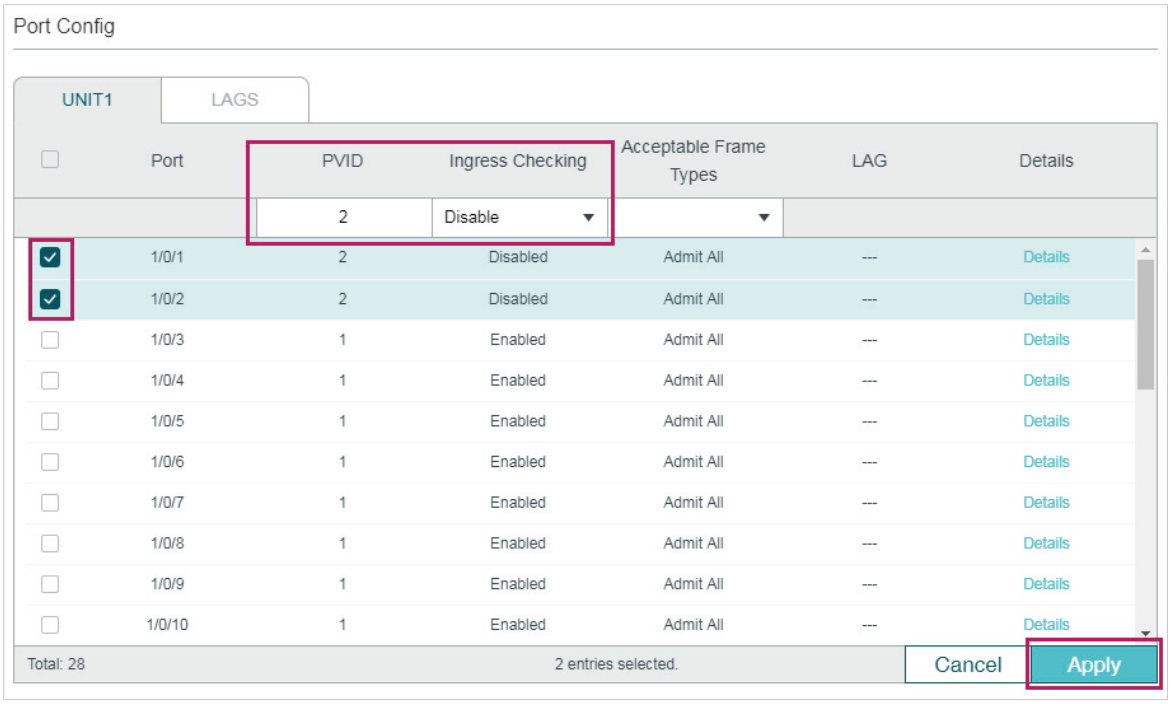
2) Click Add to load the following page. Create VLAN 3 and add untagged port 1/0/3 and port 1/0/4 to VLAN 3. Click **Create**.

Figure 6-7 Configuring VLAN 3



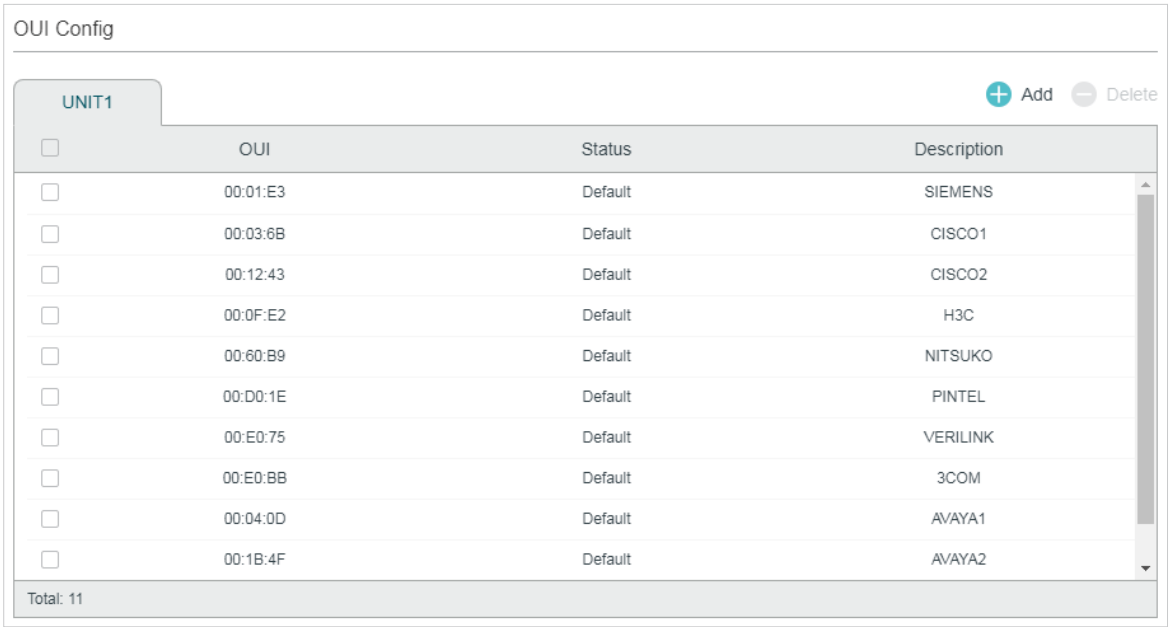
3) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config** to load the following page. Disable the Ingress Checking feature on port 1/0/1 and port 1/0/2 and specify the PVID as 2. Click **Apply**.

Figure 6-8 Specifying the Parameters of the Ports



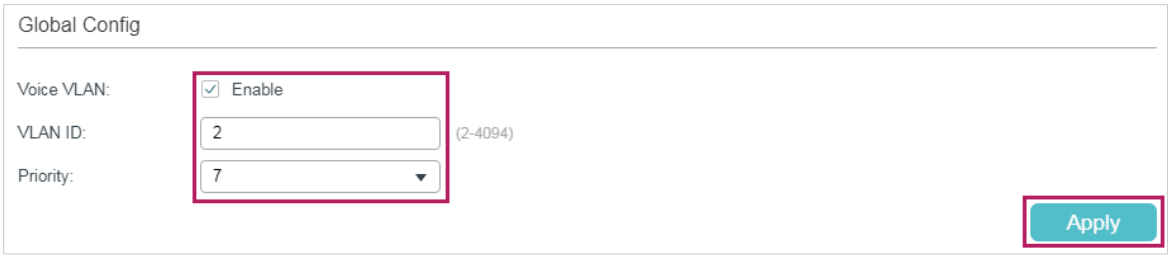
4) Choose the menu **QoS > Voice VLAN > OUI Config** to load the following page. Check the OUI table.

Figure 6-9 Checking the OUI Table



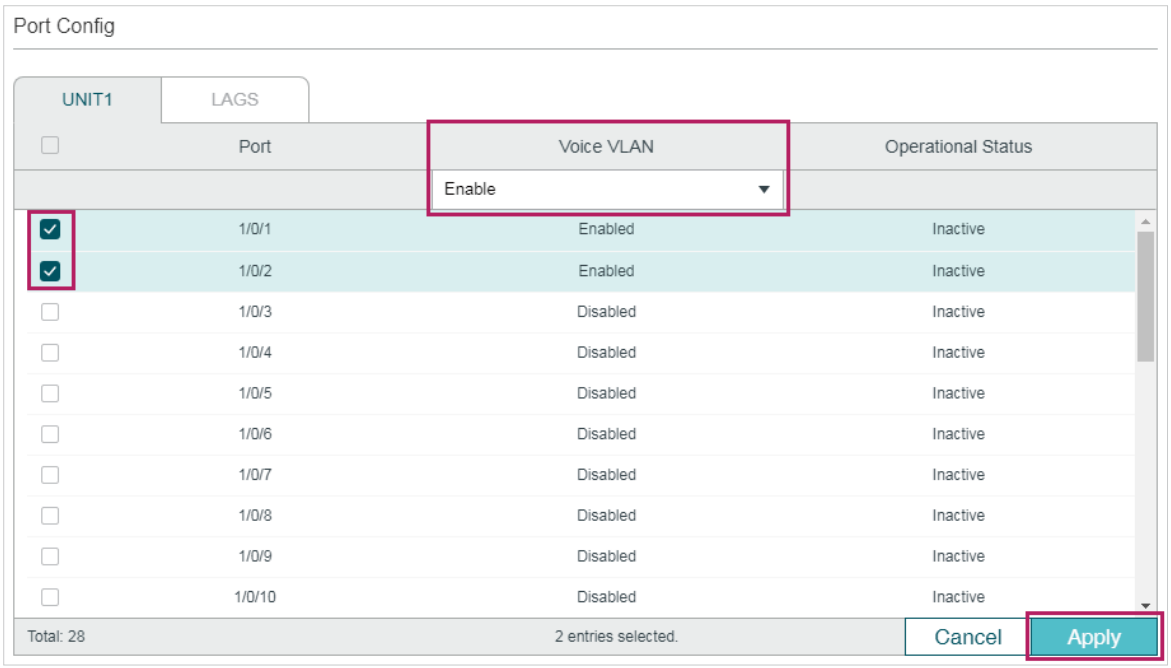
5) Choose the menu **QoS > Voice VLAN > Global Config** to load the following page. Enable Voice VLAN globally. Specify the VLAN ID as 2 and set the priority as 7. Click **Apply**.

Figure 6-10 Configuring Voice VLAN Globally



6) Choose the menu **QoS > Voice VLAN > Port Config** to load the following page. Enable Voice VLAN on port 1/0/1 and port 1/0/2. Click **Apply**.

Figure 6-11 Enabling Voice VLAN on Ports



7) Click Save to save the settings.

6.2.4 Using the CLI

1) Create VLAN 2 and add untagged port 1/0/1, port 1/0/2 and port 1/0/4 to VLAN 2.

Switch_A#configure

Switch_A(config)#vlan 2

Switch_A(config-vlan)#name VoiceVLAN

Switch_A(config-vlan)#exit

Switch_A(config)#interface gigabitEthernet 1/0/1

Switch_A(config-if)#switchport general allowed vlan 2 untagged

Switch_A(config-if)#exit

Switch_A(config)#interface gigabitEthernet 1/0/2

Switch_A(config-if)#switchport general allowed vlan 2 untagged

Switch_A(config-if)#exit

Switch_A(config)#interface gigabitEthernet 1/0/4

Switch_A(config-if)#switchport general allowed vlan 2 untagged

Switch_A(config-if)#exit

2) Create VLAN 3 and add untagged port 1/0/3 and port 1/0/4 to VLAN 3.

Switch_A(config)#vlan 3

Switch_A(config-vlan)#name VLAN3

Switch_A(config-vlan)#exit

Switch_A(config)#interface gigabitEthernet 1/0/3

Switch_A(config-if)#switchport general allowed vlan 3 untagged

Switch_A(config-if)#exit

Switch_A(config)#interface gigabitEthernet 1/0/4

Switch_A(config-if)#switchport general allowed vlan 3 untagged

Switch_A(config-if)#exit

3) Disable the Ingress Checking feature on port 1/0/1 and port 1/0/2 and specify the PVID as 2.

Switch_A(config)#interface gigabitEthernet 1/0/1

Switch_A(config-if)#no switchport check ingress

Switch_A(config-if)#switchport pvid 2

Switch_A(config-if)#exit

Switch_A(config)#interface gigabitEthernet 1/0/2

Switch_A(config-if)#no switchport check ingress

Switch_A(config-if)#switchport pvid 2

Switch_A(config-if)#exit

4) Check the OUI table.

Switch(config)#show voice vlan oui

00:01:E3 Default SIEMENS

00:03:6B Default CISCO1

00:12:43 Default CISCO2

00:0F:E2 Default H3C

00:60:B9 Default NITSUKO

00:D0:1E Default PINTEL

00:E0:75 Default VERILINK

00:E0:BB Default 3COM

00:04:0D Default AVAYA1

00:1B:4F Default AVAYA2

00:04:13 Default SNOM

5) Enable Voice VLAN globally. Specify the VLAN ID as 2 and set the priority as 7.

Switch_A(config)#voice vlan 2

Switch_A(config)#voice vlan priority 7

6) Enable Voice VLAN on port 1/0/1 and port 1/0/2.

Switch_A(config)#interface gigabitEthernet 1/0/1

Switch_A(config-if)#voice vlan

Switch_A(config-if)#exit

Switch_A(config)#interface gigabitEthernet 1/0/2

Switch_A(config-if)#voice vlan

Switch_A(config-if)#end

Switch_A#copy running-config startup-config

Verify the configurations

Verify the basic VLAN configuration:

Switch_A(config)#show vlan brief

VLAN	Name	Status	Ports
1	System-VLAN	active	Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, Gi1/0/9, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28

```
2       VoiceVLAN       active      Gi1/0/1, Gi1/0/2, Gi1/0/4
3       VLAN3           active      Gi1/0/3, Gi1/0/4
```

Verify the Voice VLAN configuration:

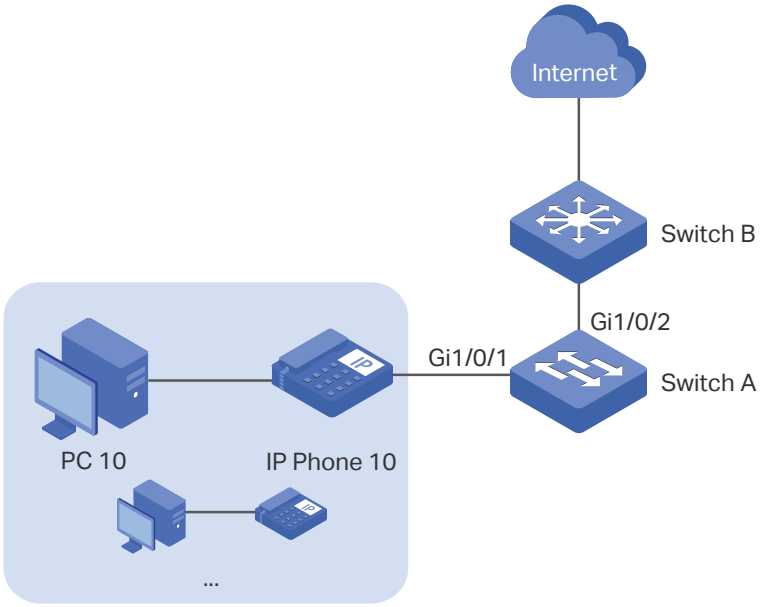
```
Switch_A(config)#show voice vlan interface
Voice VLAN ID           2
Priority                7

Interface    Voice VLAN Mode   Operational Status   LAG
---------    ---------------   ------------------   ---
Gi1/0/1      enabled           Up                   N/A
Gi1/0/2      enabled           Up                   N/A
Gi1/0/3      disabled          Down                 N/A
Gi1/0/4      disabled          Down                 N/A
Gi1/0/5      disabled          Down                 N/A
...
Gi1/0/28     disabled          Down                 N/A
```

6.3 Example for Auto VoIP

6.3.1 Network Requirements

As shown below, the company plans to install IP phones in the office area. IP phones share switch ports used by computers, because no more ports are available for IP phones. To ensure the good voice quality, the voice traffic requires a higher priority than the data traffic.

Figure 6-12 Auto VoIP Application Topology



6.3.2 Configuration Scheme

To optimize voice traffic, configure Auto VoIP and LLDP-MED to instruct IP Phones to send traffic with desired DSCP priority. Voice traffic is put in the desired queue and data traffic is put in other queues according to the Class of Service configurations. Make sure that the voice traffic can take precedence when congestion occurs.

1) Enable the Auto VoIP feature and configure the DSCP value of ports.
2) Configure Class of Service.
3) Enable LLDP-MED and configure the corresponding parameters.

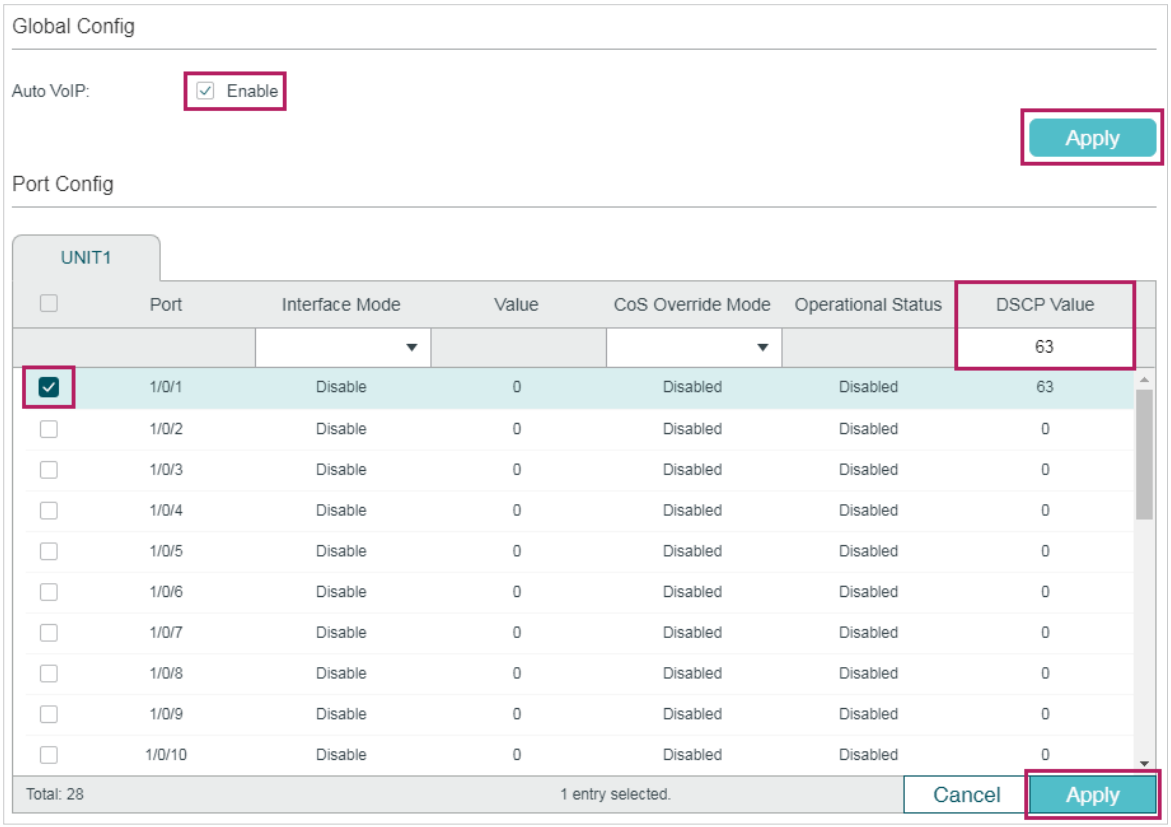
Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

6.3.3 Using the GUI

Auto VoIP configurations for port1/0/1 and other ports connected to the IP phone are the same, the following configuration procedures take port 1/0/1 as example.

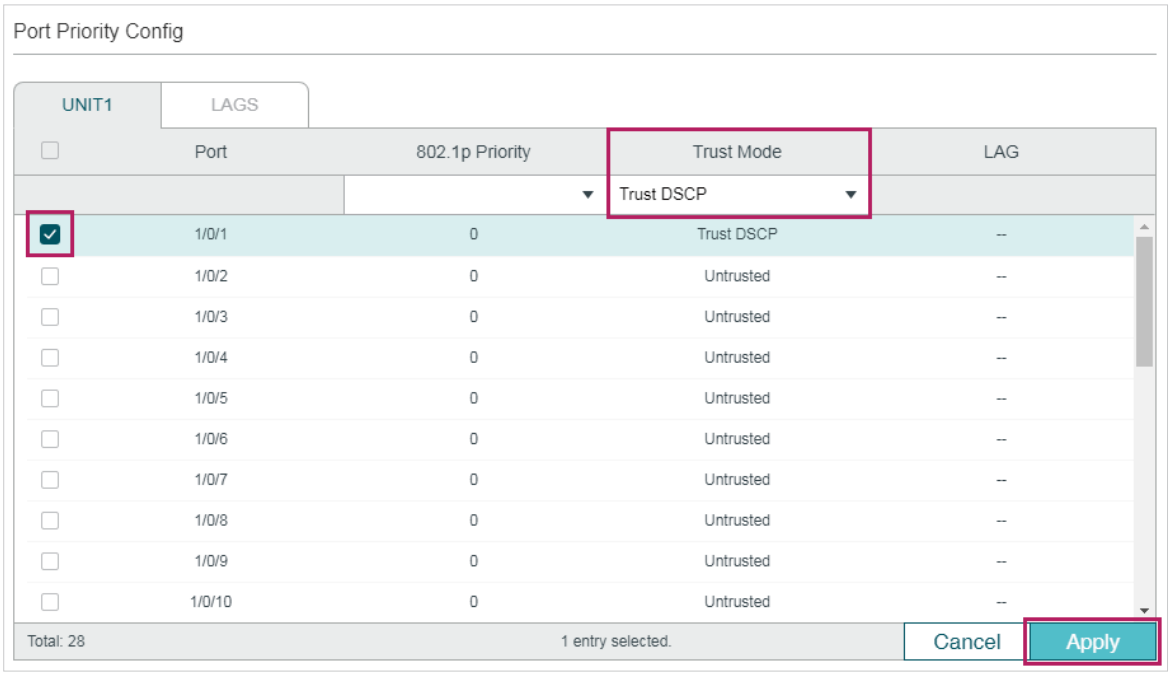
1) Choose the menu **QoS > Auto VoIP** to load the following page. Enable Auto VoIP globally and specify the DSCP value of port 1/0/1 as 63. Click **Apply**.

Figure 6-13 Configuring Auto VoIP



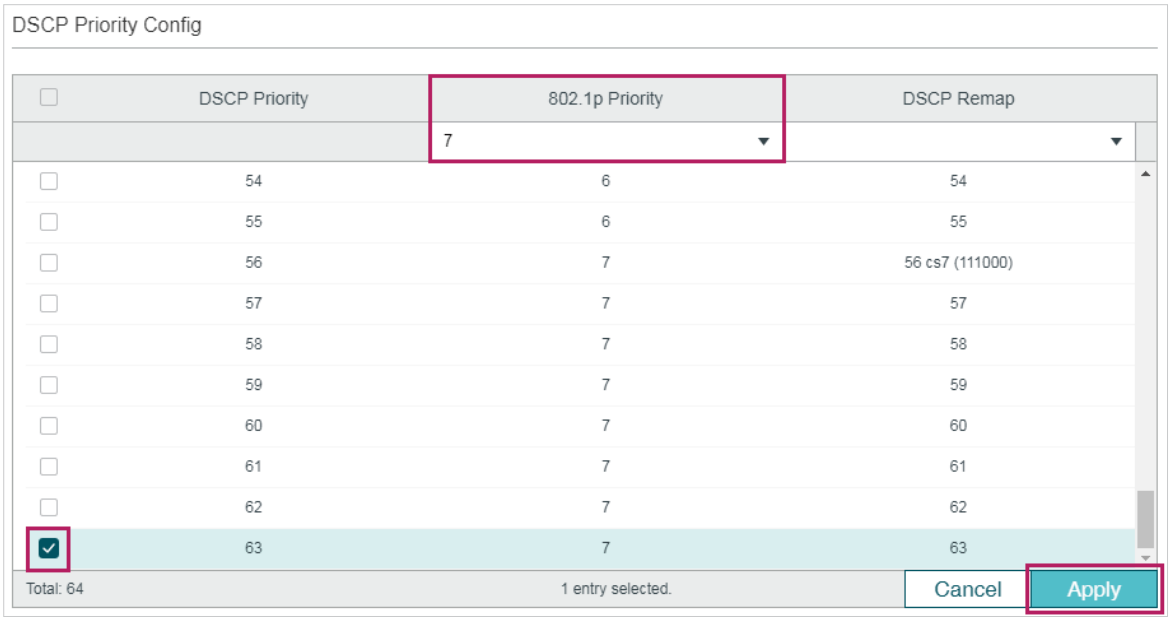
2) Choose the menu **QoS > Class of Service > Port Priority** to load the following page. Set the trust mode of port 1/0/1 as trust DSCP. Click **Apply**.

Figure 6-14 Configuring Port Priority



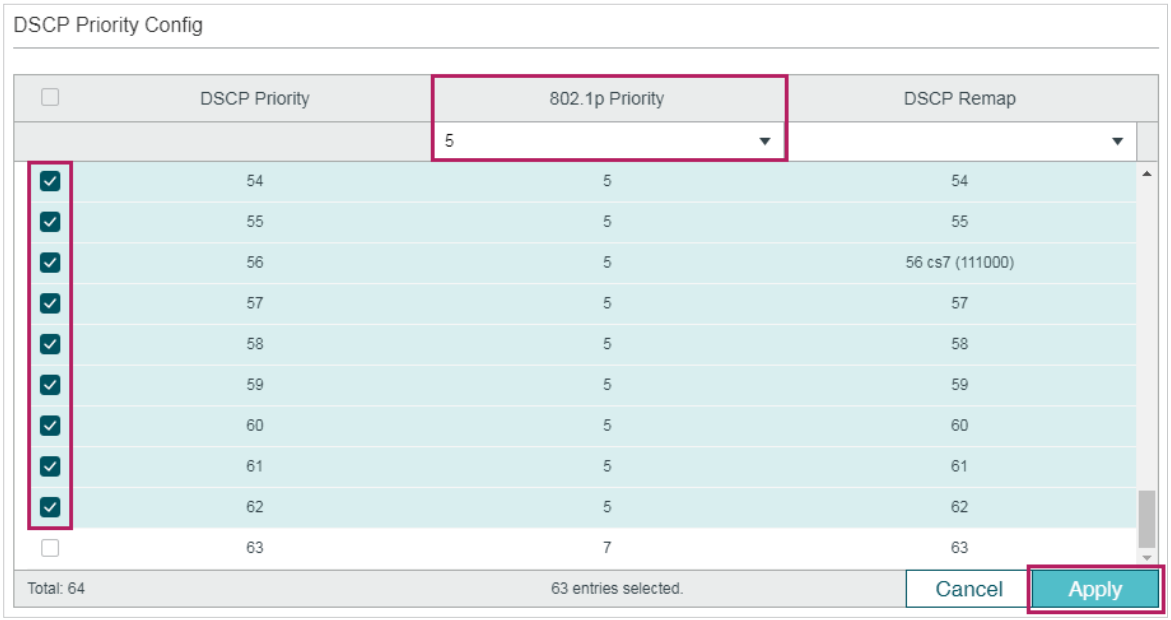
3) Choose the menu **QoS > Class of Service > DSCP Priority** to load the following page. Specify the 802.1p priority as 7 for DSCP priority 63. Click **Apply**.

Figure 6-15 Specifying the 802.1p priority for DSCP priority 63



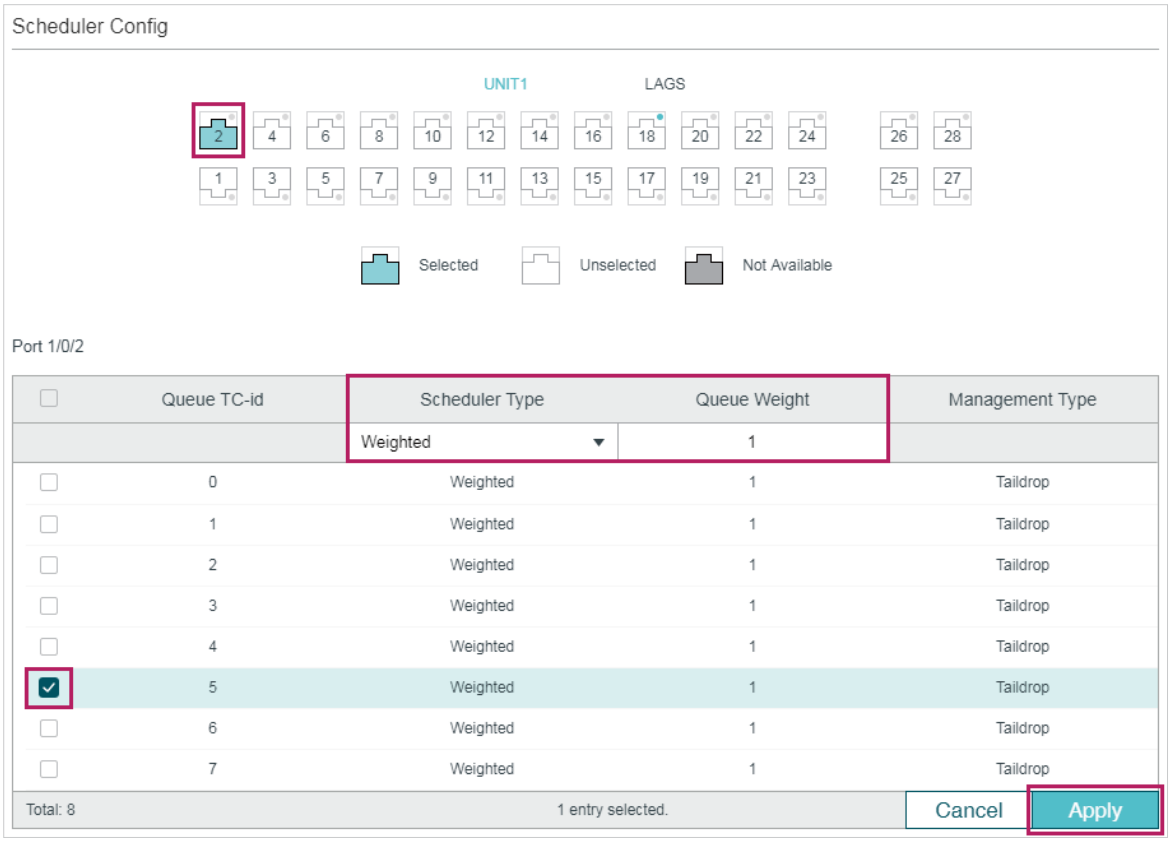
4) Specify the 802.1p priority as 5 for other DSCP priorities. Click **Apply**.

Figure 6-16 Specifying the 802.1p priority for Other DSCP priorities



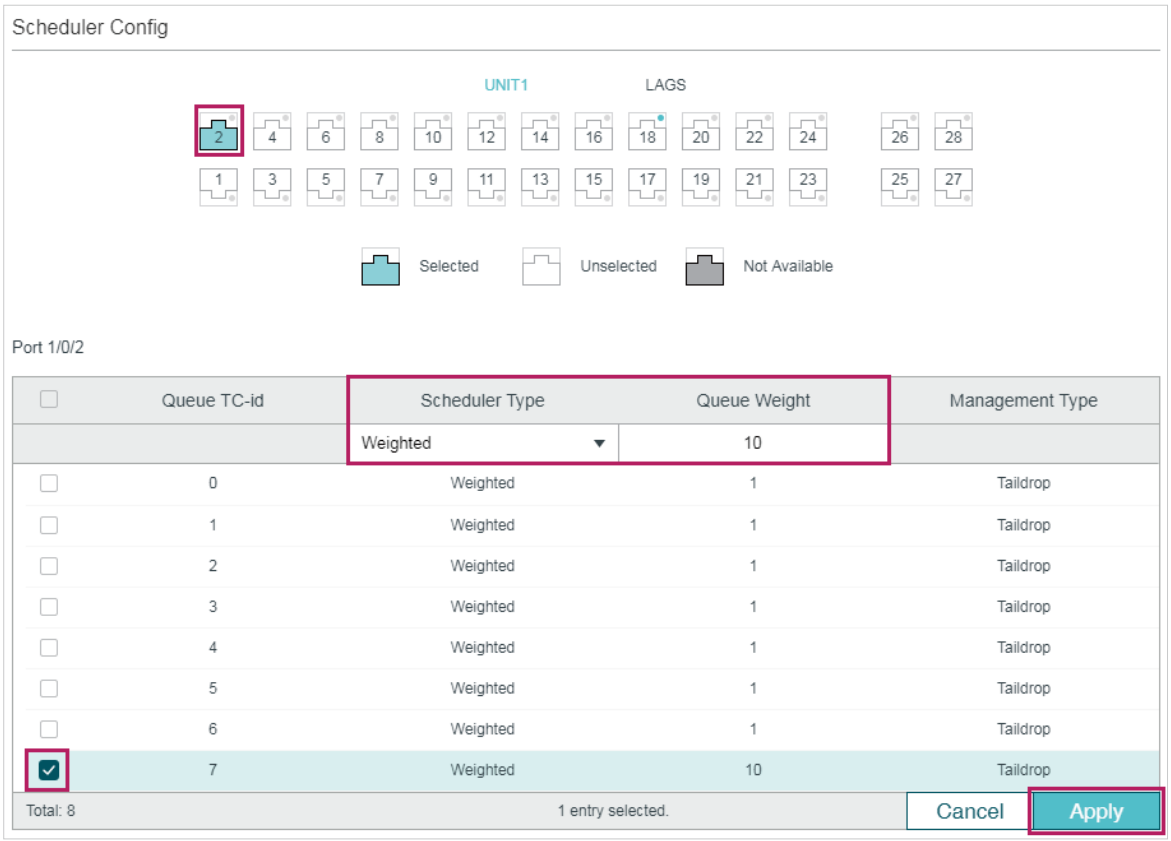
5) Choose the menu **QoS > Class of Service > Scheduler Settings** to load the following page. Select port 1/0/2. Set the scheduler mode as weighted and specify the queue weight as 1 for TC-5. Click **Apply**.

Figure 6-17 Configuring the TC-5 for the Port



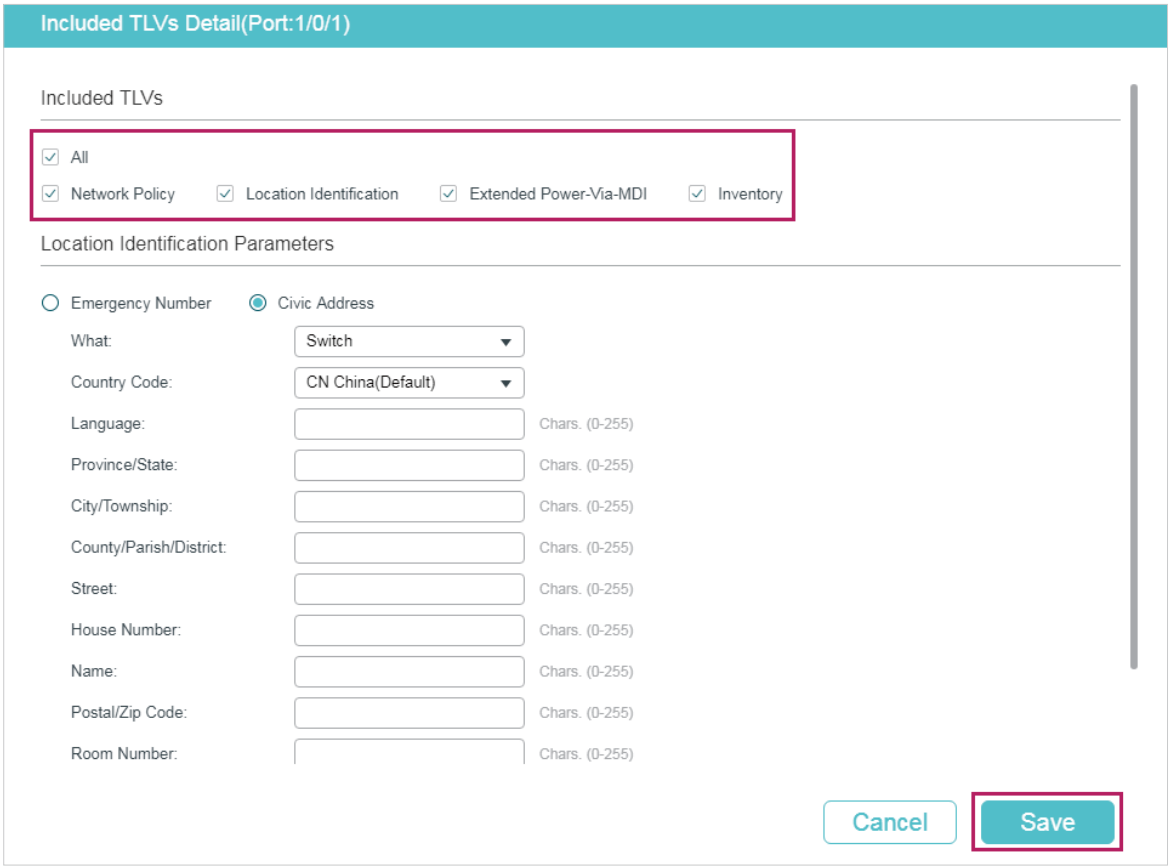
6) Select port 1/0/2. Set the scheduler mode as weighted and specify the queue weight as 10 for TC-7. Click **Apply**.

Figure 6-18 Configuring the TC-7 for the Port



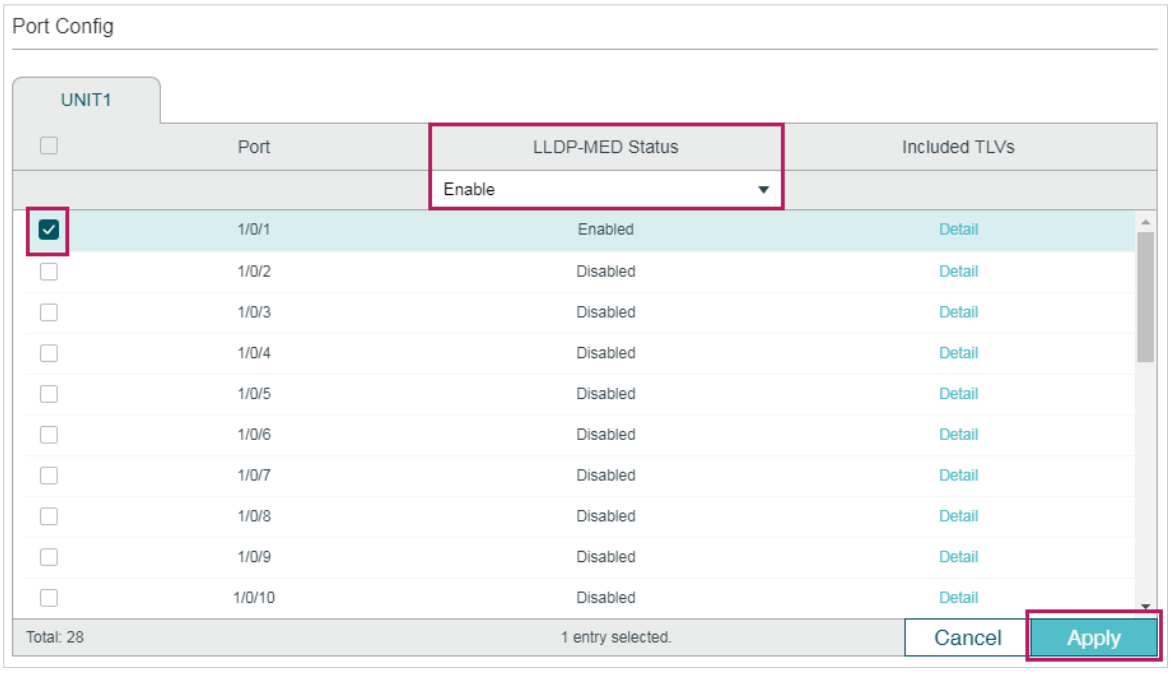
7) Choose the menu **L2 FEATURES > LLDP > LLDP-MED Config > Port Config** click Detail to of port1/0/1 to load the following page. Check the boxes of all the TLVs. Click **Save**.

Figure 6-19 Configuring the TLVs



8) Choose the menu **L2 FEATURES > LLDP > LLDP-MED Config > Port Config** to load the following page. Enable LLDP-MED on por t 1/0/1. Click **Apply**.

Figure 6-20 Enabling LLDP-MED on the Port



9) Click to save the settings.

6.3.4 Using the CLI

1) Enable Auto VoIP globally and specify the DSCP value of port 1/0/1 as 63.

   Switch_A#configure

   Switch_A(config)#auto-voip

   Switch_A(config)#interface gigabitEthernet 1/0/1

   Switch_A(config-if)#auto-voip dscp 63

   Switch_A(config-if)#exit

2) Set the trust mode of port 1/0/1 as trust DSCP. Specify the 802.1p priority as 7 for DSCP priority 63 and specify 802.1p priority as 5 for other DSCP priorities.

   Switch_A(config)#interface gigabitEthernet 1/0/1

   Switch_A(config-if)#qos trust mode dscp

   Switch_A(config-if)#exit

   Switch_A(config)#qos dscp-map 63 7

   Switch_A(config)#qos dscp-map 0-62 5

3) On port 1/0/1, set the scheduler mode as weighted and specify the queue weight as 1 for TC-5. Set the scheduler mode as weighted and specify the queue weight as 10 for TC-7.

   Switch_A(config)#interface gigabitEthernet 1/0/1

   Switch_A(config-if)#qos queue 5 mode wrr weight 1

   Switch_A(config-if)#qos queue 7 mode wrr weight 10

   Switch_A(config-if)#exit

4) Enable LLDP-MED on port 1/0/1 and select all the TLVs to be included in outgoing LLDPDU.

   Switch_A(config)#interface gigabitEthernet 1/0/1

   Switch_A(config-if)#lldp med-status

   Switch_A(config-if)#lldp med-tlv-select all

   Switch_A(config-if)#end

   Switch_A#copy running-config startup-config

Verify the configurations

Verify the configuration of Auto VoIP:

```
Switch_A(config)#show auto-voip
Administrative Mode:    Enabled
```

Verify the Auto VoIP configuration of ports:

```
Switch_A(config)#show auto-voip interface
Interface.Gi1/0/1
Auto-VoIP Interface Mode.          Disabled
Auto-VoIP COS Override.            False
Auto-VoIP DSCP Value.              63
Auto-VoIP Port Status.             Disabled

Interface.Gi1/0/2
Auto-VoIP Interface Mode.          Disabled
Auto-VoIP COS Override.            False
Auto-VoIP DSCP Value.              0
Auto-VoIP Port Status.             Disabled

Interface.Gi1/0/3
Auto-VoIP Interface Mode.          Disabled
Auto-VoIP COS Override.            False
Auto-VoIP DSCP Value.              0
Auto-VoIP Port Status.             Disabled
...
```

Verify the configuration of Class of Service:

```
Switch_A(config)#show qos trust interface gigabitEthernet 1/0/1
Port        Trust Mode      LAG
--------    ---------       ------
Gi1/0/1     trust DSCP      N/A
```

```
Switch_A(config)#show qos cos-map
---------------+-----+-----+-----+-----+-----+-----+----+----
Dot1p Value  |0     |1     |2     |3     |4     |5     |6    |7
---------------+-----+-----+-----+-----+-----+-----+----+----
TC              |TC1  |TC0  |TC2  |TC3  |TC4 |TC5  |TC6 |TC7
---------------+-----+-----+-----+-----+-----+-----+----+----
Switch_A(config)#show qos dscp-map
DSCP:              0    1    2    3    4    5    6    7
DSCP to 802.1P   5    5    5    5    5    5    5    5
                    ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              8    9    10   11   12   13   14   15
DSCP to 802.1P   5    5    5    5    5    5    5    5
                    ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              16   17   18   19   20   21   22   23
DSCP to 802.1P   5    5    5    5    5    5    5    5
                   ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              24   25   26   27   28   29   30   31
DSCP to 802.1P   5    5    5    5    5    5    5    5
                   ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              32   33   34   35   36   37   38   39
DSCP to 802.1P   5    5    5    5    5    5    5    5
                   ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              40   41   42   43   44   45   46   47
DSCP to 802.1P   5    5    5    5    5    5    5    5
                   ---- ---- ---- ---- ---- ---- ---- ---
DSCP:              48   49   50   51   52   53   54   55
DSCP to 802.1P   5    5    5    5    5    5    5    5
                  ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              56   57   58   59   60   61   62   63
```

```
DSCP to 802.1P  5    5    5    5    5    5    5    7
                ---- ---- ---- ---- ---- ---- ---- ---
```

Verify the configuration of LLDP-MED:

Switch_A(config)#show lldp interface

LLDP interface config:

gigabitEthernet 1/0/1:

Admin Status:	TxRx
SNMP Trap:	Disabled
TLV	Status
---	------
Port-Description	Yes
System-Capability	Yes
System-Description	Yes
System-Name	Yes
Management-Address	Yes
Port-VLAN-ID	Yes
Protocol-VLAN-ID	Yes
VLAN-Name	Yes
Link-Aggregation	Yes
MAC-Physic	Yes
Max-Frame-Size	Yes
Power	Yes
LLDP-MED Status:	Enabled
TLV	Status
---	------
Network Policy	Yes

Location Identification Yes

Extended Power Via MDI Yes

Inventory Management Yes

...

7 Appendix: Default Parameters

Default settings of Class of Service are listed in the following tables.

Table 7-1 Default Settings of Port Priority Configuration

Parameter	Default Setting
802.1P Priority	0
Trust Mode	Untrusted

Table 7-2 Default Settings of 802.1p to Queue Mapping

802.1p Priority	Queues (8)
0	TC1
1	TC0
2	TC2
3	TC3
4	TC4
5	TC5
6	TC6
7	TC7

Table 7-3 Default Settings of 802.1p Remap Configuration

Original 802.1p Priority	New 802.1p Priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Table 7-4 Default Settings of DSCP to 802.1p Mapping

DSCP	802.1p Priority
0 to 7	0
8 to 15	1

DSCP	802.1p Priority
16 to 23	2
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

Table 7-5 Default Settings of DSCP Remap Configuration

Original DSCP	New DSCP	Original DSCP	New DSCP	Original DSCP	New DSCP
0	0 be (000000)	22	22 af23 (010110)	44	44
1	1	23	23	45	45
2	2	24	24 cs3 (011000)	46	46 ef (101110)
3	3	25	25	47	47
4	4	26	26 af31 (011010)	48	48 cs6 (110000)
5	5	27	27	49	49
6	6	28	28 af32 (011100)	50	50
7	7	29	29	51	51
8	8 cs1 (001000)	30	30 af33 (011110)	52	52
9	9	31	31	53	53
10	10 af11 (001010)	32	32 cs4 (100000)	54	54
11	11	33	33	55	55
12	12 af12 (001100)	34	34 af41 (100010)	56	56 cs7 (111000)
13	13	35	35	57	57
14	14 af13 (001110)	36	36 af42 (100100)	58	58
15	15	37	37	59	59
16	16 cs2 (010000)	38	38 af43 (100110)	60	60
17	17	39	39	61	61
18	18 af21 (010010)	40	40 cs5 (101000)	62	62
19	19	41	41	63	63
20	20 af22 (010100)	42	42		
21	21	43	43		

Table 7-6 Default Settings of Scheduler Settings Configuration

Parameter	Default Setting
Scheduler Type	Weighted
Queue Weight	1
Management Type	Taildrop

Default settings of Class of Service are listed in the following tables.

Table 7-7 Default Settings of Bandwidth Control

Parameter	Default Setting
Ingress Rate (0-1,000,000Kbps)	0
Egress Rate (0-1,000,000Kbps)	0

Table 7-8 Default Settings of Storm Control

Parameter	Default Setting
Rate Mode	kbps
Broadcast Threshold (0-1,000,000)	0
Multicast Threshold (0-1,000,000)	0
UL-Frame Threshold (0-1,000,000)	0
Action	Drop
Recover Time	0

Default settings of Voice VLAN are listed in the following tables.

Table 7-9 Default Settings of Global Configuration

Parameter	Default Setting
Voice VLAN	Disabled
VLAN ID	None
Priority	7

Table 7-10 Default Settings of Port Configuration

Parameter	Default Setting
Voice VLAN	Disabled

Table 7-11 Default Settings of OUI Table

OUI	Status	Description
00:01:E3	Default	SIEMENS
00:03:6B	Default	CISCO1
00:12:43	Default	CISCO2
00:0F:E2	Default	H3C
00:60:B9	Default	NITSUKO
00:D0:1E	Default	PINTEL
00:E0:75	Default	VERILINK
00:E0:BB	Default	3COM
00:04:0D	Default	AVAYA1
00:1B:4F	Default	AVAYA2
00:04:13	Default	SNOM

Default settings of Auto VoIP are listed in the following tables.

Table 7-12 Default Settings of Auto VoIP

Parameter	Default Setting
Interface Mode	Disabled
Value	None
Cos Override Mode	Disabled
DSCP Value	0

Part 23

Configuring Access Security

CHAPTERS

1. Access Security
2. Access Security Configurations
3. Appendix: Default Parameters

1 Access Security

1.1 Overview

Access Security provides different security measures for accessing the switch remotely so as to enhance the configuration management security.

1.2 Supported Features

Access Control

This function is used to control the users' access to the switch based on IP address, MAC address or port.

HTTP

This function is based on the HTTP protocol. It can allow or deny users to access the switch via a web browser.

HTTPS

This function is based on the SSL or TLS protocol working in transport layer. It supports a security access via a web browser.

SSH

This function is based on the SSH protocol, a security protocol established on application and transport layers. The function with SSH is similar to a telnet connection, but SSH can provide information security and powerful authentication.

Telnet

This function is based on the Telnet protocol subjected to TCP/IP protocol. Through Telnet, users can log on to the switch remotely.

Serial Port

Note:

Serial Port is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If Serial Port is available, there is **SECURITY > Access Security > Serial Port Config** in the menu structure.

You can configure the serial port parameters.

2 Access Security Configurations

With access security configurations, you can:

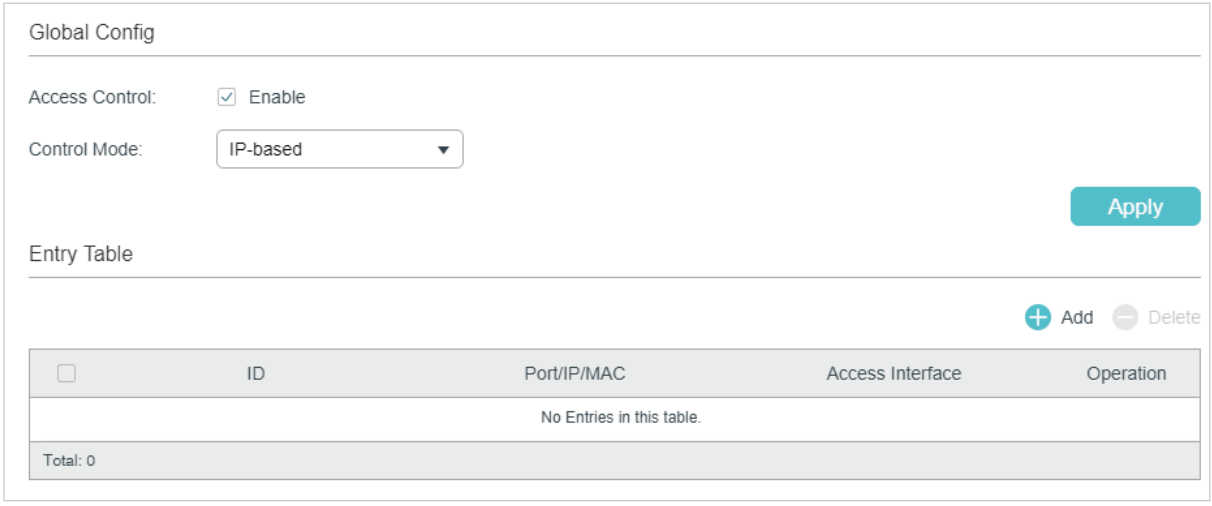
- Configure the Access Control feature
- Configure the HTTP feature
- Configure the HTTPS feature
- Configure the SSH feature
- Configure the Telnet function
- Configure the Serial Port parameters

2.1 Using the GUI

2.1.1 Configuring the Access Control Feature

Choose the menu **SECURITY** > **Access Security** > **Access Control** to load the following page.

Figure 2-1 Configuring the Access Control



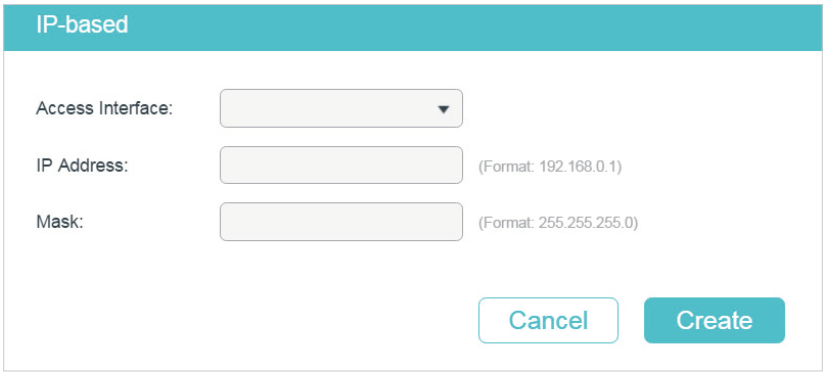
1) In the **Global Config** section, enable Access Control, select one control mode and click **Apply**.

Control Mode	Choose how to control the users' access. **IP-based**: Only the users within a certain IP-range can access the switch via the specified interfaces **MAC-based**: Only the users with a certain MAC address can access the switch via the specified interfaces. **Port-based**: Only the users who are connected to certain ports can access the switch via the specified interfaces.

2) In the Entry Table section, click Add to add an Access Control entry.

- When the **IP-based** mode is selected, the following window will pop up.

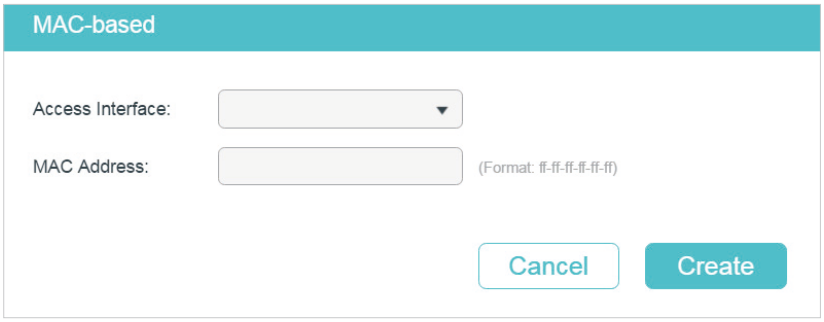
Figure 2-2 Configuring Access Control Based on IP Range



Access Interface	Select the interfaces where to apply the Access Control rule. If an interface is unselected, all users can access the switch via it. **SNMP**: A function to manage the network devices via NMS. **Telnet**: A connection type for users to remote login. **SSH**: A connection type based on SSH protocol. **HTTP**: A connection type based on HTTP protocol. **HTTPS**: A connection type based on SSL protocol. **Ping**: A communication protocol to test the connection of the network.
IP Address/ Mask	Enter the IP address and mask to specify an IP range. Only the users within this IP range can access the switch via the specified interfaces.

- When the **MAC-based** mode is selected, the following window will pop up.

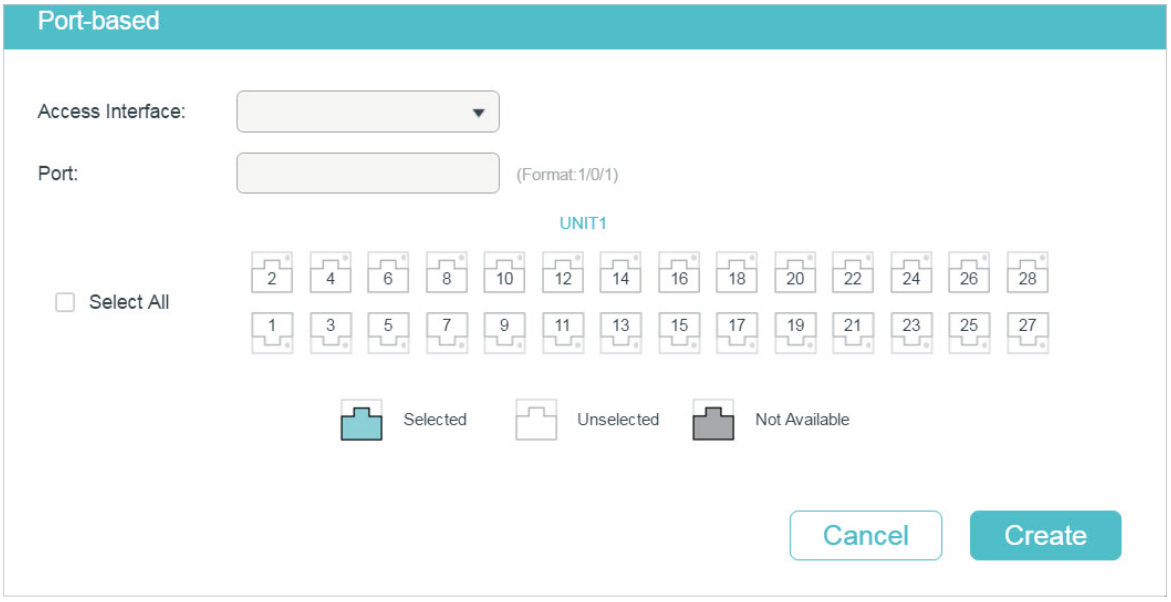
Figure 2-3 Configuring Access Control Entry Based on MAC Address



Access Interface	Select the interfaces where to apply the Access Control rule. If an interface is unselected, all users can access the switch via it. **SNMP**: A function to manage the network devices via NMS. **Telnet**: A connection type for users to remote login. **SSH**: A connection type based on SSH protocol. **HTTP**: A connection type based on HTTP protocol. **HTTPS**: A connection type based on SSL protocol. **Ping**: A communication protocol to test the connection of the network.
MAC Address	Enter the MAC address. Only the users with this MAC address can access the switch via the specified interfaces.

- When the **Port-based** mode is selected, the following window will pop up.

Figure 2-4 Configuring Access Control Entry Based on Port



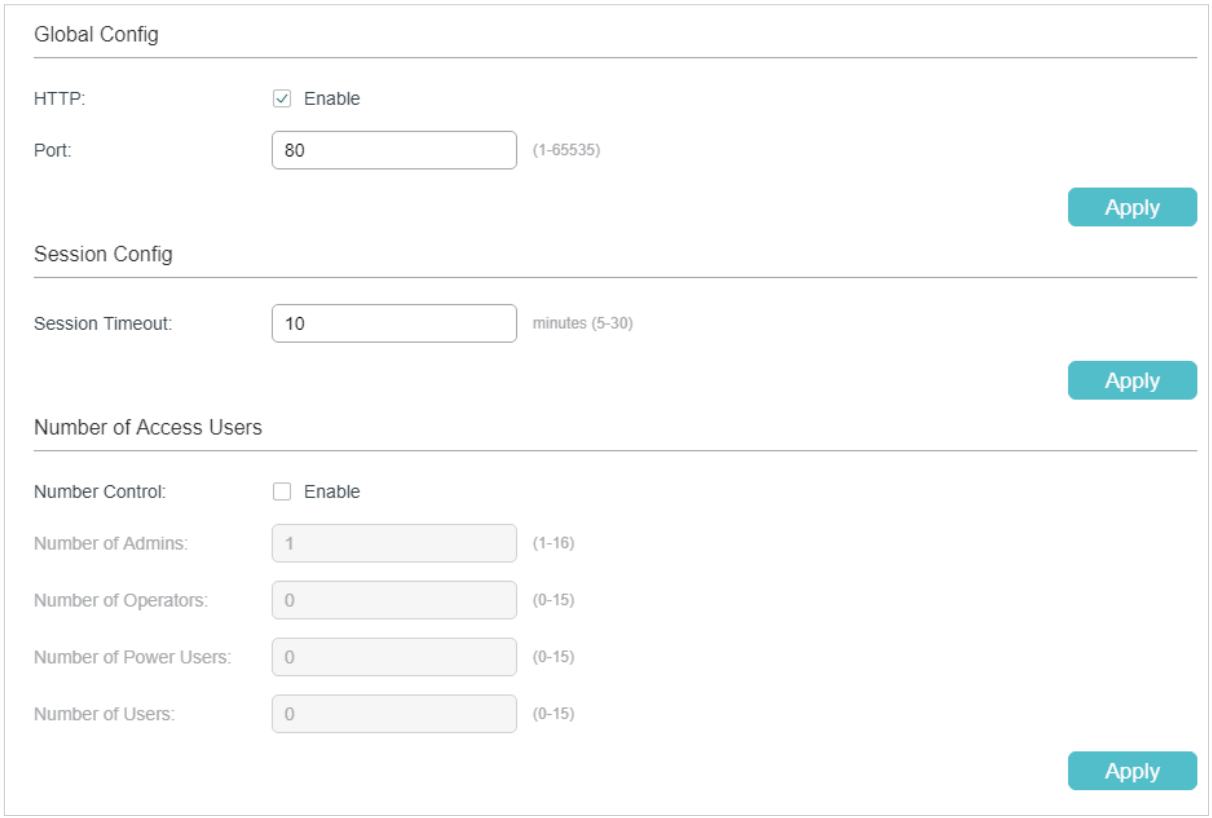
Access Interface	Select the interfaces where to apply the Access Control rule. If an interface is unselected, all users can access the switch via it. **SNMP**: A function to manage the network devices via NMS. **Telnet**: A connection type for users to remote login. **SSH**: A connection type based on SSH protocol. **HTTP**: A connection type based on HTTP protocol. **HTTPS**: A connection type based on SSL protocol. **Ping**: A communication protocol to test the connection of the network.
Port	Select one or more ports. Only the users who are connected to these ports can access the switch via the specified interfaces.

3) Click **Create**. Then you can view the created entries in the table.

2.1.2 Configuring the HTTP Function

Choose the menu **SECURITY** > **Access Security** > **HTTP Config** to load the following page.

Figure 2-5 Configuring the HTTP Function



1) In the **Global Control** section, enable HTTP function, specify the port using for HTTP, and click **Apply** to enable the HTTP function.

HTTP	HTTP function is based on the HTTP protocol. It allows users to manage the switch through a web browser.
Port	Specify the port number for HTTP service.

2) In the **Session Config** section, specify the Session Timeout and click **Apply**.

Session Timeout	The system will log out automatically if users do nothing within the Session Timeout time.

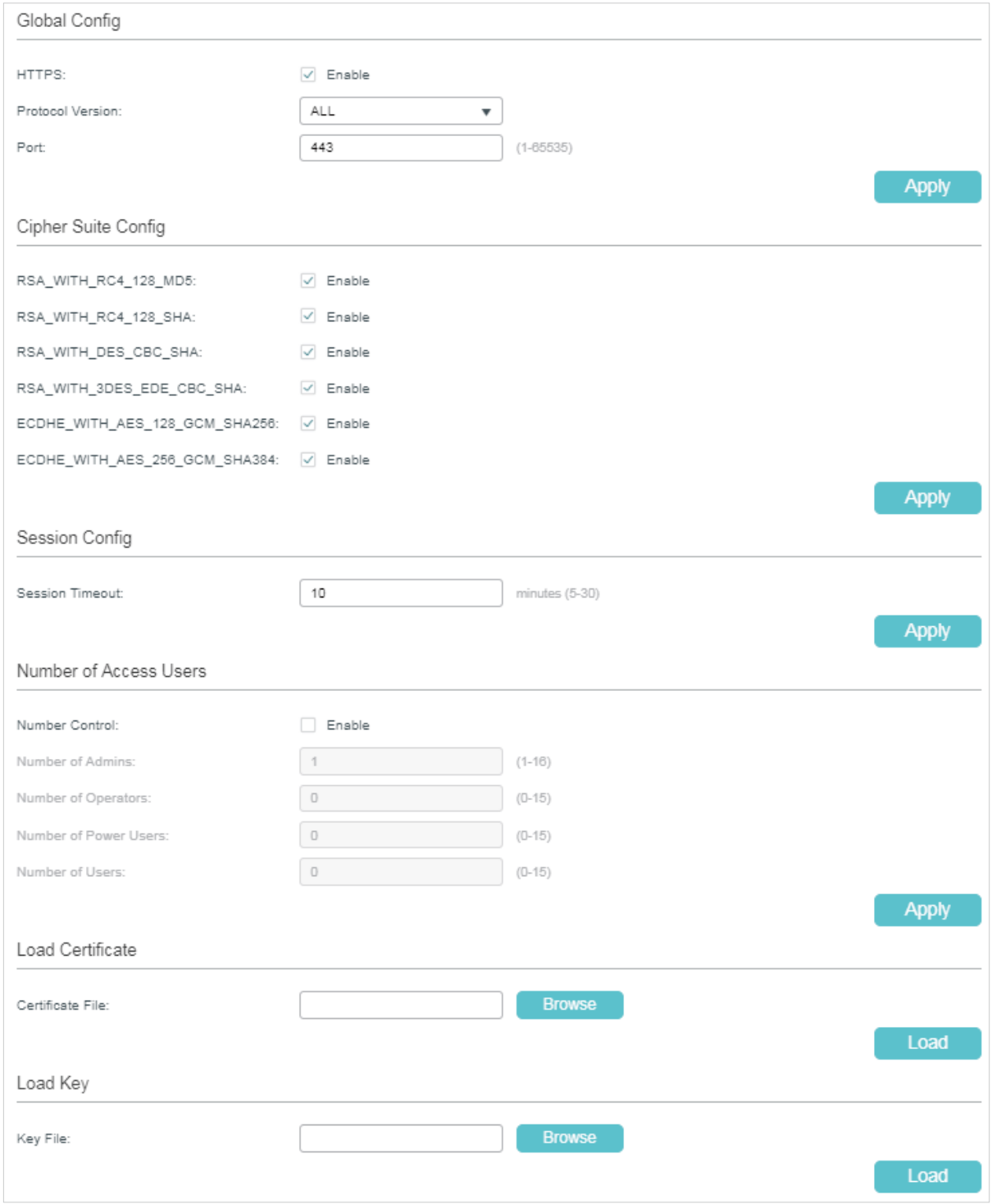
3) In the **Number of Access Users** section, enable Number Control function, specify the following parameters and click **Apply**.

Number Control	Enable or disable Number Control. With this option enabled, you can control the number of the users logging on to the web management page at the same time. The total number of users should be no more than 16.
Number of Admins	Specify the maximum number of users whose access level is Admin.
Number of Operators	Specify the maximum number of users whose access level is Operator.
Number of Power Users	Specify the maximum number of users whose access level is Power User.
Number of Users	Specify the maximum number of users whose access level is User.

2.1.3 Configuring the HTTPS Function

Choose the menu **SECURITY** > **Access Security** > **HTTPS Config** to load the following page.

Figure 2-6 Configuring the HTTPS Function



1) In the **Global Config** section, enable HTTPS function, select the protocol version that the switch supports and specify the port using for HTTPS. Click **Apply**.

HTTPS	Enable or disable the HTTPS function. HTTPS function is based on the SSL or TLS protocol. It provides a secure connection between the client and the switch.
Protocol Version	Select the protocol version for HTTPS. Make sure the protocol in use is compatible with that on your HTTPS client. SSL is a transport protocol. It can provide server authentication, encryption and message integrity to allow secure HTTP connection. TLS is a transport protocol upgraded from SSL. It can support a more secure connection than SSL. TLS and SSL are not compatible with each other. **SSL Version 3.0**: Select SSL Version 3.0 as the protocol for HTTPS. **TLS Version 1.0**: Select TLS Version 1.0 as the protocol for HTTPS. **TLS Version 1.1**: Select TLS Version 1.1 as the protocol for HTTPS. **TLS Version 1.2**: Select TLS Version 1.2 as the protocol for HTTPS. **All**: Enable all the above protocols for HTTPS. The HTTPS server and client will negotiate the protocol each time.
Port	Specify the port number for HTTPS service.

2) In the **CipherSuite Config** section, select the algorithm to be enabled and click **Apply**.

RSA_WITH_RC4_128_MD5	128-bit RC4 encryption with MD5 message authentication and RSA key exchange.
RSA_WITH_RC4_128_SHA	128-bit RC4 encryption with SHA-1 message authentication and RSA key exchange.
RSA_WITH_DES_CBC_SHA	56-bit DES encryption with SHA-1 message authentication and RSA key exchange.
RSA_WITH_3DES_EDE_CBC_SHA	168-bit Triple DES encryption with SHA-1 message authentication and RSA key exchange.
ECDHE_WITH_AES_128_GCM_SHA256	128-bit AES in Galois Counter Mode encryption with SHA-256 message authentication and elliptic curve Diffie-Hellman key exchange signed with an RSA certificate or ECDSA certificate.
ECDHE_WITH_AES_256_GCM_SHA384	256-bit AES in Galois Counter Mode encryption with SHA-384 message authentication and elliptic curve Diffie-Hellman key exchange signed with an RSA certificate or ECDSA certificate.

3) In the **Session Config** section, specify the Session Timeout and click **Apply**.

Session Timeout	The system will log out automatically if users do nothing within the Session Timeout time.

4) In the **Number of Access Users** section, enable Number Control function, specify the following parameters and click **Apply**.

Number Control	Enable or disable Number Control. With this option enabled, you can control the number of the users logging on to the web management page at the same time. The total number of users should be no more than 16.
Number of Admins	Specify the maximum number of users whose access level is Admin.
Number of Operators	Specify the maximum number of users whose access level is Operator.
Number of Power Users	Specify the maximum number of users whose access level is Power User.
Number of Users	Specify the maximum number of users whose access level is User.

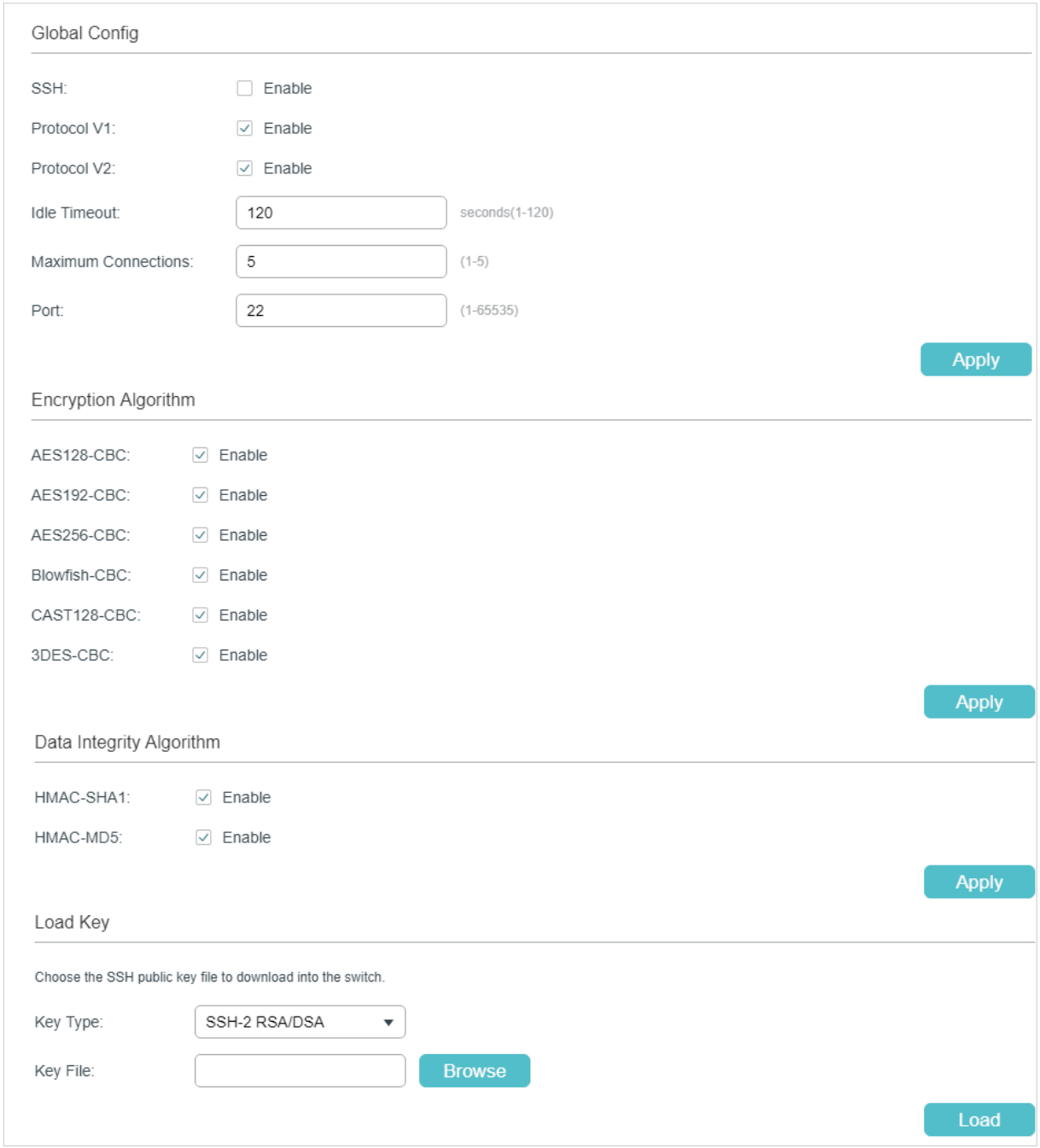
5) In the **Load Certificate** and **Load Key** section, download the certificate and key.

Certificate File	Select the desired certificate to download to the switch. The certificate must be BASE64 encoded. The SSL certificate and key downloaded must match each other, otherwise the HTTPS connection will not work.
Key File	Select the desired Key to download to the switch. The key must be BASE64 encoded. The SSL certificate and key downloaded must match each other, otherwise the HTTPS connection will not work.

2.1.4 Configuring the SSH Feature

Choose the menu **SECURITY** > **Access Security** > **SSH Config** to load the following page.

Figure 2-7 Configuring the SSH Feature



1) In the **Global Config** section, select **Enable** to enable SSH function and specify following parameters.

SSH	Select **Enable** to enable the SSH function. SSH is a protocol working in application layer and transport layer. It can provide a secure, remote connection to a device. It is more secure than Telnet protocol as it provides strong encryption.

Protocol V1	Select **Enable** to enable SSH version 1.
Protocol V2	Select **Enable** to enable SSH version 2.
Idle Timeout	Specify the idle timeout time. The system will automatically release the connection when the time is up.
Maximum Connections	Specify the maximum number of the connections to the SSH server. New connection will not be established when the number of the connections reaches the maximum number you set.
Port	Specify the port using for SSH.

2) In the **Encryption Algorithm** section, enable the encryption algorithm you want the switch to support and click **Apply**.

3) In **Data Integrity Algorithm** section, enable the integrity algorithm you want the switch to support and click **Apply**.

4) In **Import Key File** section, select key type from the drop-down list and click **Browse** to download the desired key file.

Key Type	Select the key type. The algorithm of the corresponding type is used for both key generation and authentication.
Key File	Select the desired public key to download to the switch. The key length of the downloaded file ranges of 512 to 3072 bits.

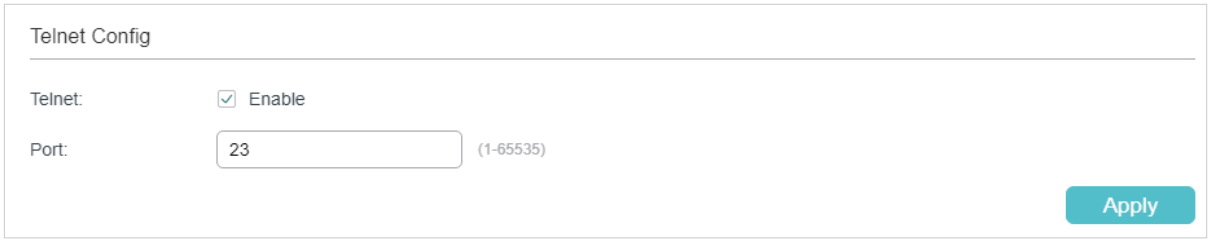
Note:

It will take a long time to download the key file. Please wait without any operation.

2.1.5 Configuring the Telnet Function

Choose the menu **SECURITY** > **Access Security** > **Telnet Config** to load the following page.

Figure 2-8 Configuring the Telnet Function



Enable Telnet and click **Apply**.

Telnet	Select **Enable** to make the Telnet function effective. Telnet function is based on the Telnet protocol subjected to TCP/IP protocol. It allows users to log on to the switch remotely.
Port	Specify the port using for Telnet.

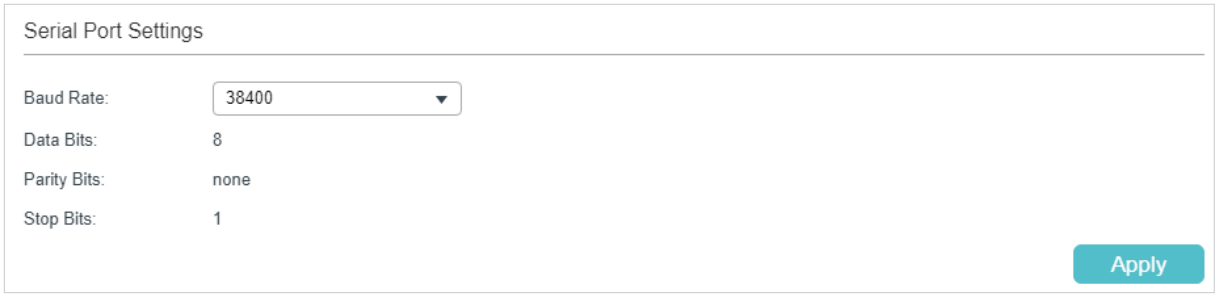
2.1.6 Configuring the Serial Port Parameters

Note:

Serial Port is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If Serial Port is available, there is **SECURITY > Access Security > Serial Port Config** in the menu structure.

Choose the menu **SECURITY** > **Access Security** > **Serial Port Config** to load the following page.

Figure 2-9 Configuring the Serial Port Parameters



Configure the Baud Rate and click **Apply**.

Baud Rate	Configure the baud rate of the console connection. The default value is 38400 bps.
Data Bits	Displays the data bits.
Parity Bits	Displays the parity bits.
Stop Bits	Displays the stop bits.

2.2 Using the CLI

2.2.1 Configuring the Access Control Feature

Follow these steps to configure the access control:

Step 1	**configure** Enter global configuration mode.

Step 2

- Use the following command to control the users' access by limiting the IP address:

user access-control ip-based enable

Configure the control mode as IP-based.

user access-control ip-based { *ip-addr ip-mask* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**

Only the users within a certain IP-range can access the switch via the specified interfaces.

ip-addr: Specify the IP address of the user.

ip-mask: Specify the subnet mask of the user.

[snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Select the interfaces where to apply the Access Control rule. If an interface is unselected, all users can access the switch via it. By default, all the interfaces are selected.

- Use the following command to control the users' access by limiting the MAC address:

user access-control mac-based enable

Configure the control mode as MAC-based.

user access-control mac-based { *mac-addr* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**

Only the users with a certain MAC address can access the switch via the specified interfaces.

mac-addr: Specify the MAC address of the user.

[snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Select the interfaces where to apply the Access Control rule. If an interface is unselected, all users can access the switch via it. By default, all the interfaces are selected.

- Use the following command to control the users' access by limiting the ports connected to the users:

user access-control port-based enable

Configure the control mode as Port-based.

user access-control port-based interface { fastEthernet *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**

Only the users who are connected to certain ports can access the switch via the specified interfaces.

port-list: Specify the list of Ethernet port, in the format of 1/0/1-4. You can appoint 5 ports at most.

[snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Select the interfaces where to apply the Access Control rule. If an interface is unselected, all users can access the switch via it. By default, all the interfaces are selected.

Step 3

show user configuration

Verify the security configuration information of the user authentication information and the access interface.

Step 4

end

Return to privileged EXEC mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the type of access control as IP-based. Set the IP address as 192.168.0.100, set the subnet mask as 255.255.255.0, and select snmp, telnet, http and https to apply the Access Control rule.

Switch#configure

Switch(config)#user access-control ip-based enable

Switch(config)#user access-control ip-based 192.168.0.100 255.255.255.255 snmp telnet http https

Switch(config)#show user configuration

User authentication mode: IP based

Index	IP Address	Access Interface
1	192.168.0.100/24	SNMP Telnet HTTP HTTPS

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring the HTTP Function

Follow these steps to configure the HTTP function:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip http server** Enable the HTTP function. By default, it is enabled.
Step 3	**ip http session timeout** *minutes* Specify the Session Timeout time. The system will log out automatically if users do nothing within the Session Timeout time. *minutes*: Specify the timeout time, which ranges from 5 to 30 minutes. The default value is 10.

Step 4	**ip http max-users** *admin-num operator-num poweruser-num user-num* Specify the maximum number of users that are allowed to connect to the HTTP server. The total number of users should be no more than 16. *admin-num*: Enter the maximum number of users whose access level is Admin. The valid values are from 1 to 16. *operator-num*: Enter the maximum number of users whose access level is Operator. The valid values are from 0 to 15. *poweruser-num*: Enter the maximum number of users whose access level is Power User. The valid values are from 0 to 15. *user-num*: Enter the maximum number of users whose access level is User. The valid values are from 0 to 15.
Step 5	**show ip http configuration** Verify the configuration information of the HTTP server, including status, session timeout, access-control, max-user number and the idle-timeout, etc.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the session timeout as 9, set the maximum admin number as 6, and set the maximum operator number as 2, the maximum power user number as 2, the maximum user number as 2.

Switch#configure

Switch(config)#ip http server

Switch(config)#ip http session timeout 9

Switch(config)#ip http max-user 6 2 2 2

Switch(config)#show ip http configuration

HTTP Status:	Enabled
HTTP Port:	80
HTTP Session Timeout:	9
HTTP User Limitation:	Enabled
HTTP Max Users as Admin:	6
HTTP Max Users as Operator:	2
HTTP Max Users as Power User:	2
HTTP Max Users as User:	2

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring the HTTPS Function

Follow these steps to configure the HTTPS function:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip http secure-server** Enable the HTTPS function. By default, it is enabled.
Step 3	**ip http secure-protocol {** ssl3 | tls1 | tls11 | tls12 | all **}** Select the protocol version for HTTPS. Make sure the protocol in use is compatible with that on your HTTPS client. SSL is a transport protocol. It can provide server authentication, encryption and message integrity to allow secure HTTP connection. TLS is a transport protocol upgraded from SSL. It can support a more secure connection than SSL. TLS and SSL are not compatible with each other. ssl3: Select SSL Version 3.0 as the protocol for HTTPS. tls1: Select TLS Version 1.0 as the protocol for HTTPS. tls11: Select TLS Version 1.1 as the protocol for HTTPS. tls12: Select TLS Version 1.2 as the protocol for HTTPS. all: Enable all the above protocols for HTTPS. The HTTPS server and client will negotiate the protocol each time.
Step 4	**ip http secure-ciphersuite { [** rc4-128-md5 **] [** rc4-128-sha **] [** des-cbc-sha **] [** 3des-ede-cbc-sha **] [** ecdhe-a128-g-s256 **] [** ecdhe-a256-g-s384 **] }** Enable the corresponding ciphersuite. By default, these types are all enabled. rc4-128-md5: 128-bit RC4 encryption with MD5 message authentication and RSA key exchange. rc4-128-sha: 128-bit RC4 encryption with SHA-1 message authentication and RSA key exchange. des-cbc-sha: 56-bit DES encryption with SHA-1 message authentication and RSA key exchange. 3des-ede-cbc-sha: 168-bit Triple DES encryption with SHA-1 message authentication and RSA key exchange. ecdhe-a128-g-s256: 128-bit AES in Galois Counter Mode encryption with SHA-256 message authentication and elliptic curve Diffie-Hellman key exchange signed with an RSA certificate or ECDSA certificate. ecdhe-a256-g-s384: 256-bit AES in Galois Counter Mode encryption with SHA-384 message authentication and elliptic curve Diffie-Hellman key exchange signed with an RSA certificate or ECDSA certificate.

Step 5	**ip http secure-session timeout** *minutes* Specify the Session Timeout time. The system will log out automatically if users do nothing within the Session Timeout time. *minutes*: Specify the timeout time, which ranges from 5 to 30 minutes. The default value is 10.
Step 6	**ip http secure-max-users** *admin-num operator-num poweruser-num user-num* Specify the maximum number of users that are allowed to connect to the HTTPS server. The total number of users should be no more than 16. *admin-num*: Enter the maximum number of users whose access level is Admin. The valid values are from 1 to 16. *operator-num*: Enter the maximum number of users whose access level is Operator. The valid values are from 0 to 15. *poweruser-num*: Enter the maximum number of users whose access level is Power User. The valid values are from 0 to 15. *user-num*: Enter the maximum number of users whose access level is User. The valid values are from 0 to 15.
Step 7	**ip http secure-server download certificate** *ssl-cert* **ip-address** *ip-addr* Download the desired certificate to the switch from TFTP server. *ssl-cert*: Specify the name of the SSL certificate, which ranges from 1 to 25 characters. The certificate must be BASE64 encoded. The SSL certificate and key downloaded must match each other. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
Step 8	**ip http secure-server download key** *ssl-key* **ip-address** *ip-addr* Download the desired key to the switch from TFTP server. *ssl-key*: Specify the name of the key file saved in TFTP server. The key must be BASE64 encoded. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
Step 9	**show ip http secure-server** Verify the global configuration of HTTPS.
Step 10	**end** Return to privileged EXEC mode.
Step 11	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the HTTPS function. Enable all the protocol versions, including SSL 3.0, TLS 1.0, TLS 1.1 and TLS1.2. Enable the ciphersuite of 3des-ede-cbc-sha. Set the session timeout time as 15, the maximum admin number as 2, the maximum operator number as 2, the maximum power user number as 2, the maximum user

number as 2. Download the certificate named ca.crt and the key named ca.key from the TFTP server with the IP address 192.168.0.100.

Switch#configure

Switch(config)#ip http secure-server

Switch(config)#ip http secure-protocol all

Switch(config)#ip http secure-ciphersuite 3des-ede-cbc-sha

Switch(config)#ip http secure-session timeout 15

Switch(config)#ip http secure-max-users 2 2 2 2

Switch(config)#ip http secure-server download certificate ca.crt **ip-address** 192.168.0.100

Start to download SSL certificate...

Download SSL certificate OK.

Switch(config)#ip http secure-server download key ca.key **ip-address** 192.168.0.100

Start to download SSL key...

Download SSL key OK.

Switch(config)#show ip http secure-server

HTTPS Status:	Enabled
HTTPS Port:	443
SSL Protocol Level(s):	all
SSL CipherSuite:	3des-ede-cbc-sha
HTTPS Session Timeout:	15
HTTPS User Limitation:	Enabled
HTTPS Max Users as Admin:	2
HTTPS Max Users as Operator:	2
HTTPS Max Users as Power User:	2
HTTPS Max Users as User:	2

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Configuring the SSH Feature

Follow these steps to configure the SSH function:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip ssh server** Enable the SSH function. By default, it is disabled.
Step 3	**ip ssh version {** v1 | v2 **}** Configure to make the switch support the corresponding protocol. By default, the switch supports SSHv1 and SSHv3. v1 | v2: Select to enable the corresponding protocol.
Step 4	**ip ssh timeout** *value* Specify the idle timeout time. The system will automatically release the connection when the time is up. *value*: Enter the value of the timeout time, which ranges from 1 to 120 seconds. The default value is 120 seconds.
Step 5	**ip ssh max-client** *num* Specify the maximum number of the connections to the SSH server. New connection will not be established when the number of the connections reaches the maximum number you set. *num*: Enter the number of the connections, which ranges from 1 to 5. The default value is 5.
Step 6	**ip ssh algorithm {** AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 **}** Enable the corresponding algorithm. By default, these types are all enabled. AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC: Specify the encryption algorithm you want the switch supports. HMAC-SHA1 | HMAC-MD5: Specify the data integrity algorithm you want the switch supports.
Step 7	**ip ssh download {** v1 | v2 **}** *key-file* **ip-address** *ip-addr* Select the type of the key file and download the desired file to the switch from TFTP server. v1 | v2: Select the key type. The algorithm of the corresponding type is used for both key generation and authentication. *key-file*: Specify the name of the key file saved in TFTP server. Ensure the key length of the downloaded file is in the range of 512 to 3072 bits. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
Step 8	**show ip ssh** Verify the global configuration of SSH.

Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

Note:

It will take a long time to download the key file. Please wait without any operation.

The following example shows how to configure the SSH function. Set the version as SSH V1 and SSH V2. Enable the AES128-CBC and Cast128-CBC encryption algorithm. Enable the HMAC-MD5 data integrity algorithm. Choose the key type as SSH-2 RSA/DSA.

Switch(config)#ip ssh server

Switch(config)#ip ssh version v1

Switch(config)#ip ssh version v2

Switch(config)#ip ssh timeout 100

Switch(config)#ip ssh max-client 4

Switch(config)#ip ssh algorithm AES128-CBC

Switch(config)#ip ssh algorithm Cast128-CBC

Switch(config)#ip ssh algorithm HMAC-MD5

Switch(config)#ip ssh download v2 publickey **ip-address** 192.168.0.100

Start to download SSH key file...

Download SSH key file OK.

Switch(config)#show ip ssh

Global Config:

SSH Server: Enabled

Protocol V1: Enabled

Protocol V2: Enabled

Idle Timeout: 100

MAX Clients: 4

Port: 22

Encryption Algorithm:

AES128-CBC: Enabled

AES192-CBC: Disabled

AES256-CBC: Disabled

Blowfish-CBC: Disabled

Cast128-CBC: Enabled

3DES-CBC: Disabled

Data Integrity Algorithm:

HMAC-SHA1: Disabled

HMAC-MD5: Enabled

Key Type: SSH-2 RSA/DSA

Key File:

---- BEGIN SSH2 PUBLIC KEY ----

Comment: "dsa-key-20160711"

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Configuring the Telnet Function

Follow these steps enable the Telnet function:

Step 1	**configure** Enter global configuration mode.
Step 2	**telnet enable** Enable the telnet function. By default, it is enabled.
Step 3	**telnet port** *port* Specify the port using for Telnet. It ranges from 1 to 65535.
Step 4	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

2.2.6 Configuring the Serial Port Parameters

Note:

Serial Port is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If Serial Port is available, there is **SECURITY > Access Security > Serial Port Config** in the menu structure.

Follow these steps enable the serial port parameters:

Step 1	**configure** Enter global configuration mode.
Step 2	**serial_port baud_rate {** 9600 | 19200 | 38400 | 57600 | 115200 **}** Specify the baud rate of the console connection. 9600 | 19200 | 38400 | 57600 | 115200: Specify the communication baud rate on the console port. The default value is 38400 bps.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

3 Appendix: Default Parameters

Default settings of Access Security are listed in the following tables.

Table 3-1 Default Settings of Access Control Configuration

Parameter	Default Setting
Access Control	Disabled

Table 3-2 Default Settings of HTTP Configuration

Parameter	Default Setting
HTTP	Enabled
Port	80
Session Timeout	10 minutes
Number Control	Disabled

Table 3-3 Default Settings of HTTPS Configuration

Parameter	Default Setting
HTTPS	Enabled
Protocol Version	All
Port	443
RSA_WITH_RC4_128_MD5	Enabled
RSA_WITH_RC4_128_SHA	Enabled
RSA_WITH_DES_CBC_SHA	Enabled
RSA_WITH_3DES_EDE_CBC_SHA	Enabled
ECDHE_WITH_AES_128_GCM_SHA256	Enabled
ECDHE_WITH_AES_256_GCM_SHA384	Enabled
Session Timeout	10 minutes
Number Control	Disabled

Table 3-4 Default Settings of SSH Configuration

Parameter	Default Setting
SSH	Disabled
Protocol V1	Enabled
Protocol V2	Enabled

Parameter	Default Setting
Idle Timeout	120 seconds
Maximum Connections	5
Port	22
AES128-CBC	Enabled
AES192-CBC	Enabled
AES256-CBC	Enabled
Blowfish-CBC	Enabled
Cast128-CBC	Enabled
3DES-CBC	Enabled
HMAC-SHA1	Enabled
HMAC-MD5	Enabled
Key Type:	SSH-2 RSA/DSA

Table 3-5 Default Settings of Telnet Configuration

Parameter	Default Setting
Telnet	Enabled
Port	23

Table 3-6 Default Settings of Serial Port

Parameter	Default Setting
Baud Rate	38400 bps

Part 24

Configuring AAA

CHAPTERS

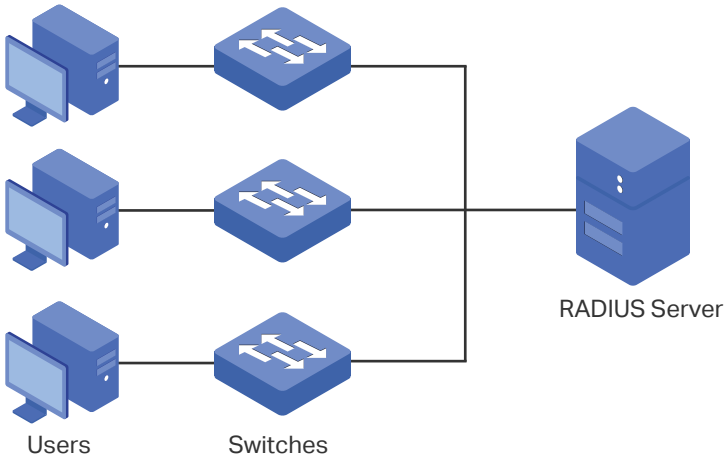
1. Overview
2. AAA Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

AAA stands for authentication, authorization and accounting. On TP-Link switches, this feature is mainly used to authenticate the users trying to log in to the switch or get administrative privileges. The administrator can create guest accounts and an Enable password for other users. The guests do not have administrative privileges without the Enable password provided.

AAA provides a safe and efficient authentication method. The authentication can be processed locally on the switch or centrally on the RADIUS/TACACS+ server(s). As the following figure shows, the network administrator can centrally configure the management accounts of the switches on the RADIUS server and use this server to authenticate the users trying to access the switch or get administrative privileges.

Figure 1-1 Network Topology of AAA



2 AAA Configuration

In the AAA feature, the authentication can be processed locally on the switch or centrally on the RADIUS/TACACS+ server(s). To ensure the stability of the authentication system, you can configure multiple servers and authentication methods at the same time. This chapter introduces how to configure this kind of comprehensive authentication in AAA.

To complete the configuration, follow these steps:

1) Add the servers.
2) Configure the server groups.
3) Configure the method list.
4) Configure the AAA application list.
5) Configure the login account and the Enable password.

Configuration Guidelines

The basic concepts and working mechanism of AAA are as follows:

- AAA Default Setting

By default, the AAA feature is enabled and cannot be disabled.

- Server Group

Multiple servers running the same protocol can be added to a server group, and the servers in the group will authenticate the users in the order they are added. The server that is first added to the group has the highest priority, and is responsible for authentication under normal circumstances. If the first one breaks down or doesn't respond to the authentication request for some reason, the second sever will start working for authentication, and so on.

- Method List

A server group is regarded as a method, and the local authentication is another method. Several methods can be configured to form a method list. The switch uses the first method in the method list to authenticate the user, and if that method fails to respond, the switch selects the next method. This process continues until the user has a successful communication with a method or until all defined methods are exhausted. If the authentication succeeds or the secure server or the local switch denies the user's access, the authentication process stops and no other methods are attempted.

Two types of method list are provided: Login method list for users of all types to access the switch, and Enable method list for guests to get administrative privileges.

- AAA Application List

The switch supports the following access applications: Telnet, SSH and HTTP. You can select the configured authentication method lists for each application.

2.1 Using the GUI

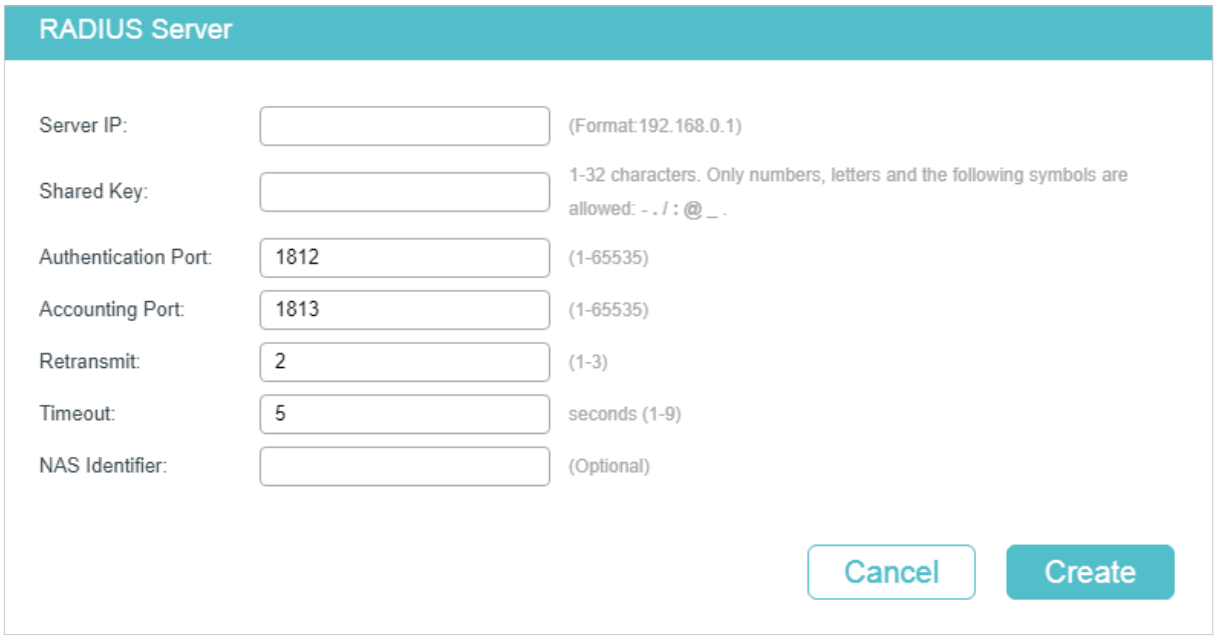
2.1.1 Adding Servers

You can add one or more RADIUS/TACACS+ servers on the switch for authentication. If multiple servers are added, the server that is first added to the group has the highest priority and authenticates the users trying to access the switch. The others act as backup servers in case the first one breaks down.

- Adding RADIUS Server

Choose the menu **SECURITY > AAA > RADIUS Config** and click Add to load the following page.

Figure 2-1 RADIUS Server Configuration



Follow these steps to add a RADIUS server:

1) Configure the following parameters.

Server IP	Enter the IP address of the server running the RADIUS secure protocol.
Shared Key	Enter the shared key between the RADIUS server and the switch. The RADIUS server and the switch use the key string to encrypt passwords and exchange responses.
Authentication Port	Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812.

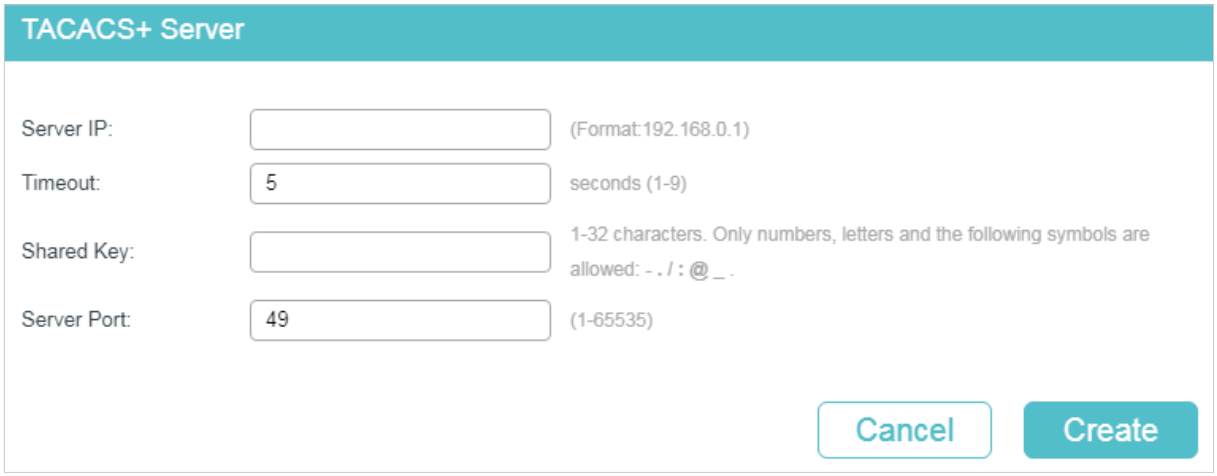
Accounting Port	Specify the UDP destination port on the RADIUS server for accounting requests. The default setting is 1813. Usually, it is used in the 802.1x feature.
Retransmit	Specify the number of times a request is resent to the server if the server does not respond. The default setting is 2.
Timeout	Specify the time interval that the switch waits for the server to reply before resending. The default setting is 5 seconds.
NAS Identifier	Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself.

2) Click **Create** to add the RADIUS server on the switch.

■ Adding TACACS+ Server

Choose the menu **SECURITY > AAA > TACACS+ Config** and click Add to load the following page.

Figure 2-2 TACACS+ Server Configuration



Follow these steps to add a TACACS+ server:

1) Configure the following parameters.

Server IP	Enter the IP address of the server running the TACACS+ secure protocol.
Timeout	Specify the time interval that the switch waits for the server to reply before resending. The default setting is 5 seconds.
Shared Key	Enter the shared key between the TACACS+ server and the switch. The TACACS+ server and the switch use the key string to encrypt passwords and exchange responses.
Server Port	Specify the TCP port used on the TACACS+ server for AAA. The default setting is 49.

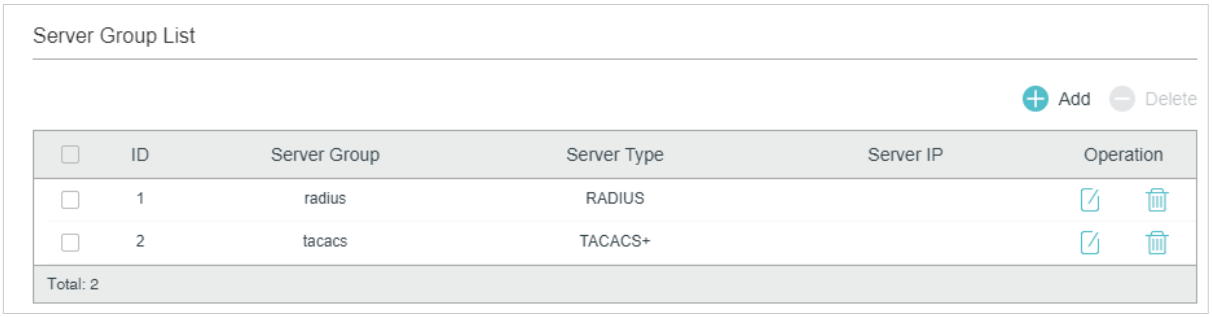
2) Click **Create** to add the TACACS+ server on the switch.

2.1.2 Configuring Server Groups

The switch has two built-in server groups, one for RADIUS servers and the other for TACACS+ servers. The servers running the same protocol are automatically added to the default server group. You can add new server groups as needed.

Choose the menu **SECURITY > AAA > Server Group** to load the following page.

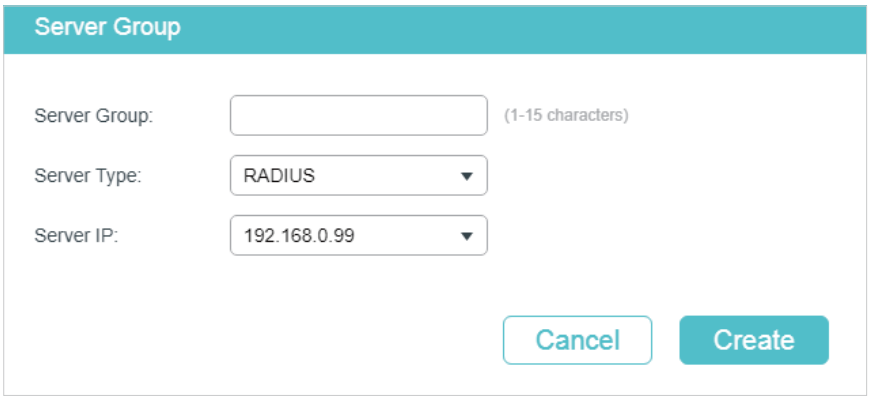
Figure 2-3 Add New Server Group



There are two default server groups in the list. You can edit the default server groups or follow these steps to configure a new server group:

1) Click Add and the following window will pop up.

Figure 2-4 Add Server Group



Configure the following parameters:

Server Group	Specify a name for the server group.
Server Type	Select the server type for the group. The following options are provided: RADIUS and TACACS+.
Server IP	Select the IP address of the server which will be added to the server group.

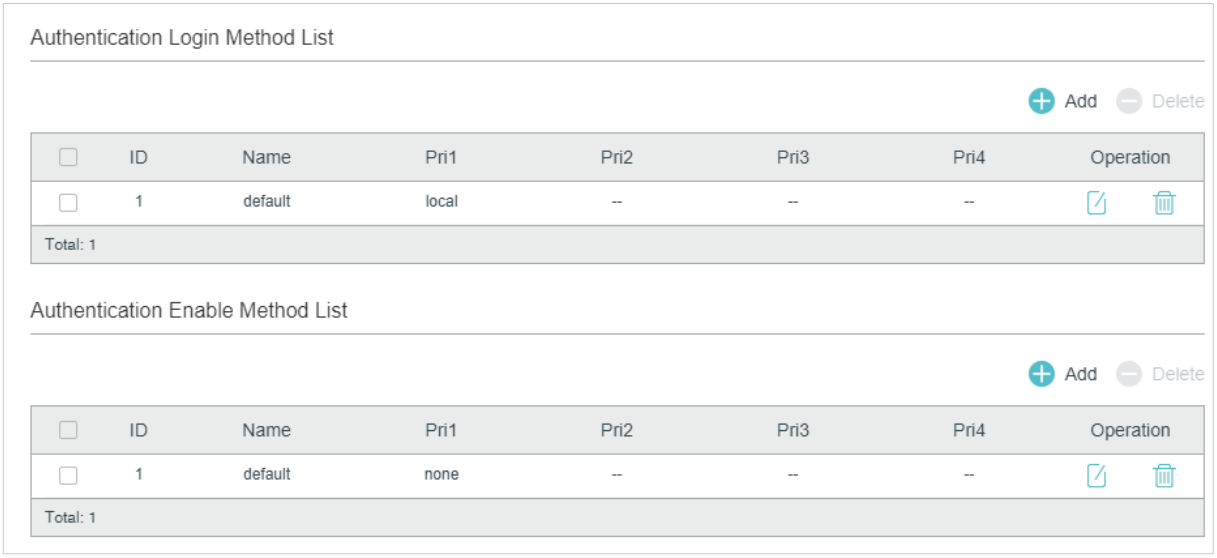
2) Click **Create**.

2.1.3 Configuring the Method List

A method list describes the authentication methods and their sequence to authenticate the users. The switch supports Login Method List for users of all types to gain access to the switch, and Enable Method List for guests to get administrative privileges.

Choose the menu **SECURITY > AAA > Method List** to load the following page.

Figure 2-5 Method List

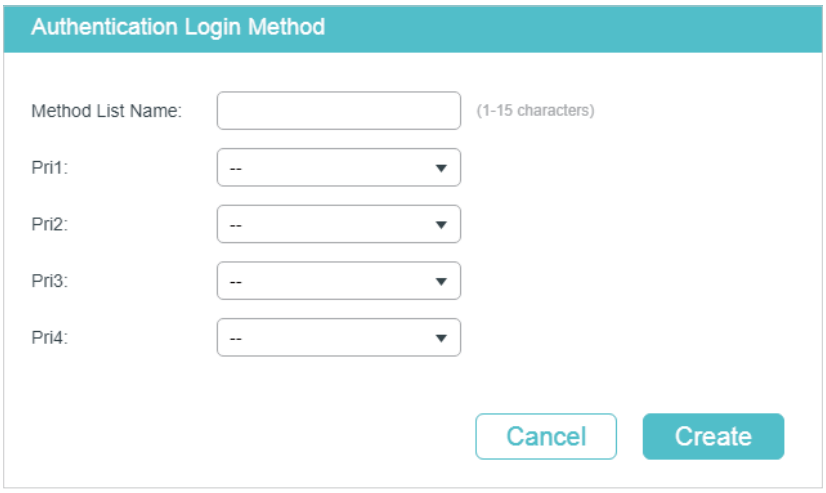


There are two default methods respectively for the Login authentication and the Enable authentication.

You can edit the default methods or follow these steps to add a new method:

1) Click Add in the **Authentication Login Method List** section or **Authentication Enable Method List** section to add corresponding type of method list. The following window will pop up.

Figure 2-6 Add New Method



Configure the parameters for the method to be added.

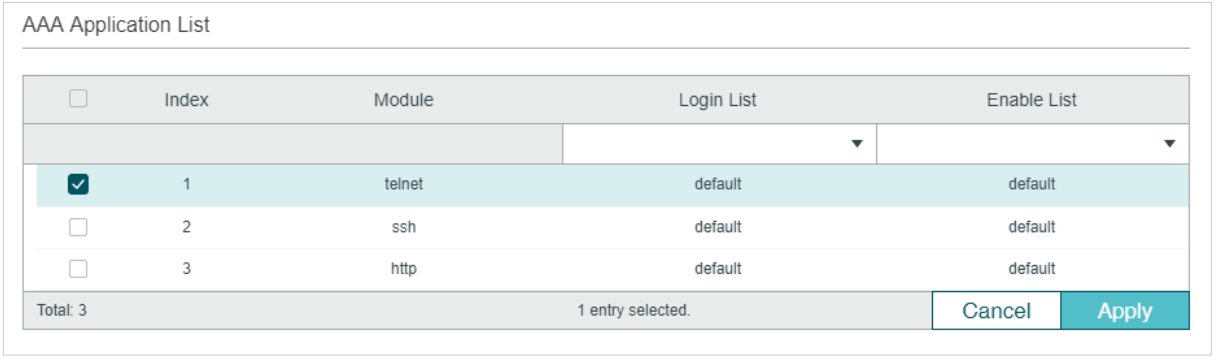
Method List Name	Specify a name for the method.
Pri1- Pri4	Specify the authentication methods in order. The method with priority 1 authenticates a user first, the method with priority 2 is tried if the previous method does not respond, and so on. **local**: Use the local database in the switch for authentication. **none**: No authentication is used. **radius**: Use the remote RADIUS server/server groups for authentication. **tacacs**: Use the remote TACACS+ server/server groups for authentication. **Other user-defined server groups**: Use the user-defined server groups for authentication.

2) Click **Create** to add the new method.

2.1.4 Configuring the AAA Application List

Choose the menu **SECURITY > AAA > Global Config** to load the following page.

Figure 2-7 Configure Application List



Follow these steps to configure the AAA application list.

1) In the **AAA Application List** section, select an access application and configure the Login list and Enable list.

Module	Displays the configurable applications on the switch: console, telnet, ssh and http. **Note**: Console is only available on certain devices.
Login List	Select a previously configured Login method list. This method list will authenticate the users trying to log in to the switch.
Enable List	Select a previously configured Enable method list. This method list will authenticate the users trying to get administrative privileges.

2) Click **Apply**.

2.1.5 Configuring Login Account and Enable Password

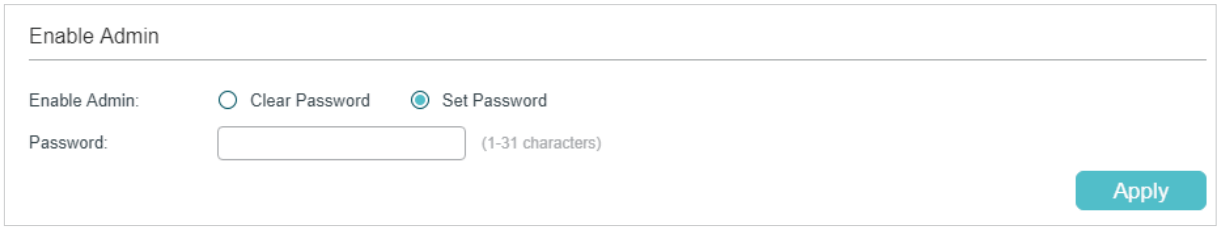
The login account and Enable password can be configured locally on the switch or centrally on the RADIUS/TACACS+ server(s).

On the Switch

The local username and password for login can be configured in the User Management feature. For details, refer to Managing System.

To configure the local Enable password for getting administrative privileges, choose the menu **SECURITY > AAA > Global Config** to load the following page.

Figure 2-8 Configure Enable Password



There are two options: **Clear Password** and **Set Password**. You can choose whether the local Enable password is required when the guests try to get administrative privileges. Click **Apply**.

Tips: The logged-in guests can enter the local Enable password on this page to get administrative privileges.

On the Server

The accounts created by the RADIUS/TACACS+ server can only view the configurations and some network information without the Enable password.

Some configuration principles on the server are as follows:

- For Login authentication configuration, more than one login account can be created on the server. Besides, both the user name and password can be customized.

- For Enable password configuration:

  On RADIUS server, the user name should be set as **$enable$**, and the Enable password is customizable. All the users trying to get administrative privileges share this Enable password.

  On TACACS+ server, configure the value of “enable 15” as the Enable password in the configuration file. All the users trying to get administrative privileges share this Enable password.

2.2 Using the CLI

2.2.1 Adding Servers

You can add one or more RADIUS/TACACS+ servers on the switch for authentication. If multiple servers are added, the server with the highest priority authenticates the users trying to access the switch, and the others act as backup servers in case the first one breaks down.

■ Adding RADIUS Server

Follow these steps to add RADIUS server on the switch:

Step 1	**configure** Enter global configuration mode.
Step 2	**radius-server host** *ip-address* **[auth-port** *port-id* **] [acct-port** *port-id* **] [timeout** *time* **] [retransmit** *number* **] [nas-id** *nas-id* **] key {** [0] *string* **|** 7 *encrypted-string* **}** Add the RADIUS server and configure the related parameters as needed. **host** *ip-address*: Enter the IP address of the server running the RADIUS protocol. **auth-port** *port-id*: Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812. **acct-port** *port-id*: Specify the UDP destination port on the RADIUS server for accounting requests. The default setting is 1813. Usually, it is used in the 802.1X feature. **timeout** *time*: Specify the time interval that the switch waits for the server to reply before resending. The valid values are from 1 to 9 seconds and the default setting is 5 seconds. **retransmit** *number*: Specify the number of times a request is resent to the server if the server does not respond. The valid values are from 1 to 3 and the default setting is 2. **nas-id** *nas-id*: Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself. **key {** [0] *string* **|** 7 *encrypted-string* **}**: Specify the shared key. 0 and 7 represent the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. *string* is the shared key for the switch and the server. *encrypted-string* is a symmetric encrypted key with a fixed length, which you can copy from the configuration file of another switch. The key or encrypted-key you configure here will be displayed in the encrypted form.
Step 3	**show radius-server** Verify the configuration of RADIUS server.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to add a RADIUS server on the switch. Set the IP address of the server as 192.168.0.10, the authentication port as 1812, the shared key as 123456, the timeout as 8 seconds and the retransmit number as 3.

Switch#configure

Switch(config)#radius-server host 192.168.0.10 **auth-port** 1812 **timeout** 8 **retransmit** 3 **key** 123456

Switch(config)#show radius-server

Server Ip	Auth Port	Acct Port	Timeout	Retransmit	NAS Identifier	Shared key
192.168.0.10	1812	1813	5	2	000AEB132397	123456

Switch(config)#end

Switch#copy running-config startup-config

Adding TACACS+ Server

Follow these steps to add TACACS+ server on the switch:

Step 1	**configure** Enter global configuration mode.
Step 2	**tacacs-server host** *ip-address* **[port** *port-id* **] [timeout** *time* **] [key {** [0] *string* **|** 7 *encrypted-string* **}]** Add the RADIUS server and configure the related parameters as needed. **host** *ip-address*: Enter the IP address of the server running the TACACS+ protocol. **port** *port-id*: Specify the TCP destination port on the TACACS+ server for authentication requests. The default setting is 49. **timeout** *time*: Specify the time interval that the switch waits for the server to reply before resending. The valid values are from 1 to 9 seconds and the default setting is 5 seconds. **key {** [0] *string* **|** 7 *encrypted-string* **}**: Specify the shared key. 0 and 7 represent the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. *string* is the shared key for the switch and the server. *encrypted-string* is a symmetric encrypted key with a fixed length, which you can copy from the configuration file of another switch. The key or encrypted-key you configured here will be displayed in the encrypted form.
Step 3	**show tacacs-server** Verify the configuration of TACACS+ server.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to add a TACACS+server on the switch. Set the IP address of the server as 192.168.0.20, the authentication port as 49, the shared key as 123456, and the timeout as 8 seconds.

Switch#configure

Switch(config)#tacacs-server host 192.168.0.20 **auth-port** 49 **timeout** 8 **key** 123456

Switch(config)#show tacacs-server

Server Ip	Port	Timeout	Shared key
192.168.0.20	49	8	123456

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring Server Groups

The switch has two built-in server groups, one for RADIUS and the other for TACACS+. The servers running the same protocol are automatically added to the default server group. You can add new server groups as needed.

The two default server groups cannot be deleted or edited. Follow these steps to add a server group:

Step 1	**configure** Enter global configuration mode.
Step 2	**aaa group {** radius | tacacs **}** *group-name* Create a server group. radius | tacacs: Specify the group type. *group-name*: Specify a name for the group.
Step 3	**server** *ip-address* Add the existing servers to the server group. *ip-address*: Specify IP address of the server to be added to the group.
Step 4	**show aaa group** [*group-name*] Verify the configuration of server group.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a RADIUS server group named RADIUS1 and add the existing two RADIUS servers whose IP address is 192.168.0.10 and 192.168.0.20 to the group.

Switch#configure

Switch(config)#aaa group radius RADIUS1

Switch(aaa-group)#server 192.168.0.10

Switch(aaa-group)#server 192.168.0.20

Switch(aaa-group)#show aaa group RADIUS1

192.168.0.10

192.168.0.20

Switch(aaa-group)#end

Switch#copy running-config startup-config

2.2.3 Configuring the Method List

A method list describes the authentication methods and their sequence to authenticate the users. The switch supports Login Method List for users of all types to gain access to the switch, and Enable Method List for guests to get administrative privileges.

Follow these steps to configure the method list:

Step 1	**configure** Enter global configuration mode.
Step 2	**aaa authentication login {** *method-list* **} {** *method1* **} [** *method2* **] [** *method3* **] [** *method4* **]** Configure a login method list. *method-list*: Specify a name for the method list. *method1*/*method2*/*method3*/*method4*: Specify the authentication methods in order. The first method authenticates a user first, the second method is tried if the previous method does not respond, and so on. The default methods include radius, tacacs, local and none. None means no authentication is used for login.
Step 3	**aaa authentication enable {** *method-list* **} {** *method1* **} [** *method2* **] [** *method3* **] [** *method4* **]** Configure an Enable password method list. *method-list*: Specify a name for the method list. *method1*/*method2*/*method3*/*method4*: Specify the authentication methods in order. The default methods include radius, tacacs, local and none. None means no authentication is used for getting administrative privileges.
Step 4	**show aaa authentication** [login | enable] Verify the configuration method list.

Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a Login method list named Login1, and configure the method 1 as the default radius server group and the method 2 as local.

Switch#configure

Switch(config)##aaa authentication login Login1 radius local

Switch(config)#show aaa authentication login

Methodlist	pri1	pri2	pri3	pri4
default	local	--	--	--
Login1	radius	local	--	--

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to create an Enable method list named Enable1, and configure the method 1 as the default radius server group and the method 2 as local.

Switch#configure

Switch(config)##aaa authentication enable Enable1 radius local

Switch(config)#show aaa authentication enable

Methodlist	pri1	pri2	pri3	pri4
default	local	--	--	--
Enable1	radius	local	--	--

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Configuring the AAA Application List

You can configure authentication method lists on the following access applications: Console, Telnet, SSH and HTTP.

Console

Note:

Console is only available on certain devices.

Follow these steps to apply the Login and Enable method lists for the application Console:

Step 1	**configure** Enter global configuration mode.
Step 2	**line console** *linenum* Enter line configuration mode. *linenum*: Enter the number of users allowed to login through console port. Its value is 0 in general, for the reason that console input is only active on one console port at a time.
Step 3	**login authentication {** *method-list* **}** Apply the Login method list for the application Console. *method-list*: Specify the name of the Login method list.
Step 4	**enable authentication {** *method-list* **}** Apply the Enable method list for the application Console. *method-list*: Specify the name of the Enable method list.
Step 5	**show aaa global** Verify the configuration of application list.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to apply the existing Login method list named Login1 and Enable method list named Enable1 for the application Console.

Switch#configure

Switch(config)#line console 0

Switch(config-line)#login authentication Login1

Switch(config-line)#enable authentication Enable1

Switch(config-line)#show aaa global

Module	Login List	Enable List
Console	Login1	Enable1

Telnet default default

Ssh default default

Http default default

Switch(config-line)#end

Switch#copy running-config startup-config

Telnet

Follow these steps to apply the Login and Enable method lists for the application Telnet:

Step 1	**configure** Enter global configuration mode.
Step 2	**line telnet** Enter line configuration mode.
Step 3	**login authentication {** *method-list* **}** Apply the Login method list for the application Telnet. *method-list*: Specify the name of the Login method list.
Step 4	**enable authentication {** *method-list* **}** Apply the Enable method list for the application Telnet. *method-list*: Specify the name of the Enable method list.
Step 5	**show aaa global** Verify the configuration of application list.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to apply the existing Login method list named Login1 and Enable method list named Enable1 for the application Telnet.

Switch#configure

Switch(config)#line telnet

Switch(config-line)#login authentication Login1

Switch(config-line)#enable authentication Enable1

Switch(config-line)#show aaa global

Module Login List Enable List

Telnet Login1 Enable1

Ssh default default

Http default default

Switch(config-line)#end

Switch#copy running-config startup-config

■ SSH

Follow these steps to apply the Login and Enable method lists for the application SSH:

Step 1	**configure** Enter global configuration mode.
Step 2	**line ssh** Enter line configuration mode.
Step 3	**login authentication {** *method-list* **}** Apply the Login method list for the application SSH. *method-list*: Specify the name of the Login method list.
Step 4	**enable authentication {** *method-list* **}** Apply the Enable method list for the application SSH. *method-list*: Specify the name of the Enable method list.
Step 5	**show aaa global** Verify the configuration of application list.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to apply the existing Login method list named Login1 and Enable method list named Enable1 for the application SSH.

Switch#configure

Switch(config)#line ssh

Switch(config-line)#login authentication Login1

Switch(config-line)#enable authentication Enable1

Switch(config-line)#show aaa global

Module Login List Enable List

Telnet default default

Ssh Login1 Enable1

Http default default

Switch(config-line)#end

Switch#copy running-config startup-config

■ HTTP

Follow these steps to apply the Login and Enable method lists for the application HTTP:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip http login authentication {** *method-list* **}** Apply the Login method list for the application HTTP. *method-list*: Specify the name of the Login method list.
Step 3	**ip http enable authentication {** *method-list* **}** Apply the Enable method list for the application HTTP. *method-list*: Specify the name of the Enable method list.
Step 4	**show aaa global** Verify the configuration of application list.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to apply the existing Login method list named Login1 and Enable method list named Enable1 for the application HTTP:

Switch#configure

Switch(config)#ip http login authentication Login1

Switch(config)#ip http enable authentication Enable1

Switch(config)#show aaa global

Module Login List Enable List

Telnet default default

Ssh default default

Http Login1 Enable1

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Configuring Login Account and Enable Password

The login account and Enable password can be configured locally on the switch or centrally on the RADIUS/TACACS+ server(s).

- On the Switch

The local username and password for login can be configured in the User Management feature. For details, refer to Managing System.

To configure the local Enable password for getting administrative privileges, follow these steps:

Step 1	**configure** Enter global configuration mode.
Step 2	Use the following command to create an enable password unencrypted or symmetric encrypted. **enable admin password {** [0] *password* **|** 7 *encrypted-password* **}** 0 indicates that an unencrypted key will follow. *password* is a string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are **!$%'()*,-./[]_{|}**. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. *encrypted-password* is a symmetric encrypted key with a fixed length, which you can copy from the configuration file of another switch. The key or encrypted-key you configured here will be displayed in the encrypted form. Use the following command to create an enable password unencrypted or MD5 encrypted. **enable admin secret {** [0] *password* **|** 5 *encrypted-password* **}** 0 indicates that an unencrypted key will follow. *password* is a string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are **!$%'()*,-./[]_{|}**. 5 indicates that an MD5 encrypted password with fixed length will follow. By default, the encryption type is 0. *encrypted-password* is an MD5 encrypted password with fixed length, which you can copy from another switch's configuration file.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

On the Server

The accounts created by the RADIUS/TACACS+ server can only view the configurations and some network information without the Enable password.

Some configuration principles on the server are as follows:

- For Login authentication configuration, more than one login account can be created on the server. Besides, both the user name and password can be customized.

- For Enable password configuration:

  On RADIUS server, the user name should be set as **$enable$**, and the Enable password is customizable. All the users trying to get administrative privileges share this Enable password.

  On TACACS+ server, configure the value of "enable 15" as the Enable password in the configuration file. All the users trying to get administrative privileges share this Enable password.

Tips: The logged-in guests can get administrative privileges by using the command **enable-admin** and providing the Enable password.

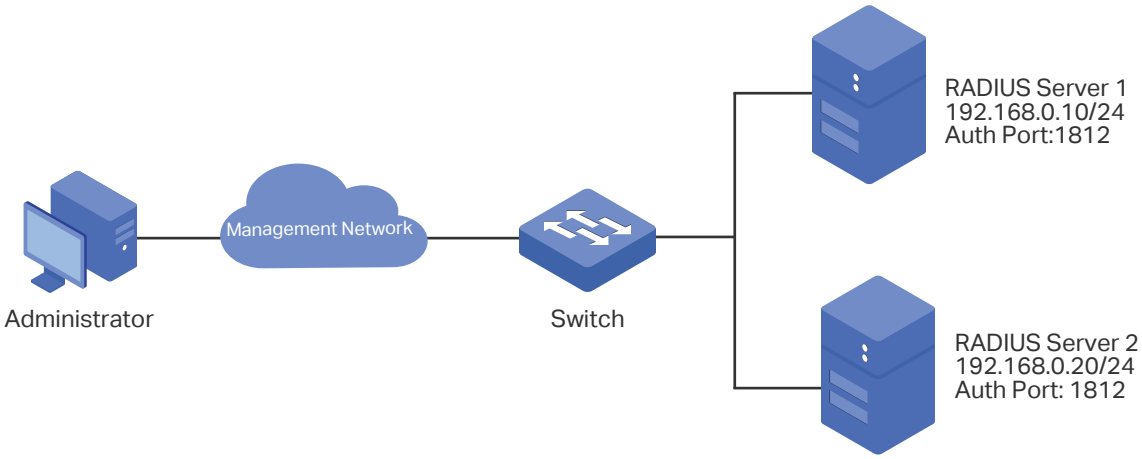
3 Configuration Example

3.1 Network Requirements

As shown below, the switch needs to be managed remotely via Telnet. In addition, the senior administrator of the company wants to create an account for the less senior administrators, who can only view the configurations and some network information without the Enable password provided.

Two RADIUS servers are deployed in the network to provide a safer authenticate method for the administrators trying to log in or get administrative privileges. If RADIUS Server 1 breaks down and doesn't respond to the authentication request, RADIUS Server 2 will work, so as to ensure the stability of the authentication system.

Figure 3-1 Network Topology



3.2 Configuration Scheme

To implement this requirement, the senior administrator can create the login account and the Enable password on the two RADIUS servers, and configure the AAA feature on the switch. The IP addresses of the two RADIUS servers are 192.168.0.10/24 and 192.168.0.20/24; the authentication port number is 1812; the shared key is 123456.

The overview of configuration on the switch is as follows:

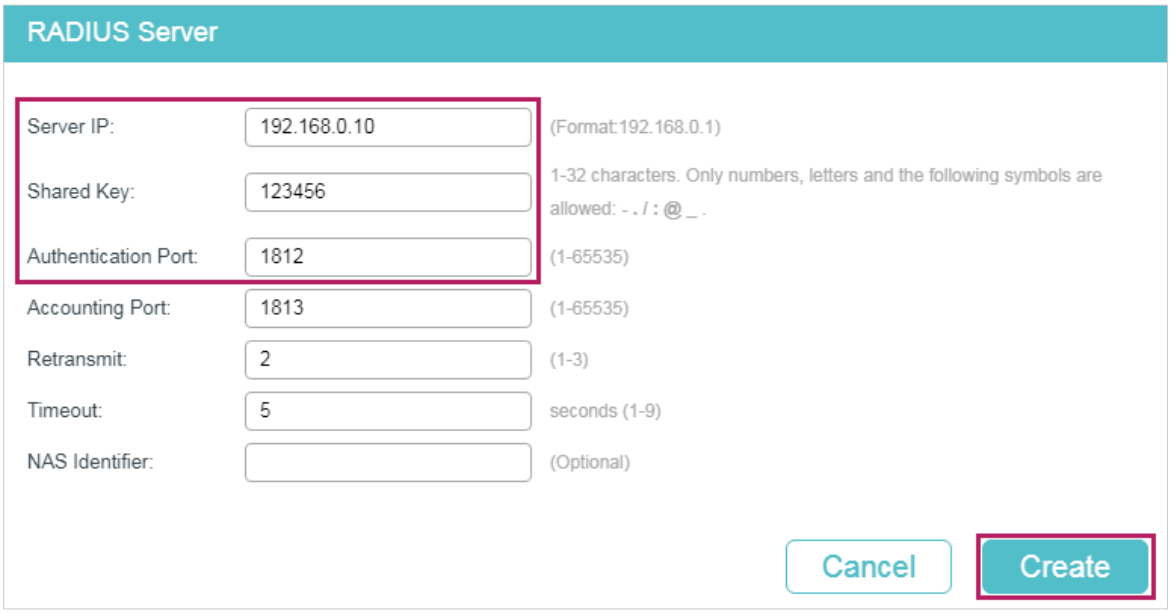
1) Add the two RADIUS servers on the switch.
2) Create a new RADIUS server group and add the two servers to the group. Make sure that RADIUS Server 1 is the first server for authentication.
3) Configure the method list.
4) Configure the AAA application list.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

3.3 Using the GUI

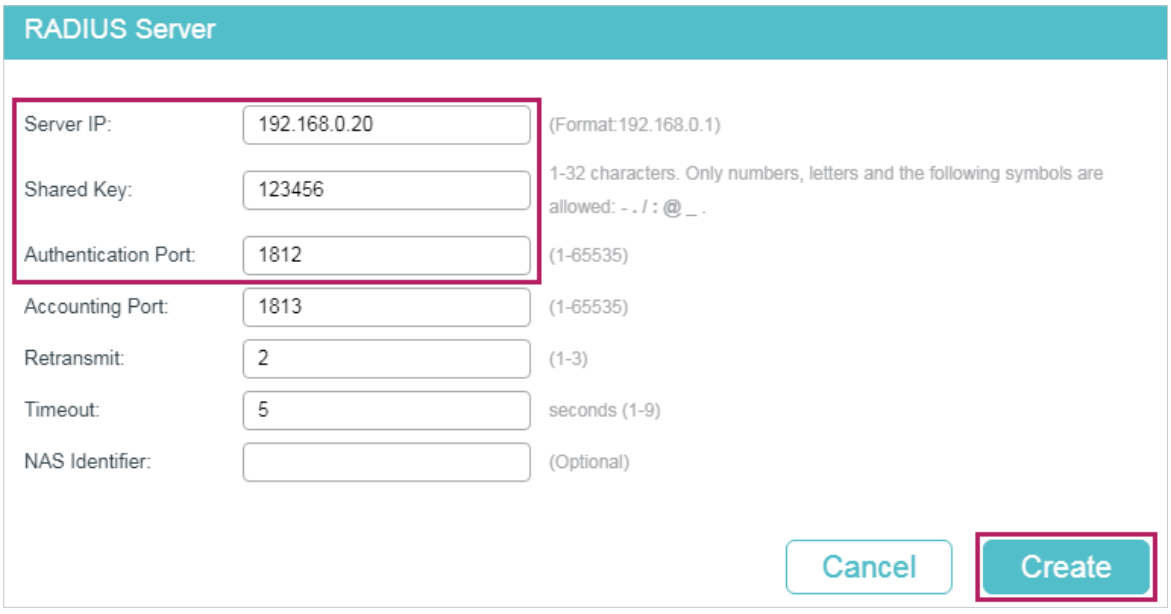
1) Choose the menu **SECURITY > AAA > RADIUS Config** and click Add to load the following page. Configure the Server IP as 192.168.0.10, the Shared Key as 123456, the Authentication Port as 1812, and keep the other parameters as default. Click **Create** to add RADIUS Server 1 on the switch.

Figure 3-2 Add RADIUS Server 1



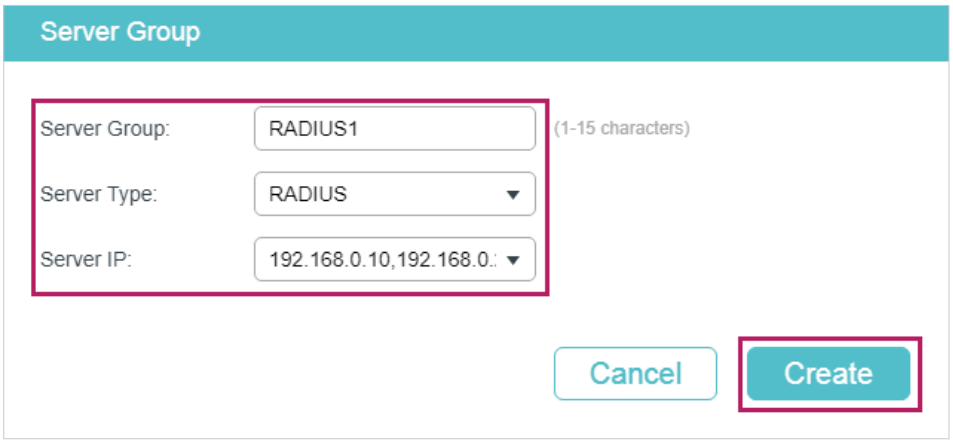
2) On the same page, click Add to load the following page. Configure the Server IP as 192.168.0.20, the Shared Key as 123456, the Auth Port as 1812, and keep the other parameters as default. Click **Create** to add RADIUS Server 2 on the switch

Figure 3-3 Add RADIUS Server 2



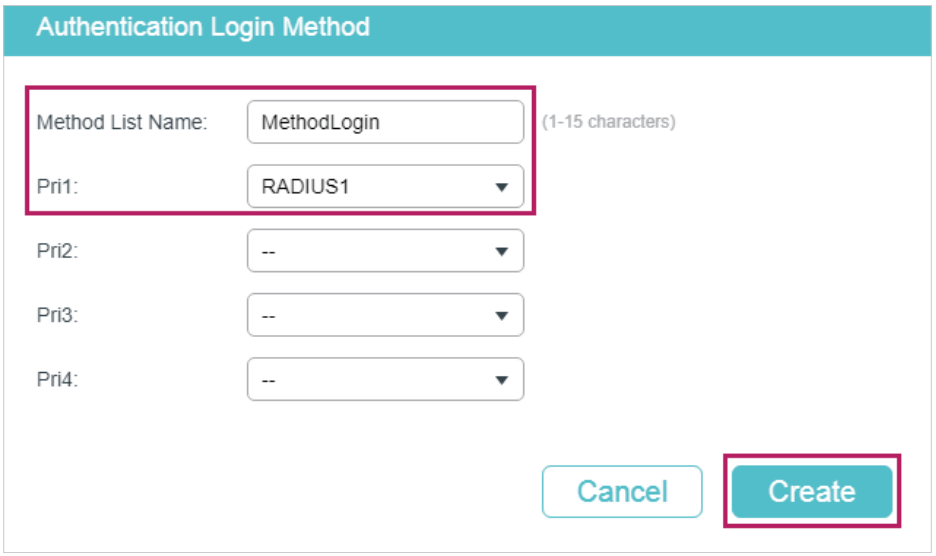
3) Choose the menu **SECURITY > AAA > Server Group** to load the following page. Click Add. Specify the group name as RADIUS1 and the server type as RADIUS. Select 192.168.0.10 and 192.168.0.20 to from the drop-down list. Click **Create** to create the server group.

Figure 3-4 Create Server Group



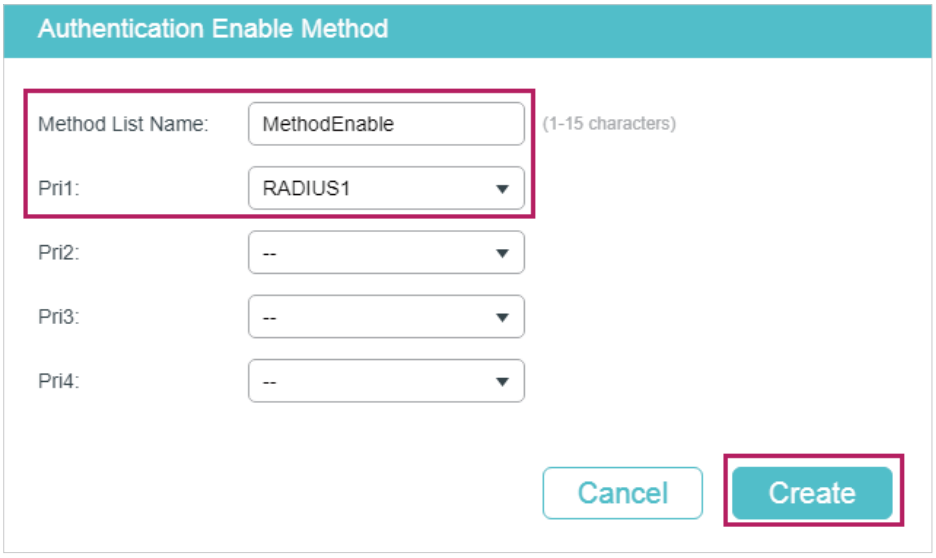
4) Choose the menu **SECURITY > AAA > Method List** and click Add in the **Authentication Login Method List** section. Specify the Method List Name as MethodLogin and select the Pri1 as RADIUS1. Click **Create** to set the method list for the Login authentication.

Figure 3-5 Configure Login Method List



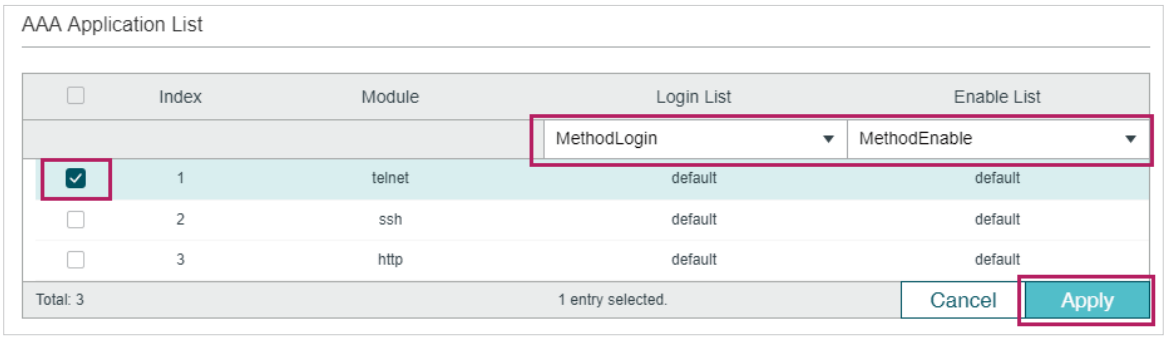
5) On the same page, click Add in the **Authentication Eanble Method List** section. Specify the Method List Name as MethodEnable and select the Pri1 as RADIUS1. Click **Create** to set the method list for the Enable password authentication.

Figure 3-6 Configure Enable Method List



6) Choose the menu **SECURITY > AAA > Global Config** to load the following page. In the **AAA Application List** section, select telnet and configure the Login List as Method-Login and Enable List as Method-Enable. Then click **Apply**.

Figure 3-7 Configure AAA Application List



7) Click Save to save the settings.

3.4 Using the CLI

1) Add RADIUS Server 1 and RADIUS Server 2 on the switch.

Switch(config)#radius-server host 192.168.0.10 auth-port 1812 key 123456

Switch(config)#radius-server host 192.168.0.20 auth-port 1812 key 123456

2) Create a new server group named RADIUS1 and add the two RADIUS servers to the server group.

Switch(config)#aaa group radius RADIUS1

Switch(aaa-group)#server 192.168.0.10

Switch(aaa-group)#server 192.168.0.20

Switch(aaa-group)#exit

3) Create two method lists: Method-Login and Method-Enable, and configure the server group RADIUS1 as the authentication method for the two method lists.

Switch(config)#aaa authentication login Method-Login RADIUS1

Switch(config)#aaa authentication enable Method-Enable RADIUS1

4) Configure Method-Login and Method-Enable as the authentication method for the Telnet application.

Switch(config)#line telnet

Switch(config-line)#login authentication Method-Login

Switch(config-line)#enable authentication Method-Enable

Switch(config-line)#end

Switch#copy running-config startup-config

Verify the Configuration

Verify the configuration of the RADIUS servers:

Switch#show radius-server

Server Ip	Auth Port	Acct Port	Timeout	Retransmit	NAS Identifier	Shared key
192.168.0.10	1812	1813	5	2	000AEB132397	123456
192.168.0.20	1812	1813	5	2	000AEB132397	123456

Verify the configuration of server group RADIUS1:

Switch#show aaa group RADIUS1

192.168.0.10

192.168.0.20

Verify the configuration of the method lists:

Switch#show aaa authentication

Authentication Login Methodlist:

Methodlist	pri1	pri2	pri3	pri4
default	local	--	--	--
Method-Login	RADIUS1	--	--	--

Authentication Enable Methodlist:

Methodlist	pri1	pri2	pri3	pri4

```
default              none          --        --        --
Method-Enable   RADIUS1     --        --        --
...
```

Verify the status of the AAA feature and the configuration of the AAA application list:

```
Switch#show aaa global
Module          Login List          Enable List
Telnet          Method-Login        Method-Enable
SSH             default             default
Http            default             default
```

4 Appendix: Default Parameters

Default settings of AAA are listed in the following tables.

Table 4-1 AAA

Parameter	Default Setting
Global Config	
AAA Feature	Enabled
RADIUS Config	
Server IP	None
Shared Key	None
Auth Port	1812
Acct Port	1813
Retransmit	2
Timeout	5 seconds
NAS Identifier	The MAC address of the switch.
TACACS+ Config	
Server IP	None
Timeout	5 seconds
Shared Key	None
Port	49
Server Group: There are two default server groups: radius and tacacs.	
Method List	
Authentication Login Method List	List name: default Pri1: local
Authentication Enable Method List	List name: default Pri1: none

Parameter	Default Setting
AAA Application List	
console	Login List: default Enable List: default
telnet	Login List: default Enable List: default
ssh	Login List: default Enable List: default
http	Login List: default Enable List: default

Part 25

Configuring 802.1x

CHAPTERS

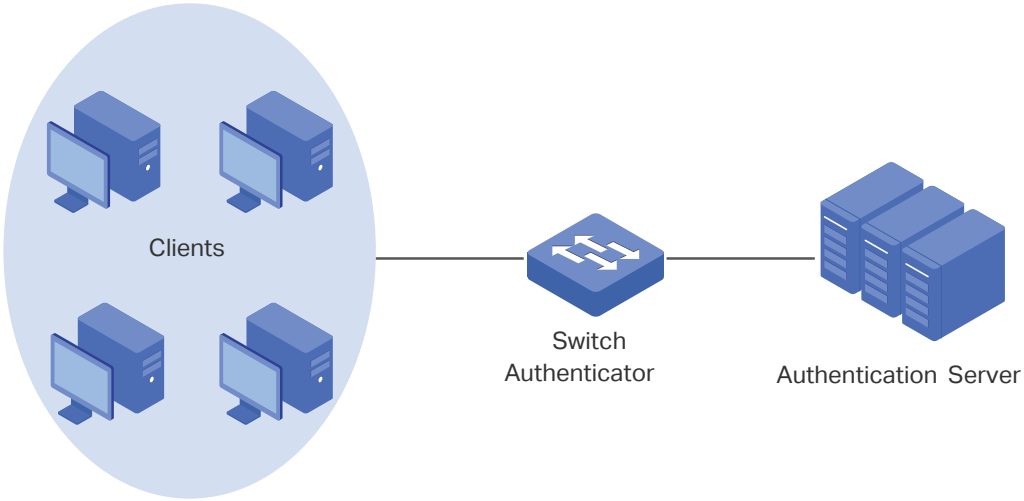
1. Overview
2. 802.1x Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

802.1x protocol is a protocol for port-based Network Access Control. It is used to authenticate and control access from devices connected to the ports. If the device connected to the port is authenticated by the authentication server successfully, its request to access the LAN will be accepted; if not, its request will be denied.

802.1x authentication uses client-server model which contains three device roles: client/supplicant, authenticator and authentication server. This is described in the figure below:

Figure 1-1 802.1x Authentication Model



- Client

A client, usually a computer, is connected to the authenticator via a physical port. We recommend that you install TP-Link 802.1x authentication client software on the client hosts, enabling them to request 802.1x authentication to access the LAN.

- Authenticator

An authenticator is usually a network device that supports 802.1x protocol. As the above figure shows, the switch is an authenticator.

The authenticator acts as an intermediate proxy between the client and the authentication server. The authenticator requests user information from the client and sends it to the authentication server; also, the authenticator obtains responses from the authentication server and send them to the client. The authenticator allows authenticated clients to access the LAN through the connected ports but denies the unauthenticated clients.

- Authentication Server

The authentication server is usually the host running the RADIUS server program. It stores information of clients, confirms whether a client is legal and informs the authenticator whether a client is authenticated.

2 802.1x Configuration

To complete the 802.1x configuration, follow these steps:

1) Configure the RADIUS server.
2) Configure 802.1x globally.
3) Configure 802.1x on ports.

In addition, you can view the authenticator state.

Configuration Guidelines

802.1x authentication and Port Security cannot be enabled at the same time. Before enabling 802.1x authentication, make sure that Port Security is disabled.

2.1 Using the GUI

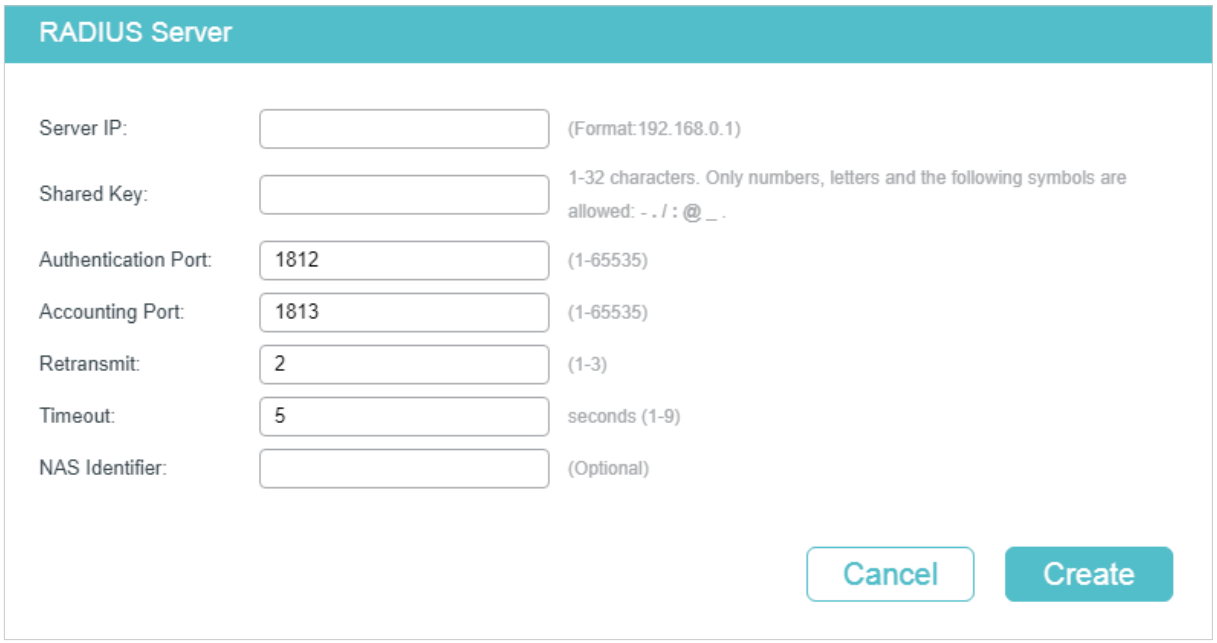
2.1.1 Configuring the RADIUS Server

Configure the parameters of RADIUS sever and configure the RADIUS server group.

- Adding the RADIUS Server

Choose the menu **SECURITY > AAA > RADIUS Config** and click Add to load the following page.

Figure 2-1 Adding RADIUS Server



Follow these steps to add a RADIUS server:

1) Configure the parameters of the RADIUS server.

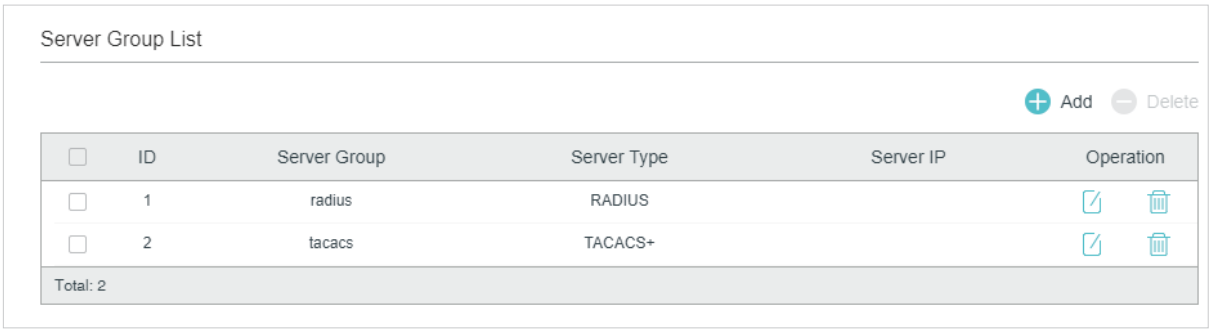
Server IP	Enter the IP address of the server running the RADIUS secure protocol.
Shared Key	Enter the shared key between the RADIUS server and the switch. The RADIUS server and the switch use the key string to encrypt passwords and exchange responses.
Authentication Port	Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812.
Accounting Port	Specify the UDP destination port on the RADIUS server for accounting requests. The default setting is 1813.
Retransmit	Specify the number of times a request is resent to the server if the server does not respond. The default setting is 2.
Timeout	Specify the time interval that the switch waits for the server to reply before resending. The default setting is 5 seconds.
NAS Identifier	Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself.

2) Click **Apply**.

■ Configuring the RADIUS Server Group

Choose the menu **SECURITY > AAA > Server Group** to load the following page.

Figure 2-2 Adding a Server Group

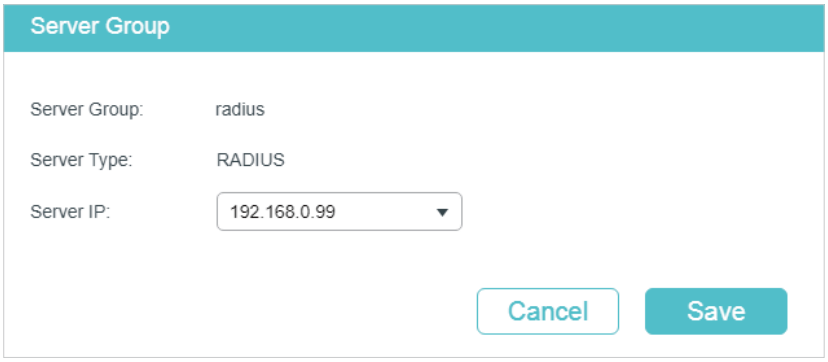


Follow these steps to add the RADIUS server to a server group:

1) Click to edit the default **radius** server group or click Add to add a new server group.

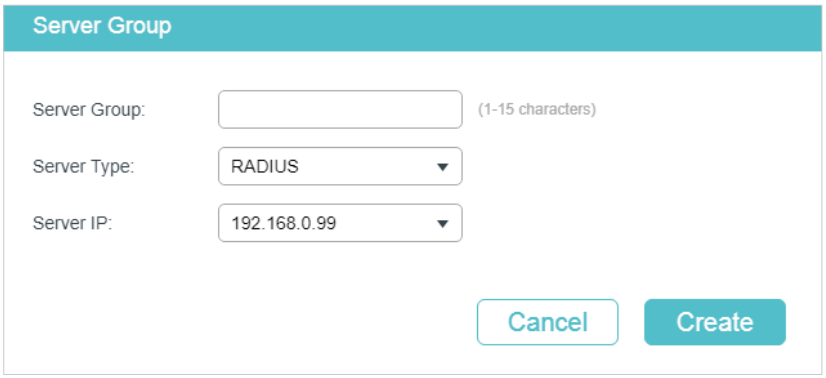
   If you click , the following window will pop up. Select a RADIUS server and click **Save**.

Figure 2-3 Editing Server Group



If you click Add , the following window will pop up. Specify a name for the server group, select the server type as RADIUS and select the IP address of the RADIUS server. Click **Save**.

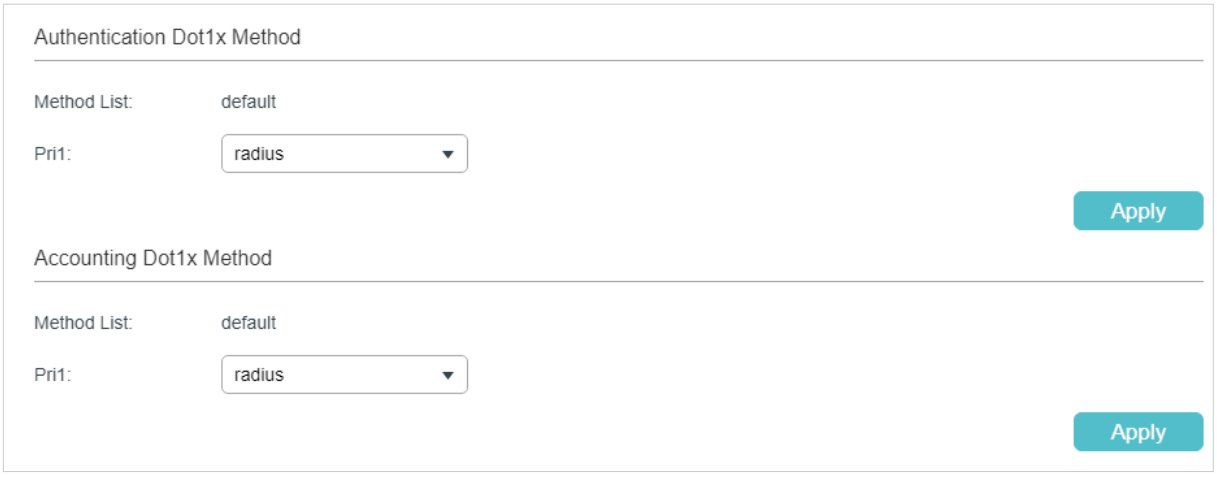
Figure 2-4 Adding Server Group



Configuring the Dot1x List

Choose the menu **SECURITY > AAA > Dot1x List** to load the following page.

Figure 2-5 Configuring the Dot1x List



Follow these steps to configure RADIUS server groups for 802.1x authentication and accounting:

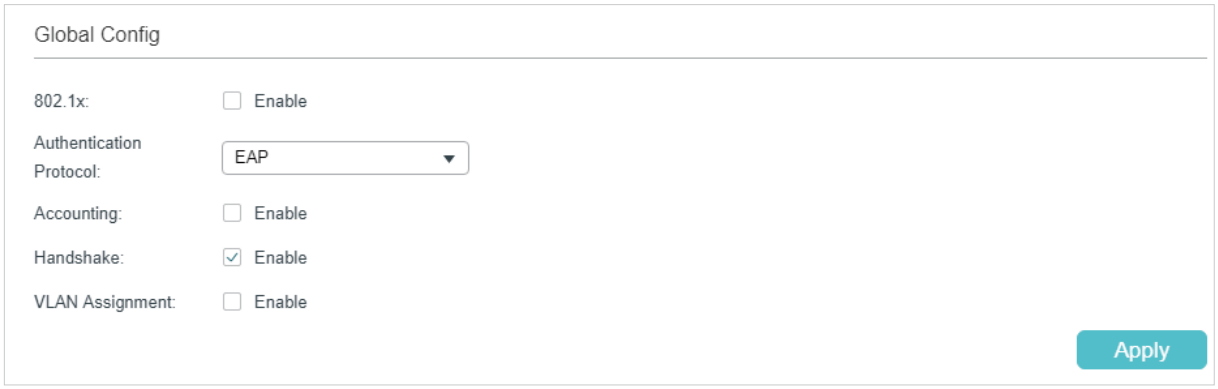
1) In the **Authentication Dot1x Method** section, select an existing RADIUS server group for authentication from the Pri1 drop-down list and click **Apply**.

2) In the **Accounting Dot1x Method** section, select an existing RADIUS server group for accounting from the Pri1 drop-down list and click **Apply**.

2.1.2 Configuring 802.1x Globally

Choose the menu **SECURITY > 802.1x > Global Config** to load the following page.

Figure 2-6 Global Config



Follow these steps to configure 802.1x global parameters:

1) In the **Global Config** section, configure the following parameters.

802.1x	Enable or disable 802.1x globally.
Auth Protocol	Select the 802.1x authentication protocol. **PAP**: The 802.1x authentication system uses EAP packets to exchange information between the switch and the client. The transmission of EAP (Extensible Authentication Protocol) packets is terminated at the switch and the EAP packets are converted to other protocol (such as RADIUS) packets, and transmitted to the authentication server. **EAP**: The 802.1x authentication system uses EAP packets to exchange information between the switch and the client. The EAP packets with authentication data are encapsulated in the advanced protocol (such as RADIUS) packets, and transmitted to the authentication server.
Accounting	Enable or disable 802.1x accounting feature.
Handshake	Enable or disable the Handshake feature. The Handshake feature is used to detect the connection status between the TP-Link 802.1x Client and the switch. Please disable Handshake feature if you are using other client softwares instead of TP-Link 802.1x Client.

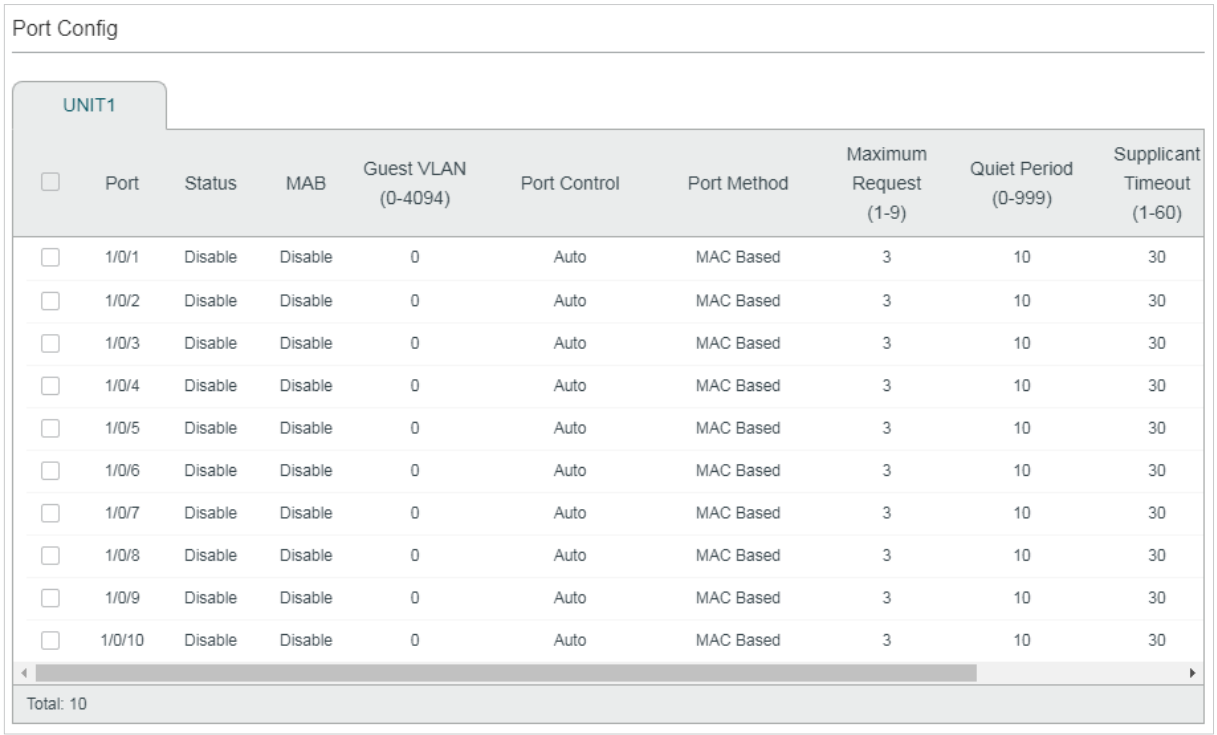
VLAN Assignment	Enable or disable the 802.1x VLAN assignment feature. 802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated. If the assigned VLAN does not exist on the switch, the switch will create the related VLAN automatically, add the authenticated port to the VLAN and change the PVID based on the assigned VLAN. If the assigned VLAN exists on the switch, the switch will directly add the authenticated port to the related VLAN and change the PVID instead of creating a new VLAN. If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication.

2) Click **Apply**.

2.1.3 Configuring 802.1x on Ports

Choose the menu **SECURITY > 802.1x > Port Config** to load the following page.

Figure 2-7 Port Config



Follow these steps to configure 802.1x authentication on the desired port:

1) Select one or more ports and configure the following parameters:

Status	Enable 802.1x authentication on the port.

MAB	Select whether to enable the MAB (MAC-Based Authentication Bypass) feature for the port. With MAB feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1x capability. For example, most printers, IP phones and fax machines do not have 802.1x capability. Note: MAB cannot work if Guest VLAN is enabled.
Guest VLAN	Specify a Guest VLAN ID. 0 means that Guest VLAN is disabled. The configured VLAN must be an existing 802.1Q VLAN. With Guest VLAN enabled, a port can access resources in the guest VLAN even though the port is not yet authenticated; if guest VLAN is disabled and the port is not authenticated, the port cannot visit any resource in the LAN.
Port Control	Select the control mode for the port. By default, it is Auto. **Auto**: If this option is selected, the port can access the network only when it is authenticated. **Force-Authorized**: If this option is selected, the port can access the network without authentication. **Force-Unauthorized**: If this option is selected, the port can never be authenticated.
Port Method	Select the port method. By default, it is MAC Based. **MAC Based**: All clients connected to the port need to be authenticated. **Port Based**: If a client connected to the port is authenticated, other clients can access the LAN without authentication.
Maximum Request (1-9)	Specify the maximum number of attempts to send the authentication packet. It ranges from 1 to 9 times and the default is 3 times.
Quiet Period (1-999)	Specify the Quiet Period. It ranges from 1 to 999 seconds and the default time is 10 seconds. The quiet period starts after the authentication fails. During the quiet period, the switch does not process authentication requests from the same client.
Supplicant Timeout (1-60)	Specify the maximum time which the switch waits for a response from the client. It ranges from 1 to 60 seconds and the default time is 30 seconds. If the switch does not receive any reply from the client within the specified time, it will resend the request.
Authorized	Displays whether the port is authorized or not.
LAG	Displays the LAG the port belongs to.

2) Click **Apply**.

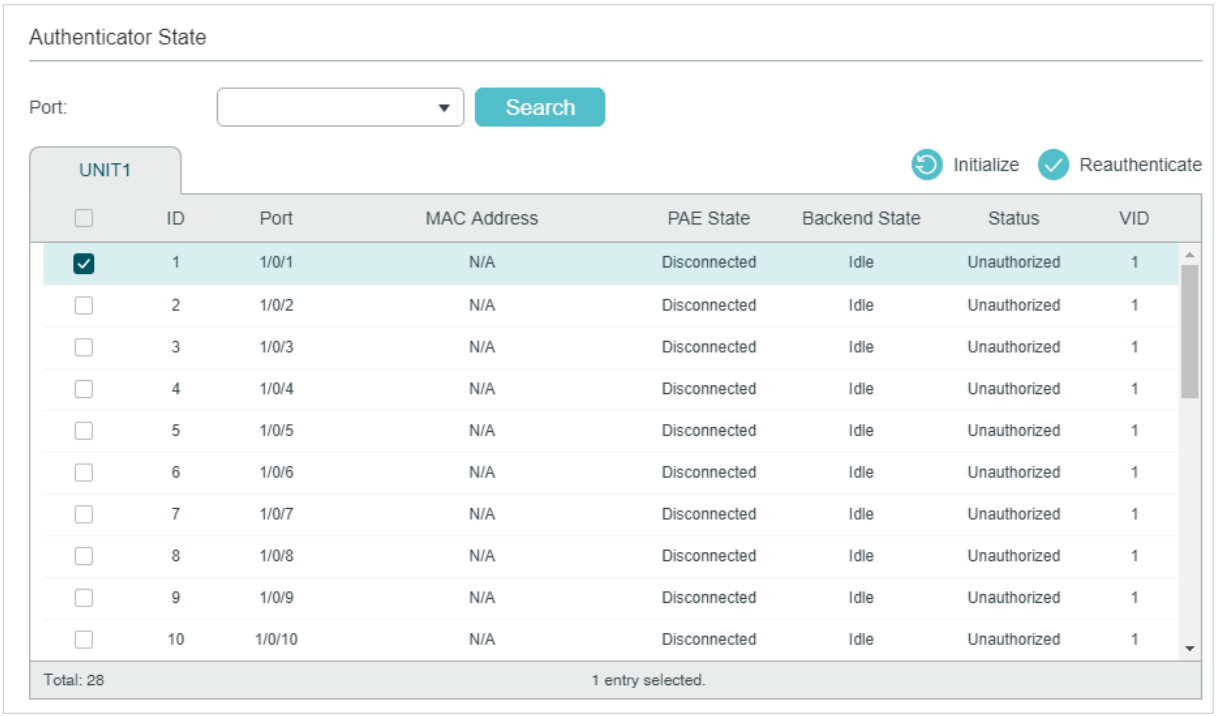
Note:

If a port is in an LAG, its 802.1x authentication function cannot be enabled. Also, a port with 802.1x authentication enabled cannot be added to any LAG.

2.1.4 View the Authenticator State

Choose the menu **SECURITY > 802.1x > Authenticator State** to load the following page.

Figure 2-8 View Authenticator State



On this page, you can view the authentication status of each port:

Port	Displays the port number.
MAC Address	Displays the MAC address of the authenticated device. When the port method is Port Based, the MAC address of the first authenticated device wil be displayed with a suffix “p”.
PAE State	Displays the current state of the authenticator PAE state machine. Possible values are: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized and ForceUnauthorized.
Backend State	Displays the current state of the backend authentication state machine. Possible values are: Request, Response, Success, Fail, Timeout, Initialize and Idle.
Status	Displays whether the port is authorized or not.
VID	Displays the VLAN ID assigned by the authenticator to the supplicant device when the related port is authorized. If the related port is unauthorized and there is a Guest VLAN ID, the Guest VLAN ID will be displayed.

2.2 Using the CLI

2.2.1 Configuring the RADIUS Server

Follow these steps to configure RADIUS:

Step 1	**configure** Enter global configuration mode.
Step 2	**radius-server host** *ip-address* **[auth-port** *port-id* **] [acct-port** *port-id* **] [timeout** *time* **] [retransmit** *number* **] [nas-id** *nas-id* **] key {** [0] *string* **|** 7 *encrypted-string* **}** Add the RADIUS server and configure the related parameters as needed. **host** *ip-address*: Enter the IP address of the server running the RADIUS protocol. **auth-port** *port-id*: Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812. **acct-port** *port-id:* Specify the UDP destination port on the RADIUS server for accounting requests. The default setting is 1813. Generally, the accounting feature is not used in the authentication account management. **timeout** *time*: Specify the time interval that the switch waits for the server to reply before resending. The valid values are from 1 to 9 seconds and the default setting is 5 seconds. **retransmit** *number*: Specify the number of times a request is resent to the server if the server does not respond. The valid values are from 1 to 3 and the default setting is 2. **nas-id** *nas-id:* Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself. **key {** [0] *string* **|** 7 *encrypted-string* **}**: Specify the shared key. 0 and 7 prevent the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. *string* is the shared key for the switch and the server. *encrypted-string* is a symmetric encrypted key with a fixed length, which you can copy from the configuration file of another switch. The key or encrypted-key you configured here will be displayed in the encrypted form.
Step 3	**aaa group** radius *group-name* Create a RADIUS server group. radius: Specify the group type as radius. *group-name*: Specify a name for the group.
Step 4	**server** *ip-address* Add the existing servers to the server group. *ip-address*: Specify IP address of the server to be added to the group.
Step 5	**exit** Return to global configuration mode.

Step 6	**aaa authentication dot1x default** { *method* } Select the RADIUS group for 802.1x authentication. *method:* Specify the RADIUS group for 802.1x authentication. **aaa accounting dot1x default** { *method* } Select the RADIUS group for 802.1x accounting. *method:* Specify the RADIUS group for 802.1x accounting. Note: If multiple RADIUS servers are available, you are suggested to add them to different server groups respectively for authentication and accounting.
Step 7	**show radius-server** (Optional) Verify the configuration of RADIUS server.
Step 8	**show aaa group** [*group-name*] (Optional) Verify the configuration of server group.
Step 9	**show aaa authentication** dot1x (Optional) Verify the authentication method list.
Step 10	**show aaa accounting** dot1x (Optional) Verify the accounting method list.
Step 11	**end** Return to privileged EXEC mode.
Step 12	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable AAA, add a RADIUS server to the server group named radius1, and apply this server group to the 802.1x authentication. The IP address of the RADIUS server is 192.168.0.100; the shared key is 123456; the authentication port is 1812; the accounting port is 1813.

Switch#configure

Switch(config)#radius-server host 192.168.0.100 **auth-port** 1812 **acct-port** 1813 **key** 123456

Switch(config)#aaa group radius radius1

Switch(aaa-group)#server 192.168.0.100

Switch(aaa-group)#exit

Switch(config)#aaa authentication dot1x default radius1

Switch(config)#aaa accounting dot1x default radius1

Switch(config)#show radius-server

Server Ip	Auth Port	Acct Port	Timeout	Retransmit	NAS Identifier	Shared key
192.168.0.100	1812	1813	5	2	000AEB132397	123456

Switch(config)#show aaa group radius1

192.168.0.100

Switch(config)#show aaa authentication dot1x

Methodlist	pri1	pri2	pri3	pri4
default	radius1	--	--	--

Switch(config)#show aaa accounting dot1x

Methodlist	pri1	pri2	pri3	pri4
default	radius1	--	--	--

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring 802.1x Globally

Follow these steps to configure 802.1x globally:

Step 1	**configure** Enter global configuration mode.
Step 2	**dot1x system-auth-control** Enable 802.1x authentication globally.

Step 3	**dot1x auth-protocol** { pap | eap } Configure the 802.1x authentication protocol. pap: Specify the authentication protocol as PAP. If this option is selected, the 802.1x authentication system uses EAP (Extensible Authentication Protocol) packets to exchange information between the switch and the client. The transmission of EAP packets is terminated at the switch and the EAP packets are converted to other protocol (such as RADIUS) packets, and transmitted to the authentication server. eap: Specify the authentication protocol as EAP. If this option is selected, the 802.1x authentication system uses EAP packets to exchange information between the switch and the client. The EAP packets with authentication data are encapsulated in the advanced protocol (such as RADIUS) packets, and transmitted to the authentication server.
Step 4	**dot1x accounting** (Optional) Enable the accounting feature.
Step 5	**dot1x handshake** (Optional) Enable the Handshake feature. The Handshake feature is used to detect the connection status between the TP-Link 802.1x Client and the switch. Please disable Handshake feature if you are using other client softwares instead of TP-Link 802.1x Client.
Step 6	**dot1x vlan-assignment** (Optional) Enable or disable the 802.1x VLAN assignment feature. 802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated. If the assigned VLAN does not exist on the switch, the switch will create the related VLAN automatically, add the authenticated port to the VLAN and change the PVID based on the assigned VLAN. If the assigned VLAN exists on the switch, the switch will directly add the authenticated port to the related VLAN and change the PVID instead of creating a new VLAN. If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication.
Step 7	**show dot1x global** (Optional) Verify global configurations of 802.1x.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable 802.1x authentication, configure PAP as the authentication method and keep other parameters as default:

Switch#configure

Switch(config)#dot1x system-auth-control

Switch(config)#dot1x auth-protocol pap

Switch(config)#show dot1x global

802.1X State: Enabled

Authentication Protocol: PAP

Handshake State: Enabled

802.1X Accounting State: Disabled

802.1X VLAN Assignment State: Disabled

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring 802.1x on Ports

Follow these steps to configure the port:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode. *port:* Enter the ID of the port to be configured.
Step 3	**dot1x** Enable 802.1x authentication for the port.
Step 4	**dot1x mab** Enable the MAB (MAC-Based Authentication Bypass) feature for the port. With MAB feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1x capability. For example, most printers, IP phones and fax machines do not have 802.1x capability. Note: MAB cannot work if Guest VLAN is enabled.

Step 5	**dot1x guest-vlan** *vid* (Optional) Configure guest VLAN on the port. *vid:* Specify the ID of the VLAN to be configured as the guest VLAN. The valid values are from 0 to 4094. 0 means that Guest VLAN is disabled on the port. The configured VLAN must be an existing 802.1Q VLAN. Clients in the guest VLAN can only access resources from specific VLANs. Note: To use Guest VLAN, the control type of the port should be configured as port-based.
Step 6	**dot1x port-control** { auto | authorized-force | unauthorized-force } Configure the control mode for the port. By default, it is auto. auto: If this option is selected, the port can access the network only when it is authenticated. authorized-force: If this option is selected, the port can access the network without authentication. unauthorized-force: If this option is selected, the port can never be authenticated.
Step 7	**dot1x port-method** { mac-based | port-based } Configure the control type for the port. By default, it is mac-based. mac-based**:** All clients connected to the port need to be authenticated. port-based**:** If a client connected to the port is authenticated, other clients can access the LAN without authentication.
Step 8	**dot1x max-req** *times* Specify the maximum number of attempts to send the authentication packet for the client. *times:* The maximum attempts for the client to send the authentication packet. It ranges from 1 to 9 and the default is 3.
Step 9	**dot1x quiet-period** [time] (Optional) Enable the quiet feature for 802.1x authentication and configure the quiet period. time: Set a value between 1 and 999 seconds for the quiet period. It is 10 seconds by default. The quiet period starts after the authentication fails. During the quiet period, the switch does not process authentication requests from the same client.
Step 10	**dot1x timeout supp-timeout** *time* Configure the supplicant timeout period. *time:* Specify the maximum time for which the switch waits for response from the client. It ranges from 1 to 60 seconds and the default time is 30 seconds. If the switch does not receive any reply from the client within the specified time, it will resend the request.
Step 11	**show dot1x interface [fastEthernet** *port* **|gigabitEthernet** *port* **| ten-gigabitEthernet** *port***]** (Optional) Verify the configurations of 802.1x authentication on the port. *port:* Enter the ID of the port to be configured. If no specific port is entered, the switch will show configurations of all ports.

Step 12	**end** Return to privileged EXEC mode.
Step 13	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable 802.1x authentication on port 1/0/2, configure the control type as port-based, and keep other parameters as default:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#dot1x

Switch(config-if)#dot1x port-method port-based

Switch(config-if)#show dot1x interface gigabitEthernet 1/0/2

Port	State	MAB State	GuestVLAN	PortControl	PortMethod
Gi1/0/2	disabled	disabled	0	auto	port-based

MaxReq	QuietPeriod	SuppTimeout	Authorized	LAG
3	10	30	unauthorized	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Viewing Authenticator State

You can view the authenticator state. If needed, you can also initialize or reauthenticate the specific client:

Step 1	**show dot1x auth-state interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port***]** Displays the authenticator state.
Step 2	**configure** Enter global configuration mode.

Step 3	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode. *port:* Enter the ID of the port to be configured.
Step 4	**dot1x auth-init** [**mac** *mac-address*] Initialize the specific client. To access the network, the client needs to provide the correct information to pass the authentication again. *mac-address:* Enter the MAC address of the client that will be unauthorized.
Step 5	**dot1x auth-reauth** [**mac** *mac-address*] Reauthenticate the specific client. *mac-address:* Enter the MAC address of the client that will be reauthenticated.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

3 Configuration Example

3.1 Network Requirements

The network administrator wants to control access from the end users (clients) in the company. It is required that all clients need to be authenticated separately and only the authenticated clients can access the internet.

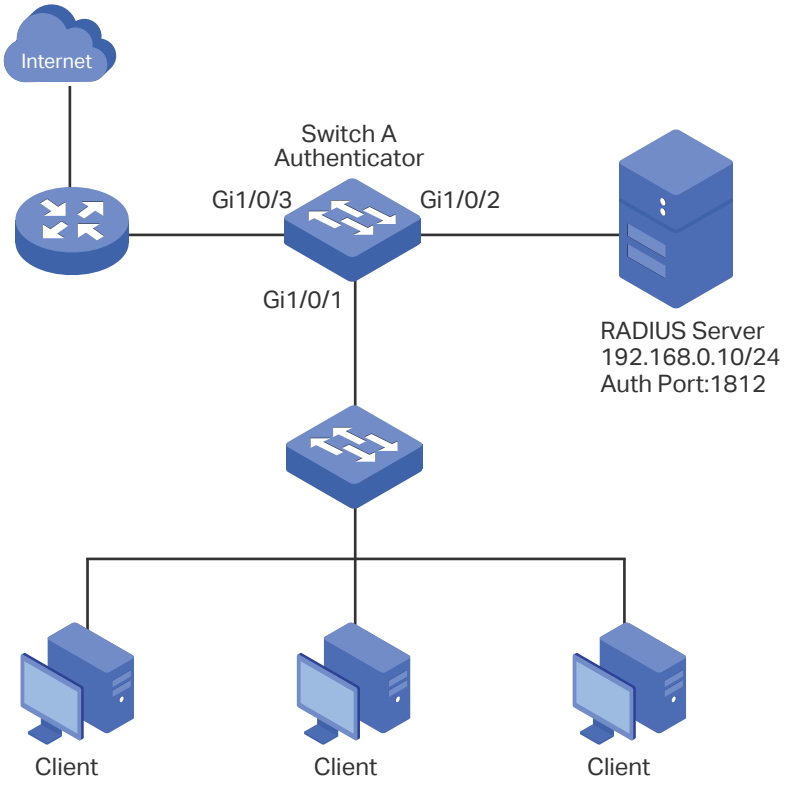
3.2 Configuration Scheme

- To authenticate clients separately, enable 802.1x authentication, configure the control mode as auto, and set the control type as MAC based.
- Enable 802.1x authentication on the ports connected to clients.
- Keep 802.1x authentication disabled on ports connected to the authentication server and the internet, which ensures unrestricted connections between the switch and the authentication server or the internet.

3.3 Network Topology

As shown in the following figure, Switch A acts as the authenticator. Port 1/0/1 is connected to the client, port 1/0/2 is connected to the RADIUS server, and port 1/0/3 is connected to the internet.

Figure 3-1 Network Topology

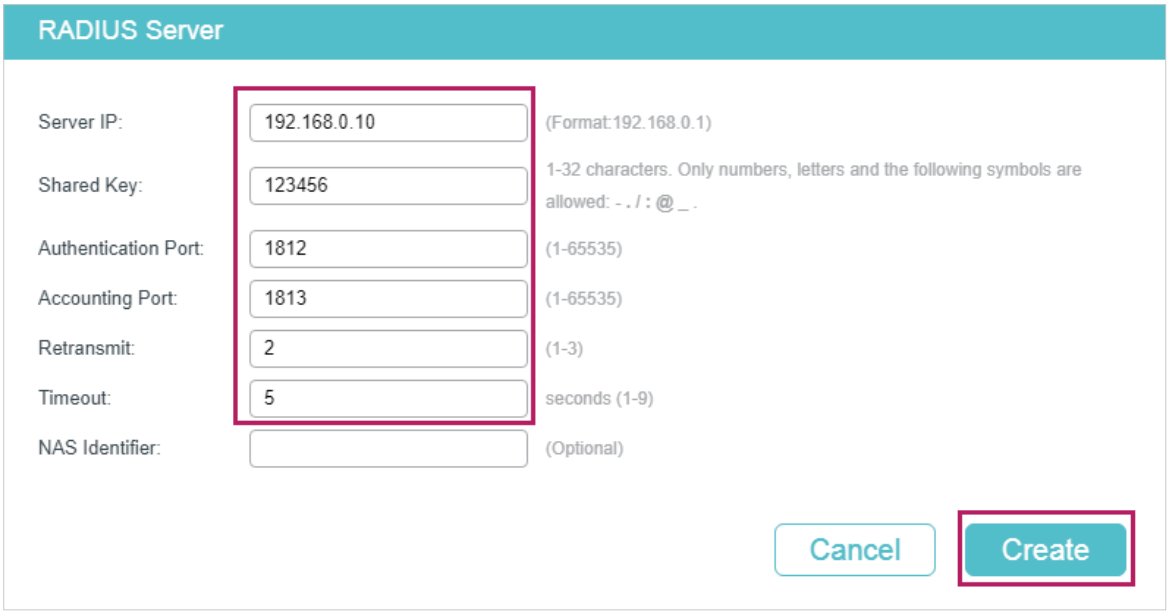


Demonstrated with T1600G-52TS acting as the authenticator, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

3.4 Using the GUI

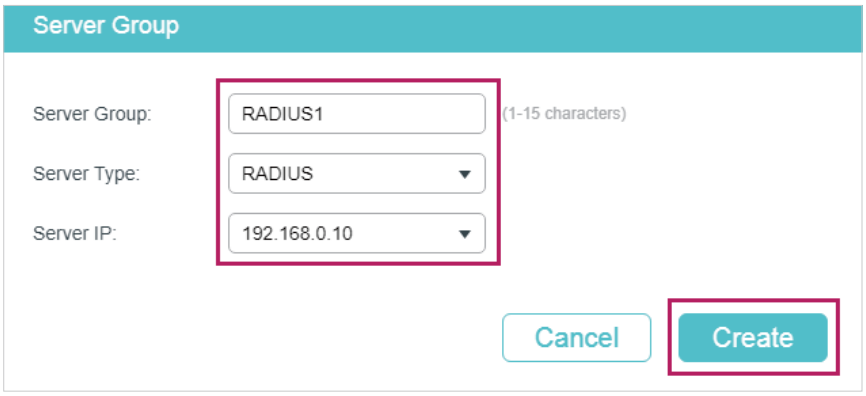
1) Choose the menu **SECURITY > AAA > RADIUS Config** and click Add to load the following page. Configure the parameters of the RADIUS server and click **Create**.

Figure 3-2 Adding RADIUS Server



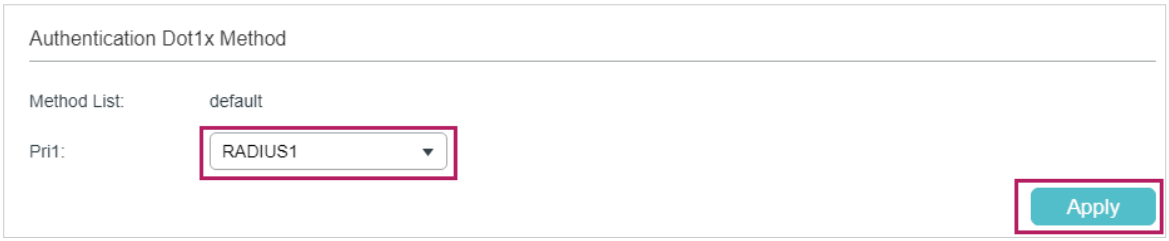
2) Choose the menu **SECURITY > AAA > Server Group** and click Add to load the following page. Specify the group name as RADIUS1, select the server type as RADIUS and server IP as 192.168.0.10. Click **Create**.

Figure 3-3 Creating Server Group



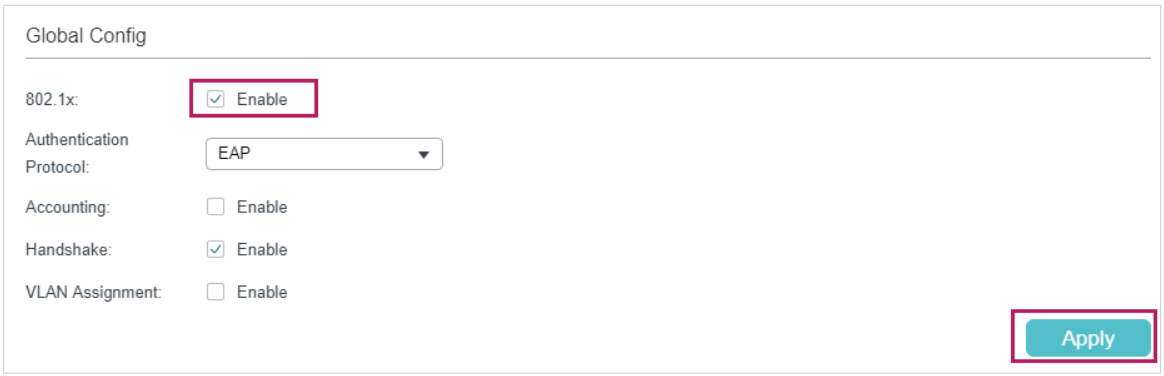
3) Choose the menu **SECURITY > AAA > Dot1x List** to load the following page. In the **Authentication Dot1x Method** section, select RADIUS1 as the RADIUS server group for authentication, and click **Apply**.

Figure 3-4 Configuring Authentication RADIUS Server



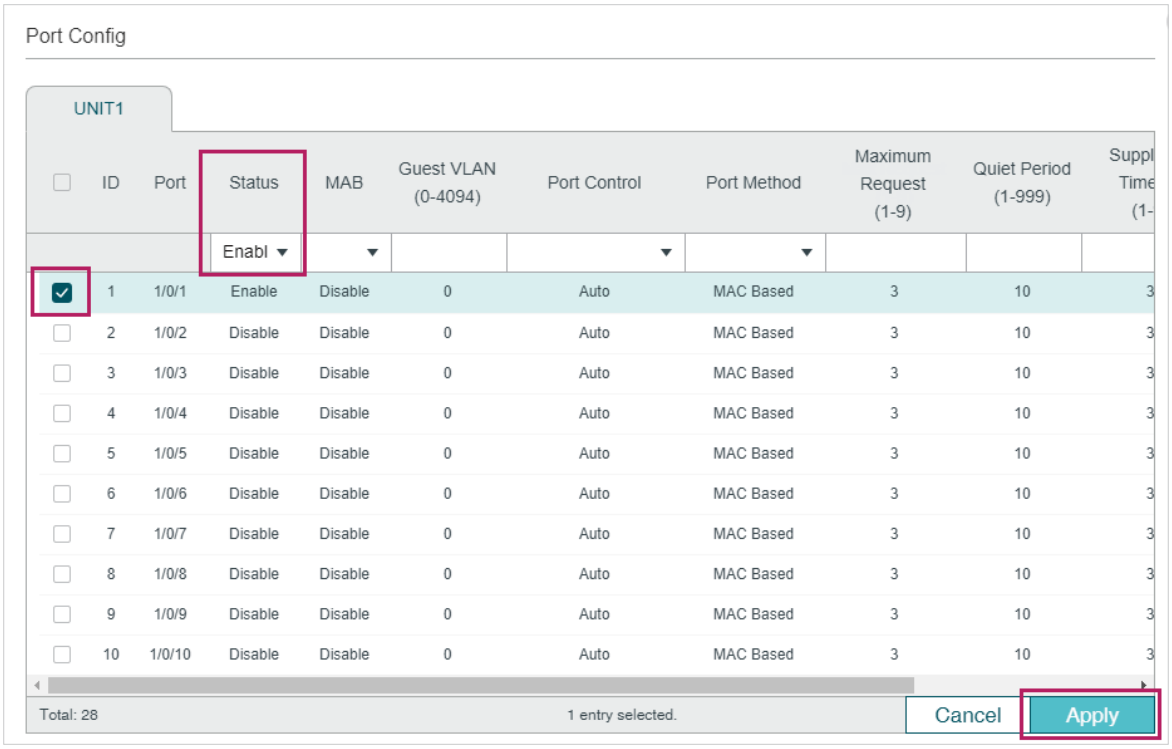
4) Choose the menu **SECURITY > 802.1x > Global Config** to load the following page. Enable 802.1x authentication and configure the Authentication Method as EAP. Keep the default authentication settings. Click **Apply**.

Figure 3-5 Configuring Global Settings



5) Choose the menu **SECURITY > 802.1x > Port Config** to load the following page. For port 1/0/1, enable 802.1x authentication, set the Control Mode as auto and set the Control Type as MAC Based; For port 1/0/2 and port 1/0/3, disable 802.1x authentication.

Figure 3-6 Configuring Port



6) Click Save to save the settings.

3.5 Using the CLI

1) Configure the RADIUS parameters.

Switch_A(config)#radius-server host 192.168.0.10 auth-port 1812 key 123456

Switch_A(config)#aaa group radius RADIUS1

Switch_A(aaa-group)#server 192.168.0.10

Switch_A(aaa-group)#exit

Switch_A(config)#aaa authentication dot1x default RADIUS1

2) Globally enable 802.1x authentication and set the authentication protocol.

Switch_A(config)#dot1x system-auth-control

Switch_A(config)#dot1x auth-protocol eap

3) Disable 802.1x authentication on port 1/0/2 and port 1/0/3. Enable 802.1x authentication on port 1/0/1, set the control mode as auto, and set the control type as MAC based.

Switch_A(config)#interface gigabitEthernet 1/0/2

Switch_A(config-if)#no dot1x

Switch_A(config-if)#exit

```
Switch_A(config)#interface gigabitEthernet 1/0/3
Switch_A(config-if)#no dot1x
Switch_A(config-if)#exit
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#dot1x
Switch_A(config-if)#dot1x port-method mac-based
Switch_A(config-if)#dot1x port-control auto
Switch_A(config-if)#exit
```

Verify the Configurations

Verify the global configurations of 802.1x authentication:

```
Switch_A#show dot1x global
 802.1X State:                Enabled
 Authentication Protocol:     EAP
 Handshake State:             Enabled
 802.1X Accounting State:     Disabled
 802.1X VLAN Assignment State:  Disabled
```

Verify the configurations of 802.1x authentication on the port:

```
Switch_A#show dot1x interface
Port       State      MAB State   GuestVLAN   PortControl    PortMethod
----       -----      ---------   ---------   -----------    ----------
Gi1/0/1    enabled    disabled    0           auto           mac-based
Gi1/0/2    disabled   disabled    0           auto           mac-based
Gi1/0/3    disabled   disabled    0           auto           mac-based
...
MaxReq   QuietPeriod   SuppTimeout   Authorized      LAG
------   -----------   -----------   ----------      ---
3        10            30            unauthorized    N/A
3        10            30            unauthorized    N/A
```

3 10 30 unauthorized N/A

...

Verify the configurations of RADIUS :

Switch_A#show aaa global

Module	Login List	Enable List
Telnet	default	default
Ssh	default	default
Http	default	default

Switch_A#show aaa authentication dot1x

Methodlist	pri1	pri2	pri3	pri4
default	RADIUS1	--	--	--

Switch_A#show aaa group RADIUS1

192.168.0.10

4 Appendix: Default Parameters

Default settings of 802.1x are listed in the following table.

Table 4-1 Default Settings of 802.1x

Parameter	Default Setting
Global Config	
802.1x Authentication	Disabled
Authentication Method	EAP
Handshake	Enabled
Accounting	Disabled
VLAN Assignment	Disabled
Port Config	
802.1x Status	Disabled
MAB	Disabled
Guest VLAN	Disabled
Port Control	Auto
Guest VLAN	0
Maximum Request	3
Quiet Period	10 seconds
Supplicant Timeout	30 seconds
Port Method	MAC Based
Dot1X List	
Authentication Dot1x Method List	List Name: default Pri1: radius
Accounting Dot1x Method List	List Name: default Pri1: radius

Part 26

Configuring Port Security

CHAPTERS

1. Overview
2. Port Security Configuration
3. Appendix: Default Parameters

1 Overview

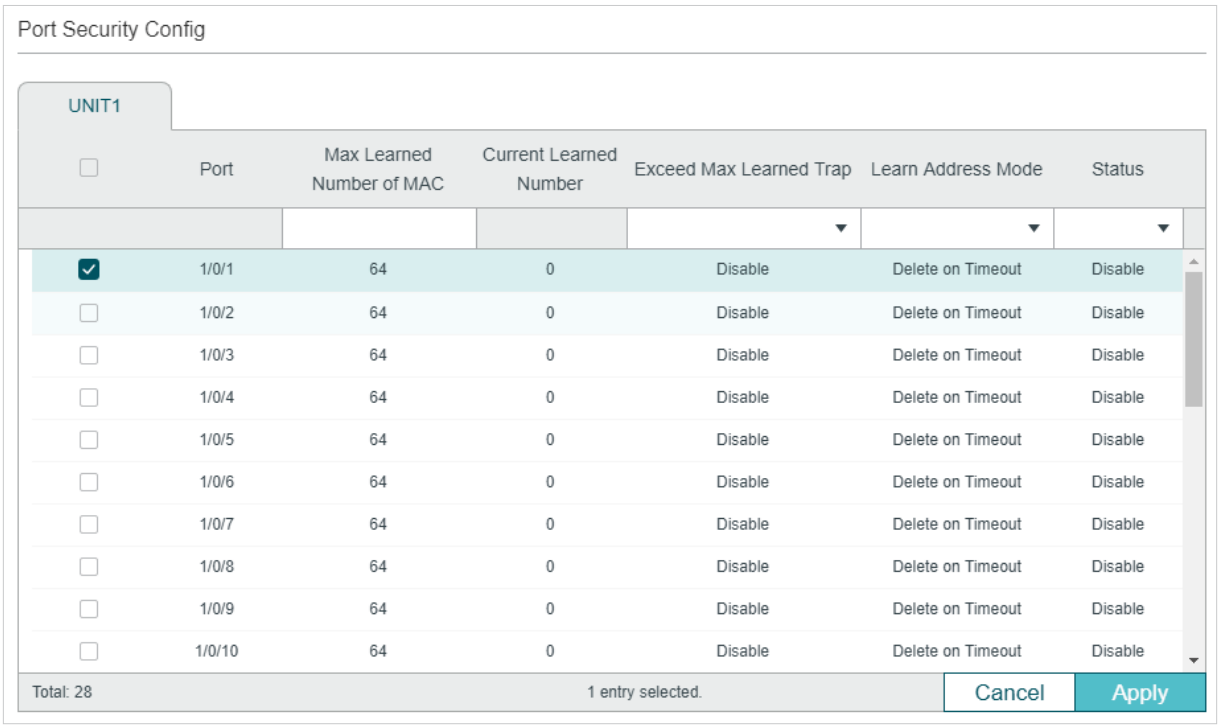
You can use the Port Security feature to limit the number of MAC addresses that can be learned on each port, thus preventing the MAC address table from being exhausted by the attack packets. In addtion, the switch can send a notification if the number of learned MAC addresses on the port exceeds the limit.

2 Port Security Configuration

2.1 Using the GUI

Choose the menu **SECURITY > Port Security** to load the following page.

Figure 2-1 Port Security



Follow these steps to configure Port Security:

1) Select one or more ports and configure the following parameters.

Port	Displays the port number.
Max Learned Number of MAC	Specify the maximum number of MAC addresses that can be learned on the port. When the learned MAC address number reaches the limit, the port will stop learning. It ranges from 0 to 64. The default value is 64.
Current Learned MAC	Displays the current number of MAC addresses that have been learned on the port.
Exceed Max Learned Trap	Enable Exceed Max Learned, and when the maximum number of learned MAC addresses on the specified port is exceeded, a notification will be generated and sent to the management host.

Learn Address Mode	Select the learn mode of the MAC addresses on the port. Three modes are provided: **Delete on Timeout**: The switch will delete the MAC addresses that are not used or updated within the aging time. It is the default setting. **Delete on Reboot**: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted. **Permanent**: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted.
Status	Select the status of Port Security. Three kinds of status can be selected: **Drop**: When the number of learned MAC addresses reaches the limit, the port will stop learning and discard the packets with the MAC addresses that have not been learned. **Forward**: When the number of learned MAC addresses reaches the limit, the port will stop learning but send the packets with the MAC addresses that have not been learned. **Disable**: The number limit on the port is not effective, and the switch follows the original forwarding rules. It is the default setting.

2) Click **Apply**.

Note:

- Port Security cannot be enabled on the member ports of a LAG, and the port with Port Security enabled cannot be added to a LAG.
- On one port, Port Security and 802.1x cannot be enabled at the same time.

2.2 Using the CLI

Follow these steps to configure Port Security:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.

Step 3	**mac address-table max-mac-count { [max-number** *num*] **[exceed-max-learned** enable | disable**] [mode** { dynamic | static | permanent } **] [status** { forward | drop | disable } **]}** Enable the port security feature of the port and configure the related parameters. *num*: The maximum number of MAC addresses that can be learned on the port. The valid values are from 0 to 64. The default value is 64. **exceed-max-learned:** With exceed-max-learned enabled, when the maximum number of MAC addresses on the specified port is exceeded, a notification will be generated and sent to the management host. enable: Enable exceed-max-learned. disable: Disable exceed-max-learned. **mode**: Learn mode of the MAC address. There are three modes: dynamic: The switch will delete the MAC addresses that are not used or updated within the aging time. static: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted. permanent: The learned MAC address is out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted. **status**: Status of port security feature. By default, it is disabled. drop: When the number of learned MAC addresses reaches the limit, the port will stop learning and discard the packets with the MAC addresses that have not been learned. forward: When the number of learned MAC addresses reaches the limit, the port will stop learning but send the packets with the MAC addresses that have not been learned. disable: The number limit on the port is not effective, and the switch follows the original forwarding rules. It is the default setting.
Step 4	**show mac address-table max-mac-count interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Verify the Port Security configuration and the current learned MAC addresses of the port.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

Note:

- Port Security cannot be enabled on the member port of a LAG, and the port with Port Security enabled cannot be added to a LAG.
- On one port, Port Security and 802.1x cannot be enabled at the same time.

The following example shows how to set the maximum number of MAC addresses that can be learned on port 1/0/1 as 30, enable exceed-max-leaned feature and configure the mode as permanent and the status as drop:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#mac address-table max-mac-count max-number 30 **exceed-max-learned** enable **mode** permanent **status** drop

Switch(config-if)#show mac address-table max-mac-count interface gigabitEthernet 1/0/1

Port	Max-learn	Current-learn	Exceed Max Limit	Mode	Status
----	---------	-----------	----------	------	--------
Gi1/0/1	30	0	disable	permanent	drop

Switch(config-if)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

Default settings of Port Security are listed in the following table.

Table 3-1 Default Parameters of Port Security

Parameter	Default Setting
Max Learned Number of MAC	64
Current Learned Number	0
Exceed Max Learned Trap	Disabled
Learn Address Mode	Delete on Timeout
Status	Disabled

Part 27

Configuring ACL

CHAPTERS

1. Overview
2. ACL Configuration
3. Configuration Example for ACL
4. Appendix: Default Parameters

1 Overview

ACL (Access Control List) filters traffic as it passes through a switch, and permits or denies packets crossing specified interfaces or VLANs. It accurately identifies and processes the packets based on the ACL rules. In this way, ACL helps to limit network traffic, manage network access behaviors, forward packets to specified ports and more.

To configure ACL, follow these steps:

1) Configure a time range during which the ACL is in effect.
2) Create an ACL and configure the rules to filter different packets.
3) Bind the ACL to a port or VLAN to make it effective.

Configuration Guidelines

- A packet "matches" an ACL rule when it meets the rule's matching criteria. The resulting action will be either to "permit" or "deny" the packet that matches the rule.

- If no ACL rule is configured, the packets will be forwarded without being processed by the ACL. If there is configured ACL rules and no matching rule is found, the packets will be dropped.

2 ACL Configuration

2.1 Using the GUI

2.1.1 Configuring Time Range

Some ACL-based services or features may need to be limited to take effect only during a specified time period. In this case, you can configure a time range for the ACL. For details about Time Range configuration, please refer to Managing System

2.1.2 Creating an ACL

You can create different types of ACL and define the rules based on source MAC or IP address, destination MAC or IP address, protocol type, port number and so on.

MAC ACL: MAC ACL uses source and destination MAC address for matching operations.

IP ACL: IP ACL uses source and destination IP address, IP protocols and so on for matching operations.

Combined ACL: Combined ACL uses source and destination MAC address, and source and destination IP address for matching operations.

IPv6 ACL: IPv6 ACL uses source and destination IPv6 address for matching operations.

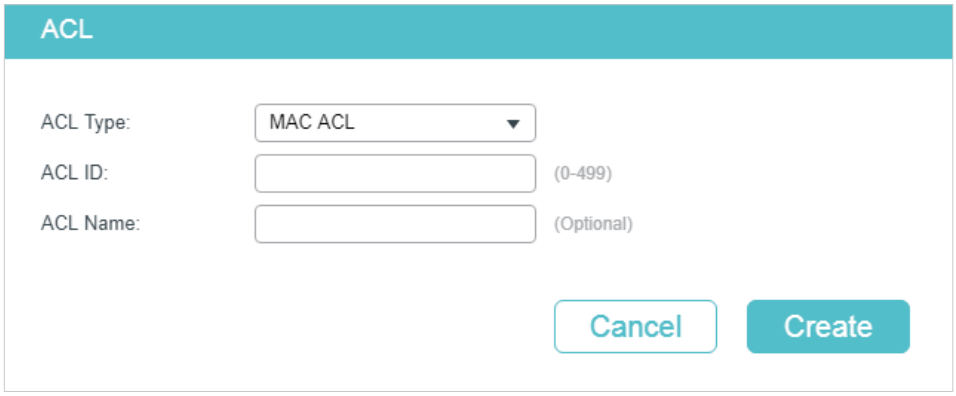
Packet Content ACL: Packet Content ACL analyzes and processes data packets based on 4 chunk match conditions, each chunk can specify a user-defined 4-byte segment carried in the packet's first 128 bytes.

Note:

Packet Content ACL is only available on certain devices.

Choose the menu **SECURITY > ACL > ACL Config** and click Add to load the following page.

Figure 2-1 Creating an ACL



Follow these steps to create an ACL:

1) Choose one ACL type and enter a number to identify the ACL.
2) (Optional) Assign a name to the ACL.
3) Click **Create**.

Note:

The supported ACL type and ID range varies on different switch models. Please refer to the on-screen information.

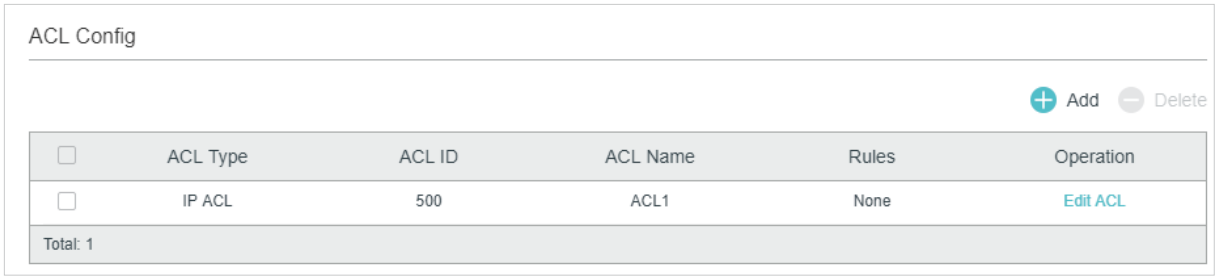
2.1.3 Configuring ACL Rules

Note:

Every ACL has an implicit deny all rule at the end of an ACL rule list. That is, if an ACL is applied to a packet and none of the explicit rules match, then the final implicit deny all rule takes effect and the packet is dropped.

The created ACL will be displayed on the **SECURITY > ACL > ACL Config** page.

Figure 2-2 Editing ACL



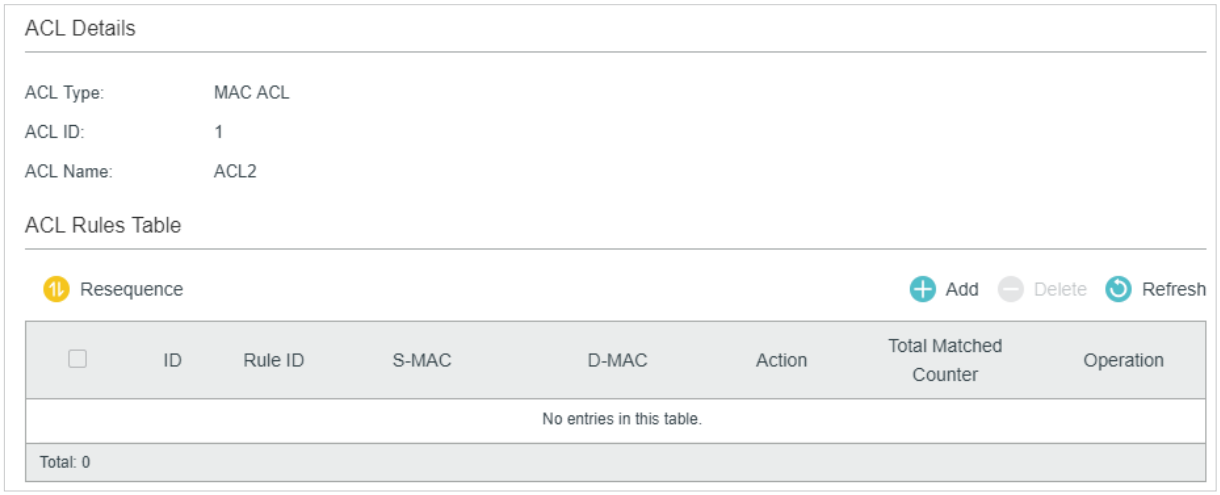
Click **Edit ACL** in the **Operation** column. Then you can configure rules for this ACL.

The following sections introduce how to configure MAC ACL, IP ACL, Combined ACL and IPv6 ACL.

Configuring MAC ACL Rule

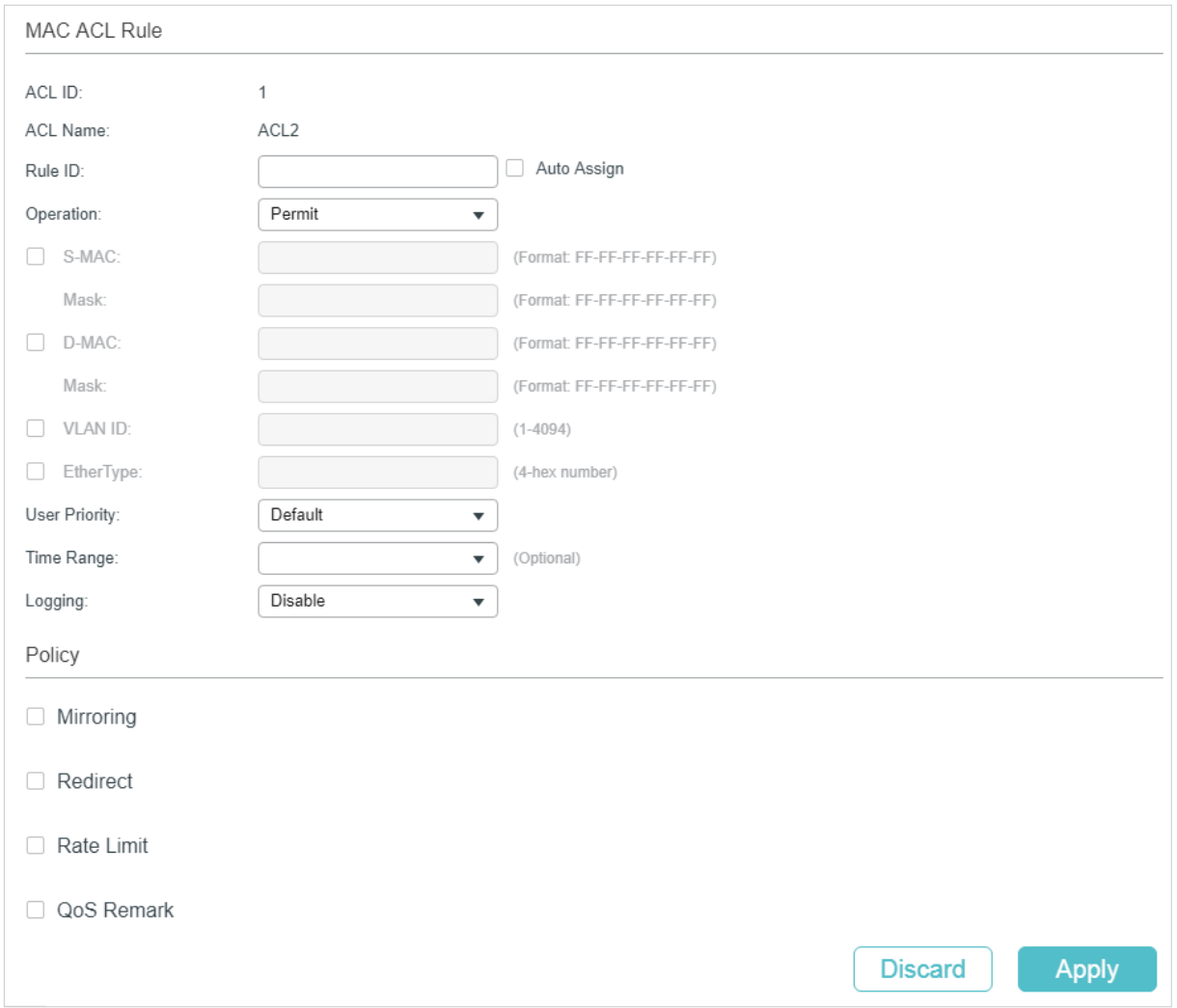
Click **Edit ACL** for a MAC ACL entry to load the following page.

Figure 2-3 Configuring the MAC ACL Rule



In **ACL Rules Table** section, click Add and the following page will appear.

Figure 2-4 Configuring the MAC ACL Rule



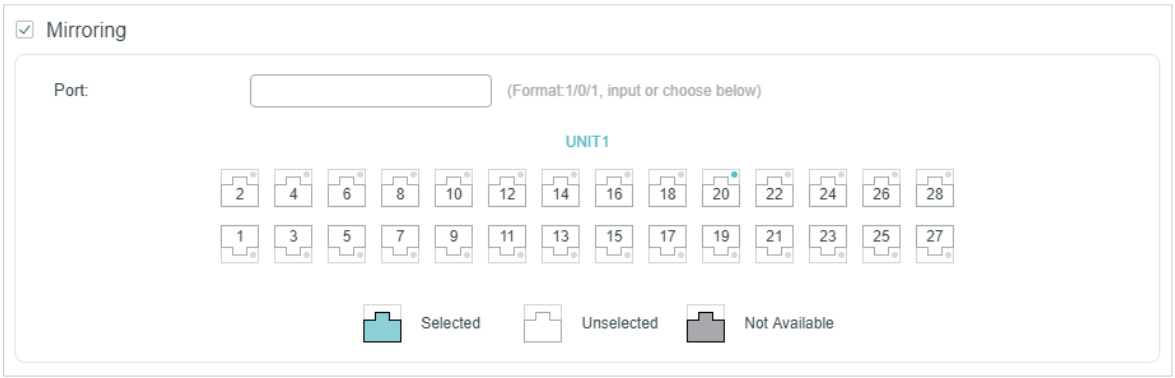
Follow these steps to configure the MAC ACL rule:

1) In the **MAC ACL Rule** section, configure the following parameters:

Rule ID	Enter an ID number to identify the rule. It should not be the same as any current rule ID in the same ACL. For the convenience of inserting new rules to an ACL, you should set the appropriate interval between rule IDs. If you select **Auto Assign**, the rule ID will be assigned automatically by the system and the default increment between neighboring rule IDs is 5.
Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.
S-MAC/Mask	Enter the source MAC address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-MAC/Mask	Enter the destination MAC address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
VLAN ID	Enter the ID number of the VLAN with which packets will match. The valid range is 1-4094. If the ACL is bound to a VLAN, the system requires the VLAN ID of a packet to match the ID of the VLAN instead of the ID listed here.
EtherType	Specify the EtherType to be matched using 4 hexadecimal numbers.
User Priority	Specify the User Priority to be matched.
Time Range	Select a time range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect. The Time Range referenced here can be created on the **SYSTEM > Time Range** page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

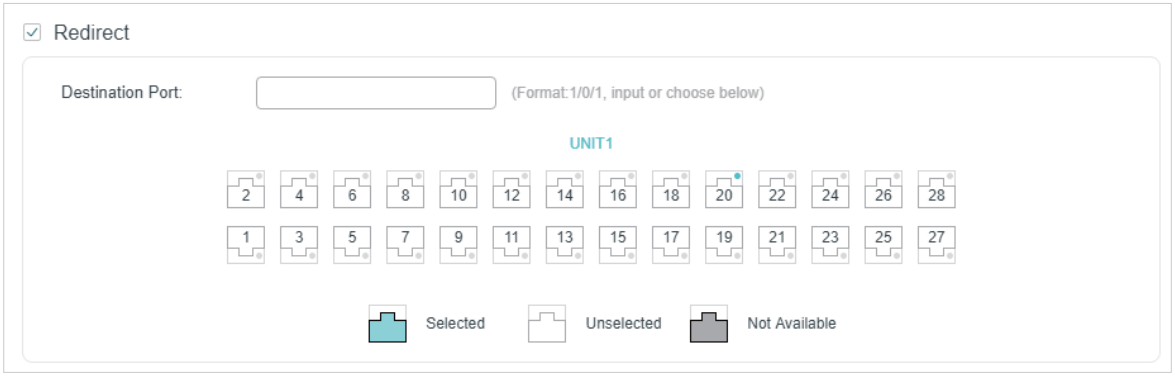
2) In the **Policy** section, enable or disable the Mirroring feature for the matched packets. With this option enabled, choose a destination port to which the packets will be mirrored.

Figure 2-5 Configuring Mirroring



3) In the **Policy** section, enable or disable the Redirect feature for the matched packets. With this option enabled, choose a destination port to which the packets will be redirected.

Figure 2-6 Configuring Redirect

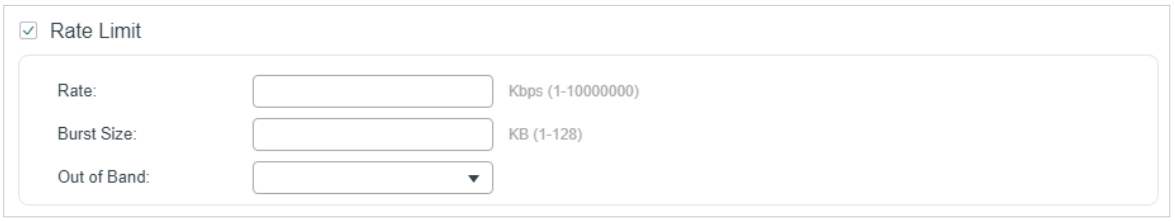


Note:

In the Mirroring feature, the matched packets will be copied to the destination port and the original forwarding will not be affected. While in the Redirect feature, the matched packets will be forwarded only on the destination port.

4) In the **Policy** section, enable or disable the Rate Limit feature for the matched packets. With this option enabled, configure the related parameters.

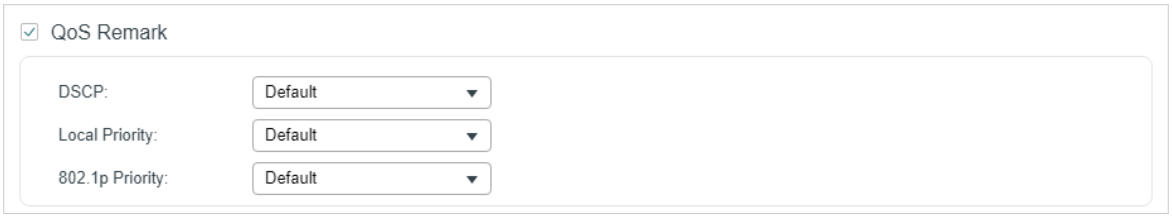
Figure 2-7 Configuring Rate Limit



Rate	Specify the transmission rate for the matched packets.
Burst Size	Specify the maximum number of bytes allowed in one second.
Out of Band	Select the action for the packets whose rate is beyond the specified rate. **None:** The packets will be forwarded normally. **Drop:** The packets will be discarded. **Remark DSCP:** You can specify a DSCP value, and the DSCP field of the packets will be changed to the specified one. Note: Remark DSCP is only available on certain devices.

5) In the **Policy** section, enable or disable the QoS Remark feature for the matched packets. With this option enabled, configure the related parameters, and the remarked values will take effect in the QoS processing on the switch.

Figure 2-8 Configuring QoS Remark



DSCP	Specify the DSCP field for the matched packets. The DSCP field of the packets will be changed to the specified one.
Local Priority	Specify the local priority for the matched packets. The local priority of the packets will be changed to the specified one.
802.1p Priority	Specify the 802.1p priority for the matched packets. The 802.1p priority of the packets will be changed to the specified one.

6) Click **Apply**.

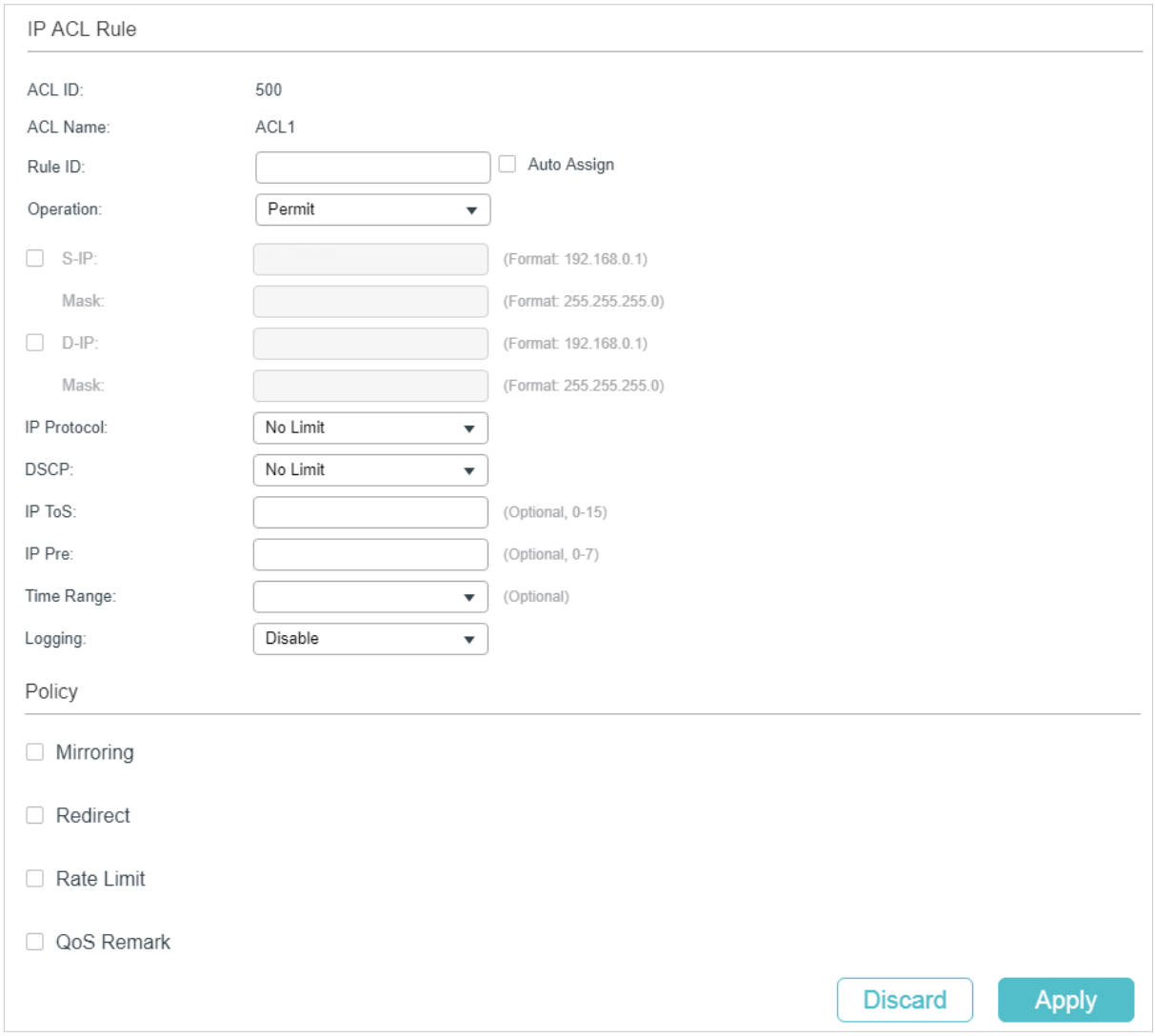
Configuring IP ACL Rule

Click **Edit ACL** for an IP ACL entry to load the following page.

Figure 2-9 Configuring the IP ACL Rule

In **ACL Rules Table** section, click Add and the following page will appear.

Figure 2-10 Configuring the IP ACL Rule



Follow these steps to configure the IP ACL rule:

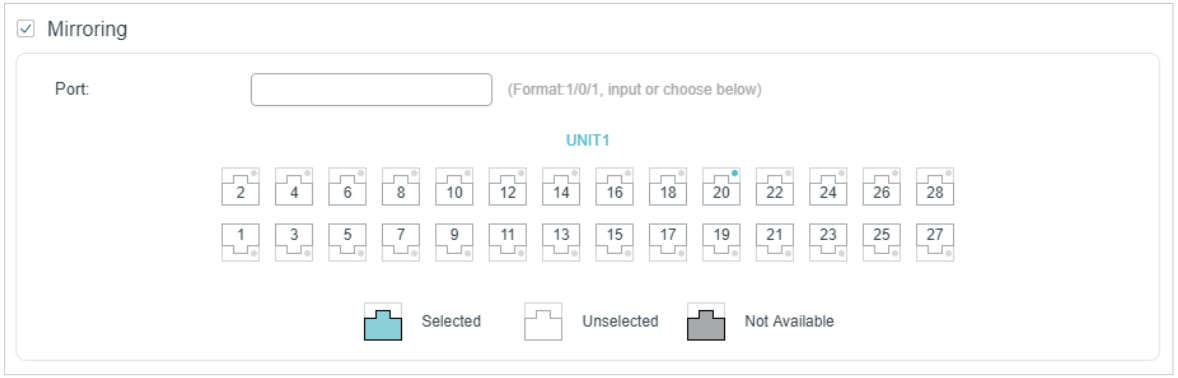
1) In the **IP ACL Rule** section, configure the following parameters:

Rule ID	Enter an ID number to identify the rule. It should not be the same as any current rule ID in the same ACL. For the convenience of inserting new rules to an ACL, you should set the appropriate interval between rule IDs. If you select **Auto Assign**, the rule ID will be assigned automatically by the system and the default increment between neighboring rule IDs is 5
Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.

Fragment	With this option selected, the rule will be applied to all fragment packets except for the last fragment packet in the fragment packet group. Note: Fragment is only availavle on certain devices.
S-IP/Mask	Enter the source IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-IP/Mask	Enter the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
IP Protocol	Select a protocol type from the drop-down list. The default is No Limit, which indicates that packets of all protocols will be matched. You can also select User-defined to customize the IP protocol.
TCP Flag	If TCP protocol is selected, you can configure the TCP Flag to be used for the rule's matching operations. There are six flags and each has three options, which are *, 0 and 1. The default is *, which indicates that the flag is not used for matching operations. **URG**: Urgent flag. **ACK**: Acknowledge flag. **PSH**: Push flag. **RST**: Reset flag. **SYN**: Synchronize flag. **FIN**: Finish flag.
S-Port / D-Port	If TCP/UDP is selected as the IP protocol, specify the source and destination port number with a mask. **Value**: Specify the port number. **Mask**: Specify the port mask with 4 hexadacimal numbers.
DSCP	Specify a DSCP value to be matched between 0 and 63. The default is No Limit.
IP ToS	Specify an IP ToS value to be matched between 0 and 15. The default is No Limit.
IP Pre	Specify an IP Precedence value to be matched to be matched between 0 and 7. The default is No Limit.
Time Range	Select a time range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect. The Time Range referenced here can be created on the **SYSTEM > Time Range** page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

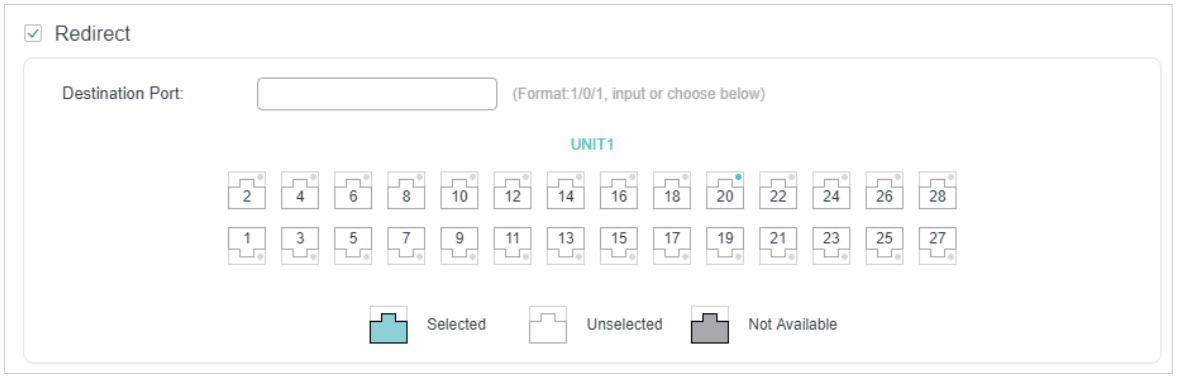
2) In the **Policy** section, enable or disable the Mirroring feature for the matched packets. With this option enabled, choose a destination port to which the packets will be mirrored.

Figure 2-11 Configuring Mirroring



3) In the **Policy** section, enable or disable the Redirect feature for the matched packets. With this option enabled, choose a destination port to which the packets will be redirected.

Figure 2-12 Configuring Redirect

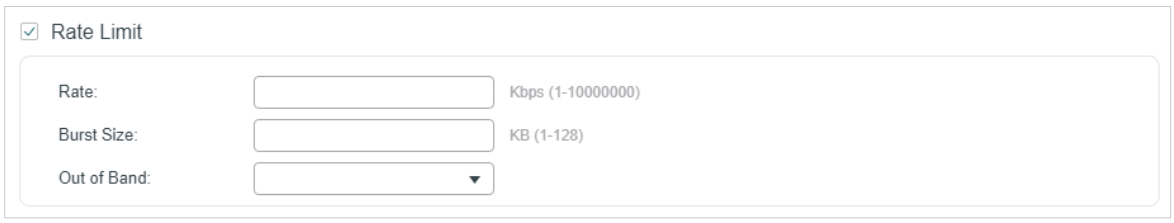


Note:

In the Mirroring feature, the matched packets will be copied to the destination port and the original forwarding will not be affected. While in the Redirect feature, the matched packets will be forwarded only on the destination port.

4) In the **Policy** section, enable or disable the Rate Limit feature for the matched packets. With this option enabled, configure the related parameters.

Figure 2-13 Configuring Rate Limit



Rate	Specify the transmission rate for the matched packets.

Burst Size	Specify the maximum number of bytes allowed in one second.
Out of Band	Select the action for the packets whose rate is beyond the specified rate. **None:** The packets will be forwarded normally. **Drop:** The packets will be discarded. **Remark DSCP:** You can specify a DSCP value, and the DSCP field of the packets will be changed to the specified one. Note: Remark DSCP is only available on certain devices.

5) In the **Policy** section, enable or disable the QoS Remark feature for the matched packets. With this option enabled, configure the related parameters, and the remarked values will take effect in the QoS processing on the switch.

Figure 2-14 Configuring QoS Remark

DSCP	Specify the DSCP field for the matched packets. The DSCP field of the packets will be changed to the specified one.
Local Priority	Specify the local priority for the matched packets. The local priority of the packets will be changed to the specified one.
802.1p Priority	Specify the 802.1p priority for the matched packets. The 802.1p priority of the packets will be changed to the specified one.

6) Click **Apply**.

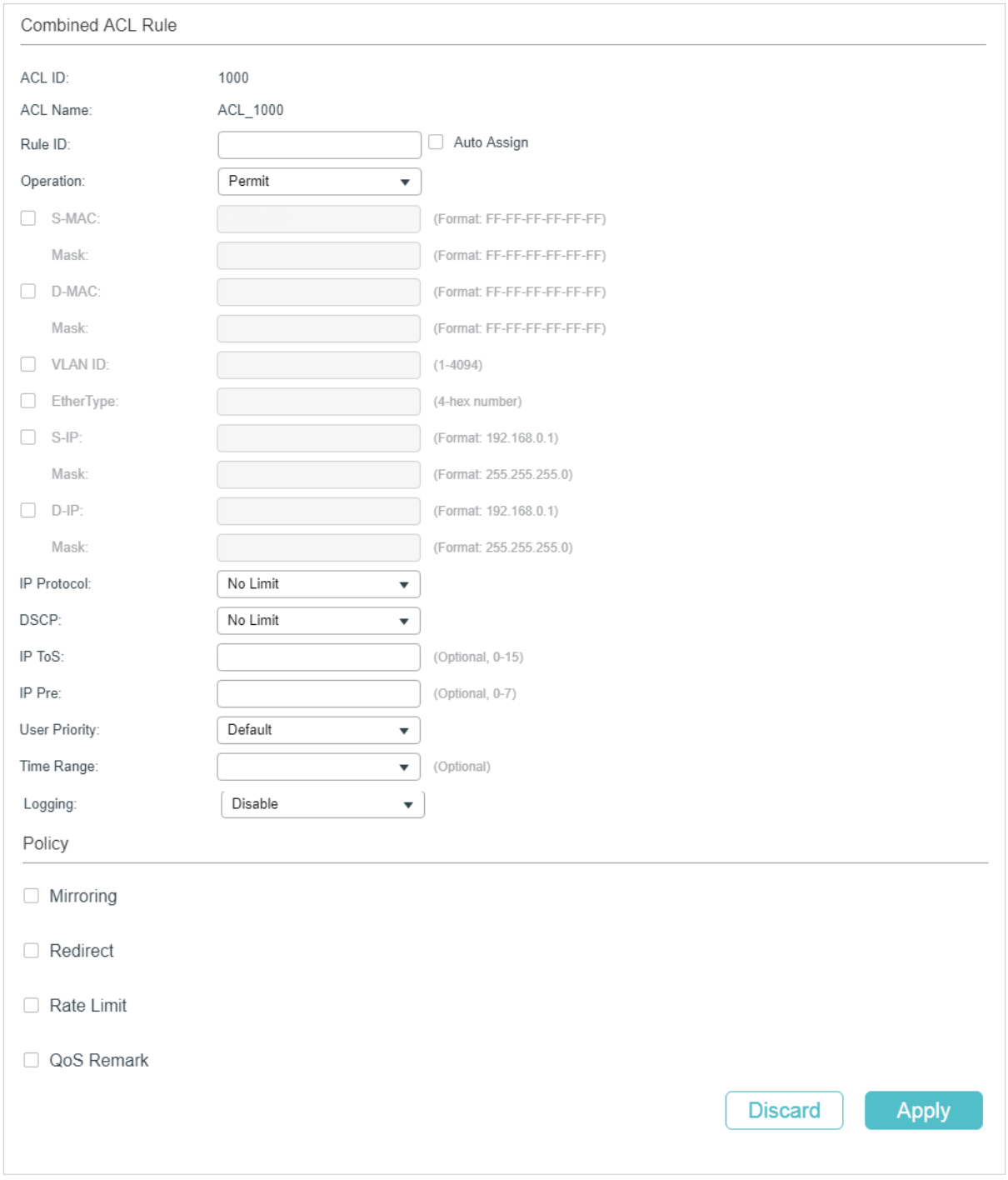
Configuring Combined ACL Rule

Click **Edit ACL** for a Combined ACL entry to load the following page.

Figure 2-15 Configuring the Combined ACL Rule

In **ACL Rules Table** section, click Add and the following page will appear.

Figure 2-16 Configuring the Combined ACL Rule



Follow these steps to configure the Combined ACL rule:

1) In the **Combined ACL Rule** section, configure the following parameters:

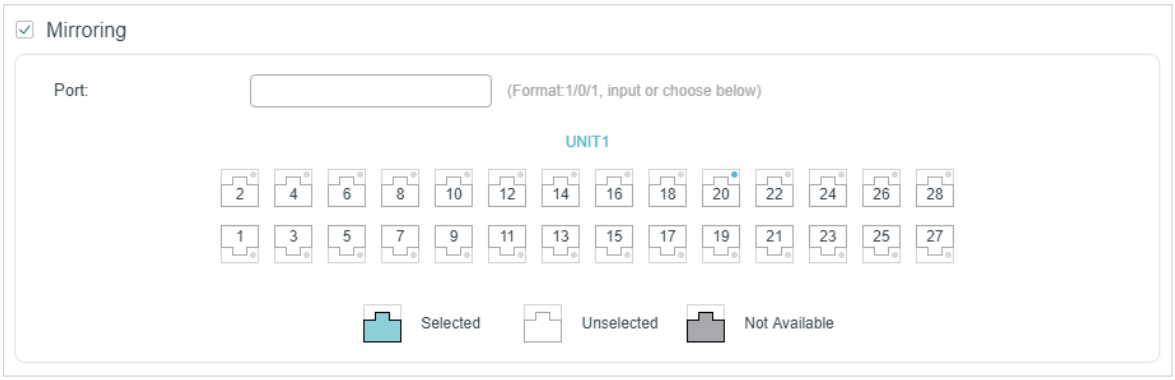
Rule ID	Enter an ID number to identify the rule. It should not be the same as any current rule ID in the same ACL. For the convenience of inserting new rules to an ACL, you should set the appropriate interval between rule IDs. If you select **Auto Assign**, the rule ID will be assigned automatically by the system and the default increment between neighboring rule IDs is 5

Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.
S-MAC/Mask	Enter the source MAC address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-MAC/Mask	Enter the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
VLAN ID	Enter the ID number of the VLAN with which packets will match. The valid range is 1-4094. If the ACL is bound to a VLAN, the system requires the VLAN ID of a packet to match the ID of the VLAN instead of the ID listed here.
EtherType	Specify the EtherType to be matched using 4 hexadecimal numbers.
S-IP/Mask	Enter the source IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-IP/Mask	Enter the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
IP Protocol	Select a protocol type from the drop-down list. The default is No Limit, which indicates that packets of all protocols will be matched. You can also select User-defined to customize the IP protocol.
TCP Flag	If TCP protocol is selected, you can configure the TCP Flag to be used for the rule's matching operations. There are six flags and each has three options, which are *, 0 and 1. The default is *, which indicates that the flag is not used for matching operations. **URG**: Urgent flag. **ACK**: Acknowledge flag. **PSH**: Push flag. **RST**: Reset flag. **SYN**: Synchronize flag. **FIN**: Finish flag.
S-Port / D-Port	If TCP/UDP is selected as the IP protocol, specify the source and destination port number with a mask. **Value**: Specify the port number. **Mask**: Specify the port mask with 4 hexadacimal numbers.
DSCP	Specify a DSCP value to be matched between 0 and 63. The default is No Limit.
IP ToS	Specify an IP ToS value to be matched between 0 and 15. The default is No Limit.

IP Pre	Specify an IP Precedence value to be matched to be matched between 0 and 7. The default is No Limit.
User Priority	Specify the User Priority to be matched.
Time Range	Select a time range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect. The Time Range referenced here can be created on the **SYSTEM > Time Range** page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

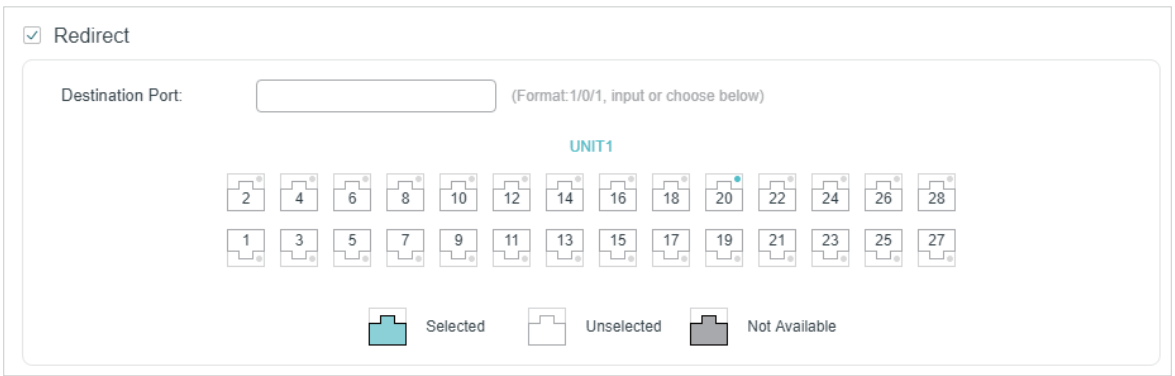
2) In the **Policy** section, enable or disable the Mirroring feature for the matched packets. With this option enabled, choose a destination port to which the packets will be mirrored.

Figure 2-17 Configuring Mirroring



3) In the **Policy** section, enable or disable the Redirect feature for the matched packets. With this option enabled, choose a destination port to which the packets will be redirected.

Figure 2-18 Configuring Redirect

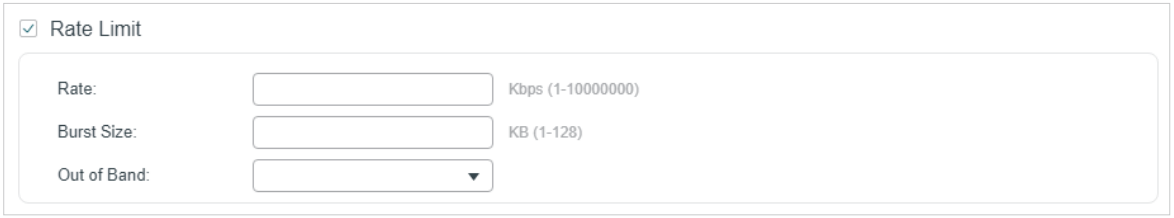


Note:

In the Mirroring feature, the matched packets will be copied to the destination port and the original forwarding will not be affected. While in the Redirect feature, the matched packets will be forwarded only on the destination port.

4) In the **Policy** section, enable or disable the Rate Limit feature for the matched packets. With this option enabled, configure the related parameters.

Figure 2-19 Configuring Rate Limit



Rate	Specify the transmission rate for the matched packets.
Burst Size	Specify the maximum number of bytes allowed in one second.
Out of Band	Select the action for the packets whose rate is beyond the specified rate. **None:** The packets will be forwarded normally. **Drop:** The packets will be discarded. **Remark DSCP:** You can specify a DSCP value, and the DSCP field of the packets will be changed to the specified one. Note: Remark DSCP is only available on certain devices.

5) In the **Policy** section, enable or disable the QoS Remark feature for the matched packets. With this option enabled, configure the related parameters, and the remarked values will take effect in the QoS processing on the switch.

Figure 2-20 Configuring QoS Remark

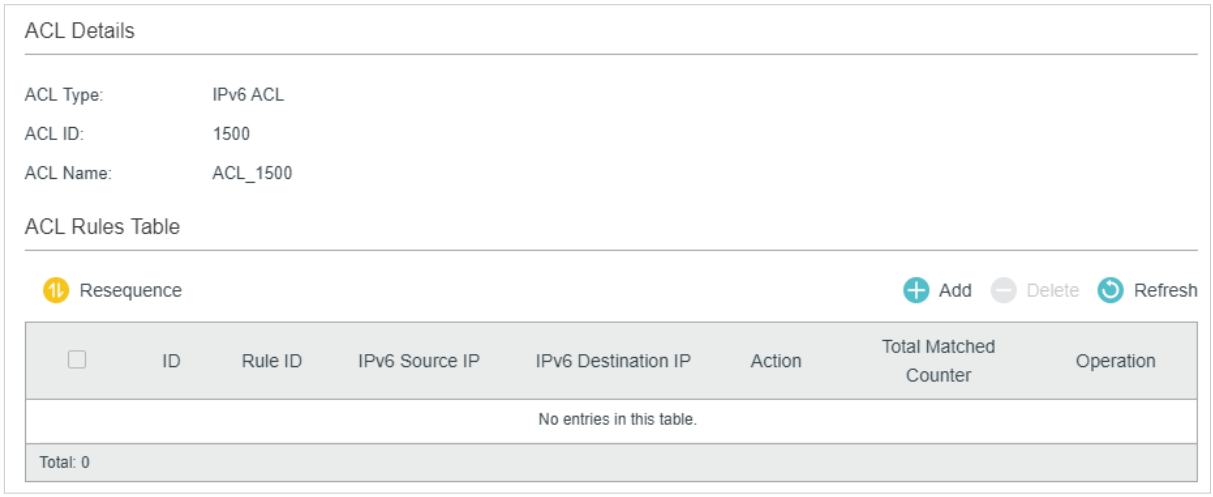
DSCP	Specify the DSCP field for the matched packets. The DSCP field of the packets will be changed to the specified one.
Local Priority	Specify the local priority for the matched packets. The local priority of the packets will be changed to the specified one.
802.1p Priority	Specify the 802.1p priority for the matched packets. The 802.1p priority of the packets will be changed to the specified one.

6) Click **Apply**.

Configuring the IPv6 ACL Rule

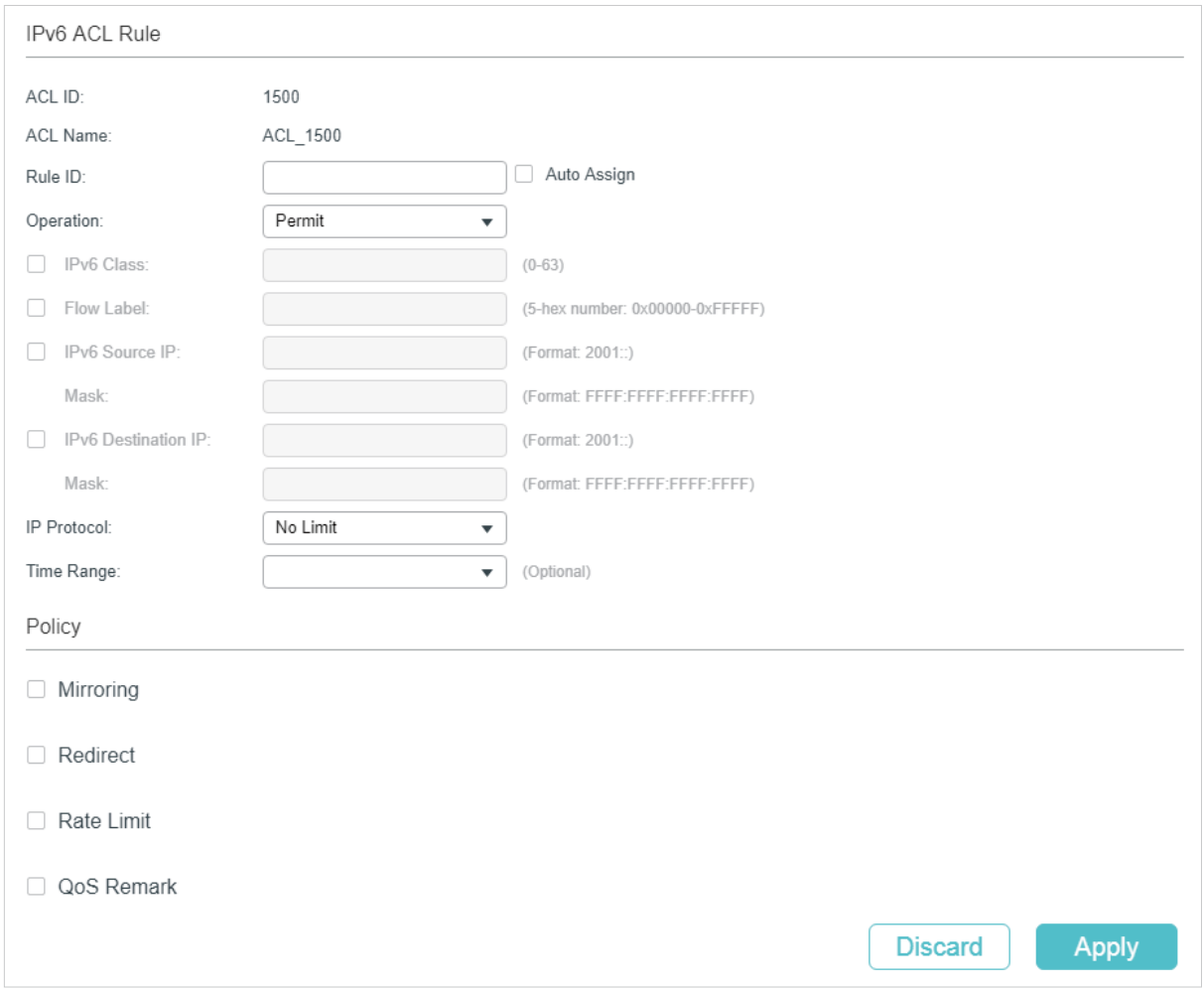
Click **Edit ACL** for an IPv6 ACL entry to load the following page.

Figure 2-21 Configuring the IPv6 ACL Rule



In **ACL Rules Table** section, click Add and the following page will appear.

Figure 2-22 Configuring the IPv6 ACL Rule



Follow these steps to configure the IPv6 ACL rule:

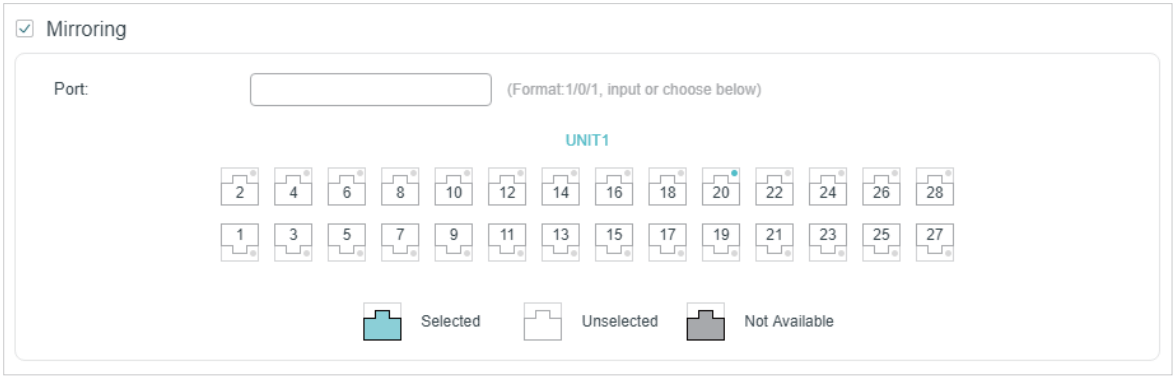
1) In the **IPv6 ACL Rule** section, configure the following parameters:

Rule ID	Enter an ID number to identify the rule. It should not be the same as any current rule ID in the same ACL. For the convenience of inserting new rules to an ACL, you should set the appropriate interval between rule IDs. If you select **Auto Assign**, the rule ID will be assigned automatically by the system and the default increment between neighboring rule IDs is 5
Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.
IPv6 Class	Specify an IPv6 class value to be matched. The switch will check the class field of the IPv6 header.
Flow Label	Specify a Flow Label value to be matched.
IPv6 Source IP	Enter the source IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid.
Mask	The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, FFFF:FFFF:0000:FFFF). The IP address mask specifies which bits in the source IPv6 address to match the rule. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
IPv6 Destination IP	Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid.
Mask	The mask is required if the destination IPv6 address is entered. Enter the complete mask (for example, FFFF:FFFF:0000:FFFF). The IP address mask specifies which bits in the source IP address to match the rule. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
IP Protocol	Select a protocol type from the drop-down list. **No Limit:** Packets of all protocols will be matched. **UDP:** Specify the source port and destination port for the UDP packet to be matched. **TCP**: Specify the source port and destination port for the TCP packet to be matched. **User-defined**: You can customize an IP protocol.
S-Port / D-Port	If TCP/UDP is selected as the IP protocol, specify the source and destination port numbers.

Time Range	Select a time range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect. The Time Range referenced here can be created on the **SYSTEM > Time Range** page.

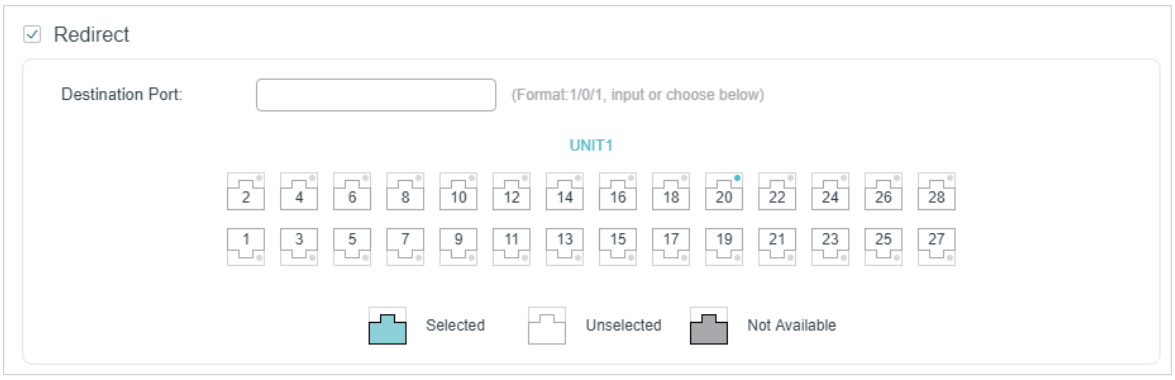
2) In the **Policy** section, enable or disable the Mirroring feature for the matched packets. With this option enabled, choose a destination port to which the packets will be mirrored.

Figure 2-23 Configuring Mirroring



3) In the **Policy** section, enable or disable the Redirect feature for the matched packets. With this option enabled, choose a destination port to which the packets will be redirected.

Figure 2-24 Configuring Redirect

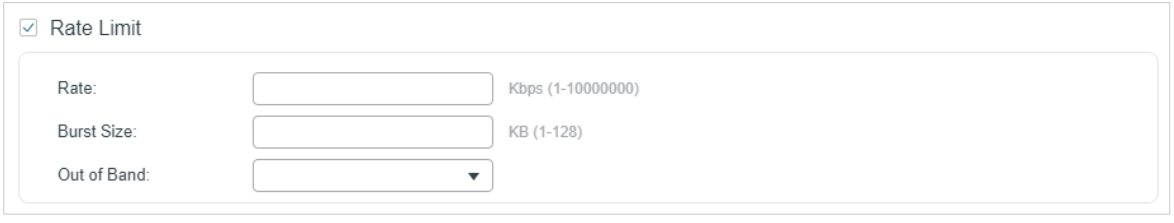


Note:

In the Mirroring feature, the matched packets will be copied to the destination port and the original forwarding will not be affected. While in the Redirect feature, the matched packets will be forwarded only on the destination port.

4) In the **Policy** section, enable or disable the Rate Limit feature for the matched packets. With this option enabled, configure the related parameters.

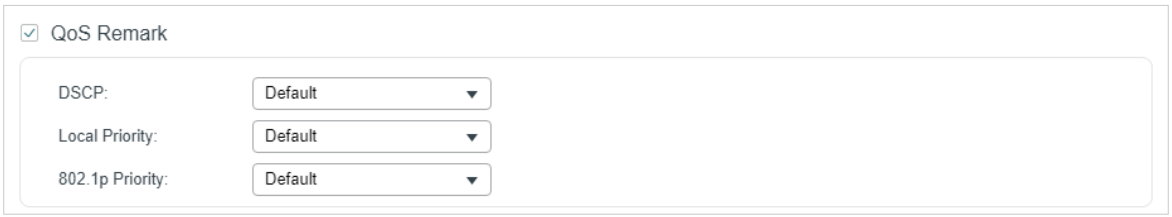
Figure 2-25 Configuring Rate Limit



Rate	Specify the transmission rate for the matched packets.
Burst Size	Specify the maximum number of bytes allowed in one second.
Out of Band	Select the action for the packets whose rate is beyond the specified rate. **None:** The packets will be forwarded normally. **Drop:** The packets will be discarded. **Remark DSCP:** You can specify a DSCP value, and the DSCP field of the packets will be changed to the specified one. Note: Remark DSCP is only available on certain devices.

5) In the **Policy** section, enable or disable the QoS Remark feature for the matched packets. With this option enabled, configure the related parameters, and the remarked values will take effect in the QoS processing on the switch.

Figure 2-26 Configuring QoS Remark



DSCP	Specify the DSCP field for the matched packets. The DSCP field of the packets will be changed to the specified one.
Local Priority	Specify the local priority for the matched packets. The local priority of the packets will be changed to the specified one.
802.1p Priority	Specify the 802.1p priority for the matched packets. The 802.1p priority of the packets will be changed to the specified one.

6) Click **Apply**.

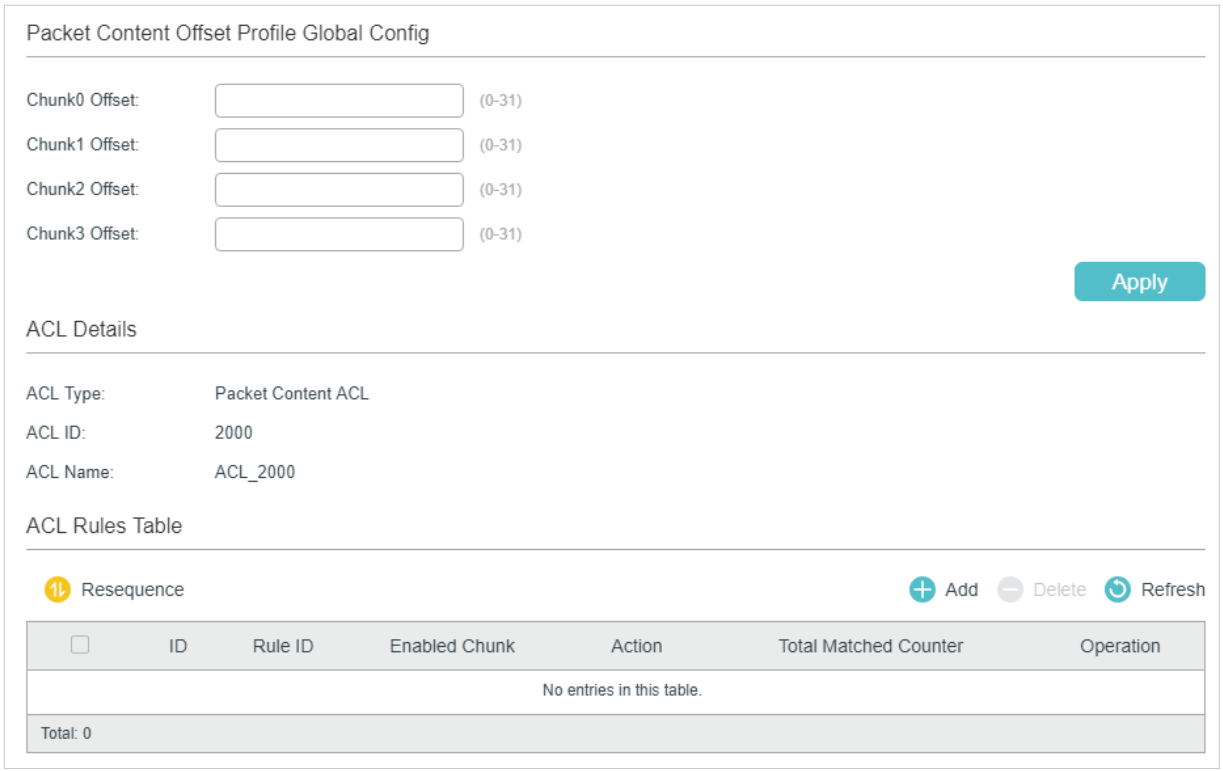
Configuring the Packet Content ACL Rule

Note:

Packet Content ACL is only available on certain devices.

Click **Edit ACL** for a Packet Content ACL entry to load the following page.

Figure 2-27 Configuring the Packet Content ACL Rule

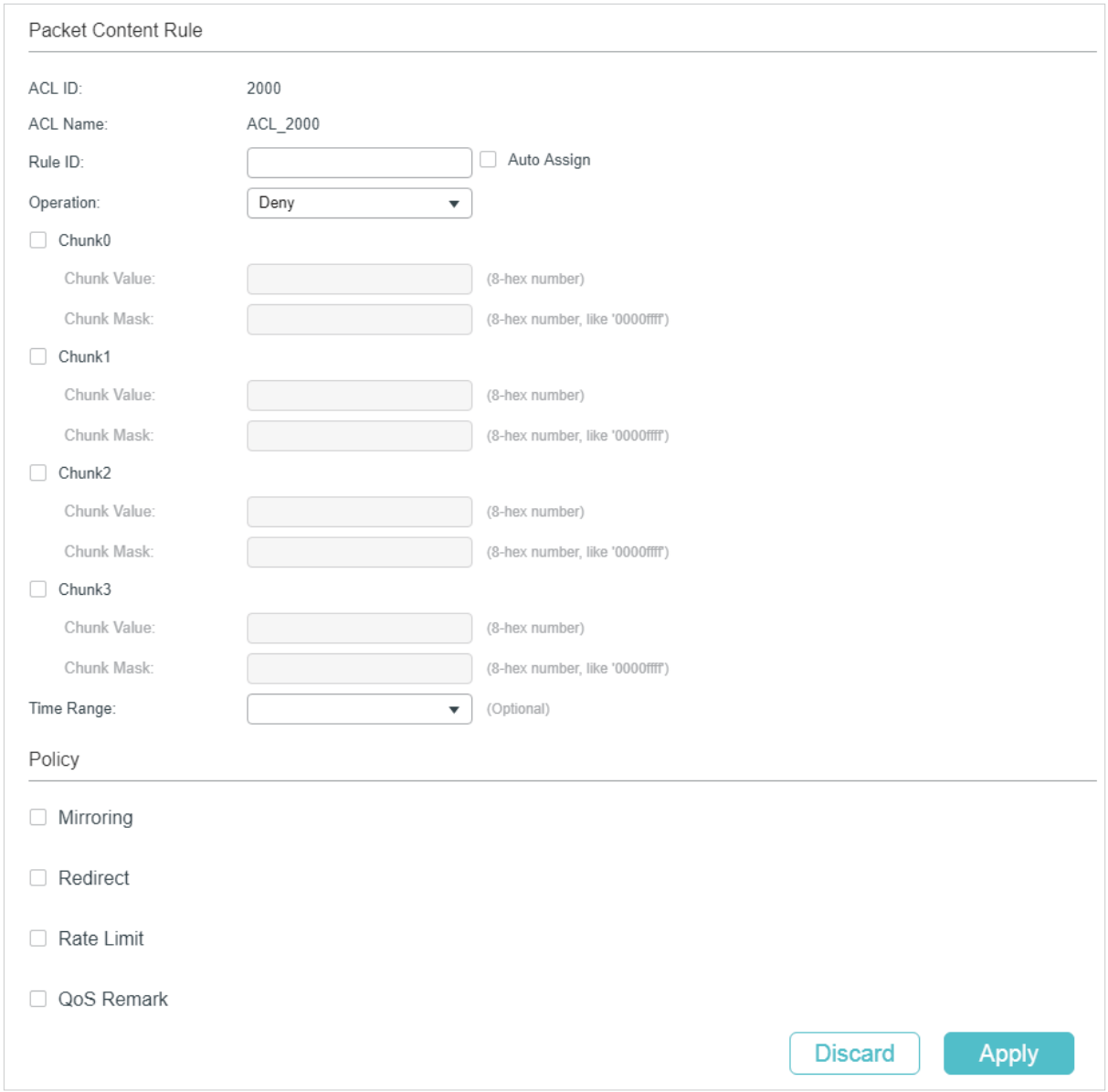


In the **Packet Content Offset Profile Global Config** section, configure the Chunk Offset. Click **Apply**.

Chunk0 Offset/ Chunk1 Offset/ Chunk2 Offset/ Chunk3 Offset	Enter the offset of a chunk. Packet Content ACL analyzes and processes data packets based on 4 chunk match conditions, and each chunk can specify a user-defined 4-byte segment carried in the packet's first 128 bytes. Offset 31 matches the 127, 128, 1, 2 bytes of the packet, offset 0 matches the 3,4,5,6 bytes of the packet, and so on, for the rest of the offset value. *Note:* All 4 chunks must be set at the same time.

In **ACL Rules Table** section, click Add and the following page will appear.

Figure 2-28 Configuring the Packet Content ACL Rule



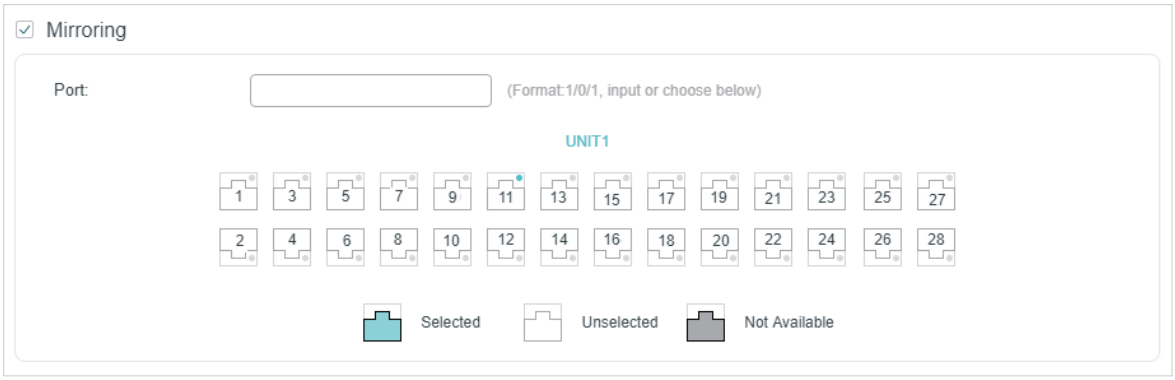
Follow these steps to configure the Packet Content ACL rule:

1) In the **Packet Content Rule** section, configure the following parameters:

Rule ID	Enter an ID number to identify the rule. It should not be the same as any current rule ID in the same ACL. If you select Auto Assign, the rule ID will be assigned automatically and the interval between rule IDs is 5.
Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.
Chunk0-Chunk3	Specify the EtherType to be matched using 4 hexadecimal numbers.
Chunk Value	Enter the 4-byte value in hexadecimal for the desired chunk, like '0000ffff'. The Packet Content ACL will check this chunk of packets to examine if the packets match the rule or not.
Chunk Mask	Enter the 4-byte mask in hexadecimal for the desired chunk. The mask must be written completely in 4-byte hex mode, like '0000ffff'. The mask specifies which bits to match the rule.
Time Range	Select a time range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect. The Time Range referenced here can be created on the **SYSTEM > Time Range** page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

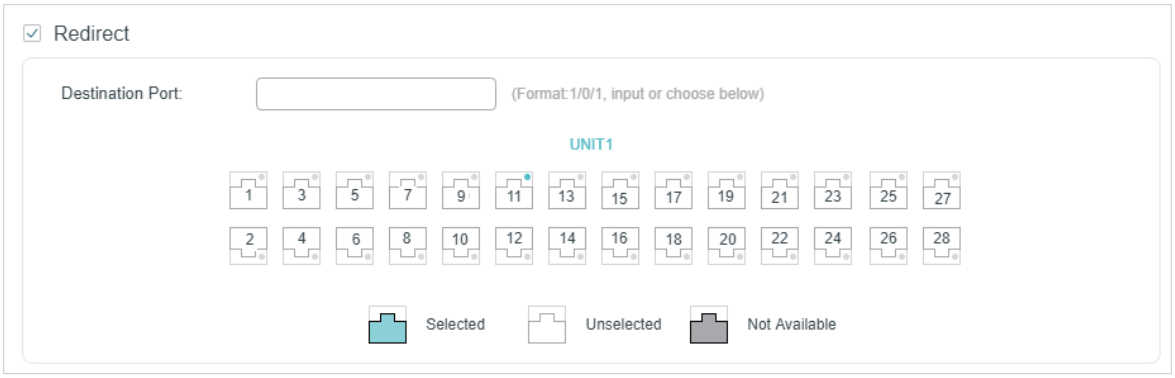
2) In the **Policy** section, enable or disable the Mirroring feature for the matched packets. With this option enabled, choose a destination port to which the packets will be mirrored.

Figure 2-29 Configuring Mirroring



3) In the **Policy** section, enable or disable the Redirect feature for the matched packets. With this option enabled, choose a destination port to which the packets will be redirected.

Figure 2-30 Configuring Redirect

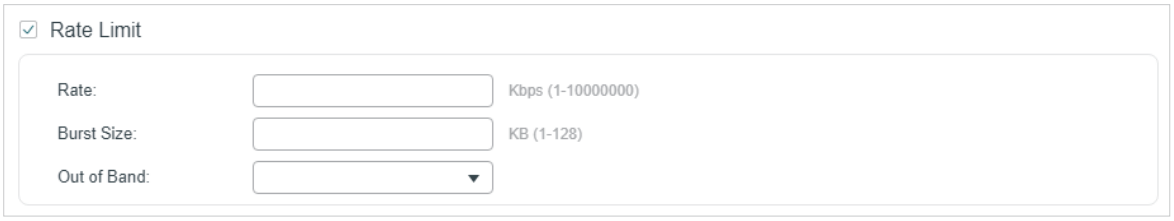


Note:

In the Mirroring feature, the matched packets will be copied to the destination port and the original forwarding will not be affected. While in the Redirect feature, the matched packets will be forwarded only on the destination port.

4) In the **Policy** section, enable or disable the Rate Limit feature for the matched packets. With this option enabled, configure the related parameters.

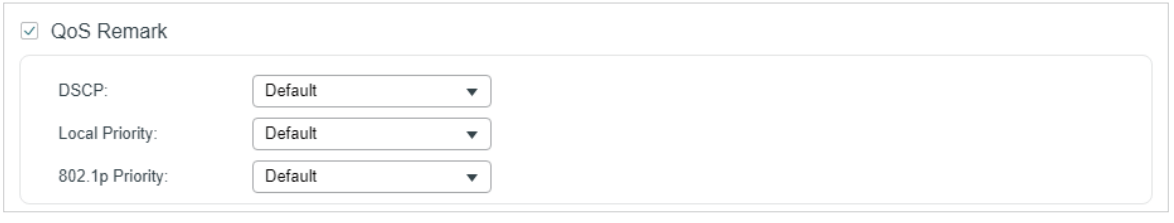
Figure 2-31 Configuring Rate Limit



Rate	Specify the transmission rate for the matched packets.
Burst Size	Specify the maximum number of bytes allowed in one second.
Out of Band	Select the action for the packets whose rate is beyond the specified rate. **None:** The packets will be forwarded normally. **Drop:** The packets will be discarded. **Remark DSCP:** You can specify a DSCP value, and the DSCP field of the packets will be changed to the specified one. Note: Remark DSCP is only available on certain devices.

5) In the **Policy** section, enable or disable the QoS Remark feature for the matched packets. With this option enabled, configure the related parameters, and the remarked values will take effect in the QoS processing on the switch.

Figure 2-32 Configuring QoS Remark



DSCP	Specify the DSCP field for the matched packets. The DSCP field of the packets will be changed to the specified one.
Local Priority	Specify the local priority for the matched packets. The local priority of the packets will be changed to the specified one.
802.1p Priority	Specify the 802.1p priority for the matched packets. The 802.1p priority of the packets will be changed to the specified one.

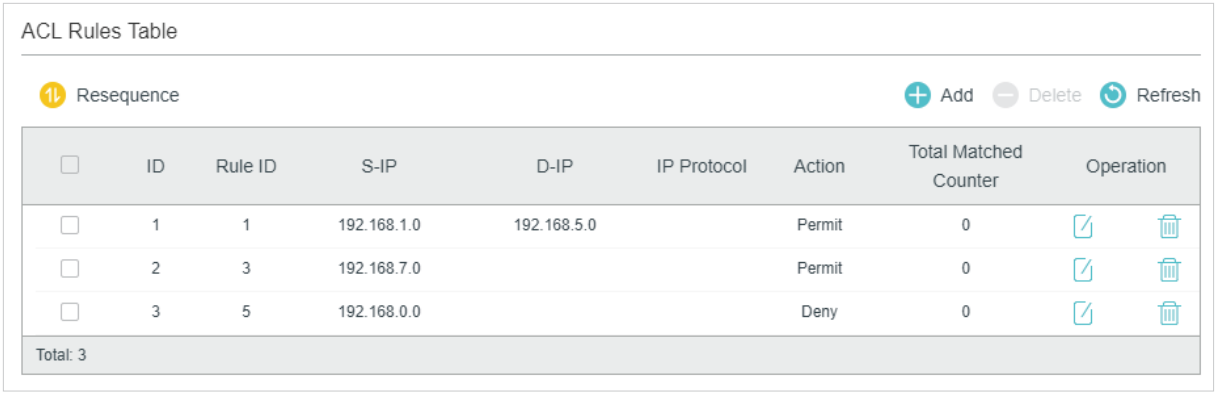
6) Click **Apply**.

Viewing the ACL Rules

The rules in an ACL are listed in ascending order of their rule IDs. The switch matches a received packet with the rules in order. When a packet matches a rule, the switch stops the match process and performs the action defined in the rule.

Click **Edit ACL** for an entry you have created and you can view the rule table. We take IP ACL rules table for example.

Figure 2-33 Viewing ACL Rules Table



Here you can view and edit the ACL rules. You can also click **Resequence** to resequence the rules by providing a Start Rule ID and Step value.

2.1.4 Configuring ACL Binding

You can bind the ACL to a port or a VLAN. The received packets on the port or in the VLAN will then be matched and processed according to the ACL rules. An ACL takes effect only after it is bound to a port or VLAN.

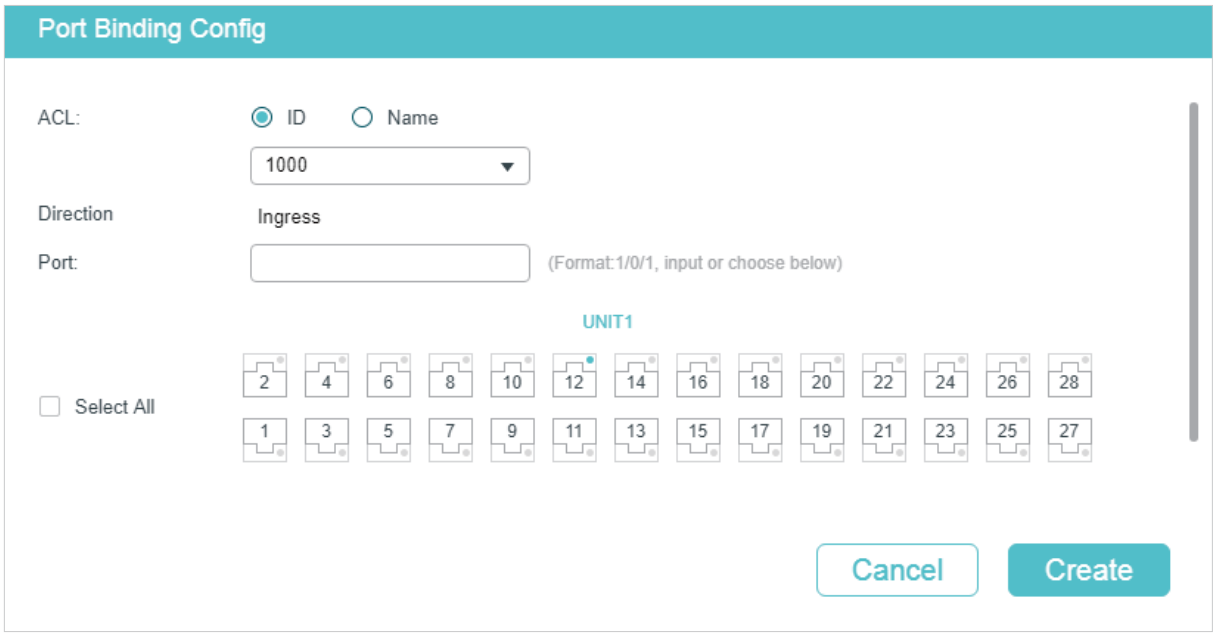
Note:

- Different types of ACLs cannot be bound to the same port or VLAN.
- Multiple ACLs of the same type can be bound to the same port or VLAN. The switch matches the received packets using the ACLs in order. The ACL that is bound earlier has a higher priority.

Binding the ACL to a Port

Choose the menu **SECURITY > ACL > ACL Binding > Port Binding** and click Add to load the following page.

Figure 2-34 Binding the ACL to a Port



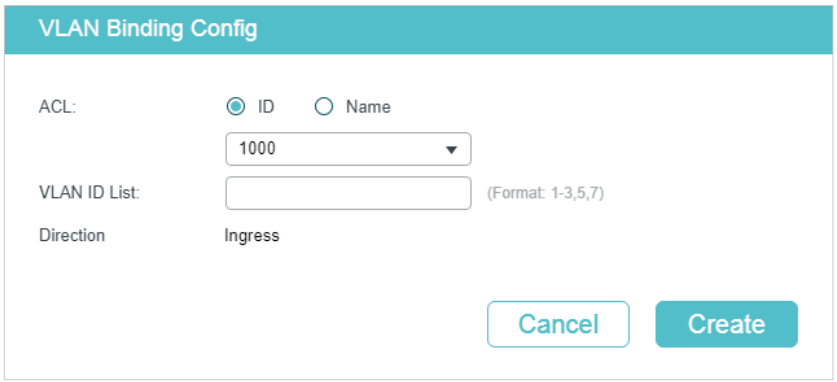
Follow these steps to bind the ACL to a Port:

1) Choose ID or Name to be used for matching the ACL. Then select an ACL from the drop-down list.
2) Specify the port to be bound.
3) Click **Create**.

■ Binding the ACL to a VLAN

Choose the menu **SECURITY > ACL > ACL Binding > VLAN Binding** to load the following page.

Figure 2-35 Binding the ACL to a VLAN



Follow these steps to bind the ACL to a VLAN:

1) Choose ID or Name to be used for matching the ACL. Then select an ACL from the drop-down list.
2) Enter the ID of the VLAN to be bound.
3) Click **Create**.

2.2 Using the CLI

2.2.1 Configuring Time Range

Some ACL-based services or features may need to be limited to take effect only during a specified time period. In this case, you can configure a time range for the ACL. For details about Time Range Configuration, please refer to Managing System.

2.2.2 Configuring ACL

Follow the steps to create different types of ACL and configure the ACL rules.

You can define the rules based on source or destination IP address, source or destination MAC address, protocol type, port number and others.

MAC ACL

Follow these steps to configure MAC ACL:

Step 1	**configure** Enter global configuration mode.
Step 2	**access-list create** *acl-id* **[name** *acl-name***]** Create a MAC ACL. *acl-id:* Enter an ACL ID. The ID ranges from 0 to 499. *acl-name:* Enter a name to identify the ACL.

Step 3	**access-list mac** *acl-id-or-name* **rule** { auto | *rule-id* } { deny | permit } **logging** {enable | disable} [**smac** *source-mac* **smask** *source-mac-mask*] [**dmac** *destination-mac* **dmask** *destination-mac-mask*] [**type** ether-type] [**pri** *dot1p-priority*] [**vid** *vlan-id*] [**tseg** *time-range-name*] Add a MAC ACL Rule. *acl-id-or-name*: Enter the ID or name of the ACL that you want to add a rule for. *auto:* The rule ID will be assigned automatically and the interval between rule IDs is 5. *rule-id*: Assign an ID to the rule. deny | permit: Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected. **logging** {enable | disable}: Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes. *source-mac*: Enter the source MAC address. The format is FF:FF:FF:FF:FF:FF. *source-mac-mask*: Enter the mask of the source MAC address. This is required if a source MAC address is entered. The format is FF:FF:FF:FF:FF:FF. *destination-mac*: Enter the destination MAC address. The format is FF:FF:FF:FF:FF:FF. *destination-mac-mask*: Enter the mask of the destination MAC address. This is required if a destination MAC address is entered. The format is FF:FF:FF:FF:FF:FF. ether-type: Specify an Ethernet-type with 4 hexadecimal numbers. *dot1p-priority*: The user priority ranges from 0 to 7. The default is No Limit. *vlan-id*: The VLAN ID ranges from 1 to 4094. *time-range-name*: The name of the time-range. The default is No Limit.
Step 4	**exit** Return to global configuration mode.
Step 5	**show access-list** [*acl-id-or-name*] Display the current ACL configuration. *acl-id-or-name*: The ID number or name of the ACL.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create MAC ACL 50 and configure Rule 5 to permit packets with source MAC address 00:34:A2:D4:34:B5:

Switch#configure

Switch(config)#access-list create 50

Switch(config-mac-acl)#access-list mac 50 **rule** 5 **permit logging** disable **smac** 00:34:A2:D4:34:B5 **smask** FF:FF:FF:FF:FF:FF

Switch(config-mac-acl)#exit

Switch(config)#show access-list 50

MAC access list 50 name: ACL_50

rule 5 permit logging disable smac 00:34:a2:d4:34:b5 smask ff:ff:ff:ff:ff:ff

Switch(config)#end

Switch#copy running-config startup-config

IP ACL

Follow these steps to configure IP ACL:

Step 1	**configure** Enter global configuration mode.
Step 2	**access-list create** *acl-id* **[name** *acl-name***]** Create an IP ACL. *acl-id*: Enter an ACL ID. The ID ranges from 500 to 999. *acl-name*: Enter a name to identify the ACL.

Step 3 **access-list ip** *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**sip** *sip-address* **sip-mask** *sip-address-mask*] [**dip** *dip-address* **dip-mask** *dip-address-mask*] [**dscp** *dscp-value*] [**tos** *tos-value*] [**pre** *pre-value*] [**frag** {enable | disable}] [**protocol** *protocol* [**s-port** *s-port-number* **s-port-mask** *s-port-mask*] [**d-port** *d-port-number* **d-port-mask** *d-port-mask*] [**tcpflag** *tcpflag*]] [**tseg** *time-range-name*]

Add rules to the ACL.

acl-id-or-name: Enter the ID or name of the ACL that you want to add a rule for.

auto: The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id: Assign an ID to the rule.

deny | permit: Specify the action to be taken with the packets that match the rule. Deny means to discard; permit means to forward. By default, it is set to permit.

logging {enable | disable}: Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

sip-address: Enter the source IP address.

sip-address-mask: Enter the mask of the source IP address. This is required if a source IP address is entered.

dip-address: Enter the destination IP address.

dip-address-mask: Enter the mask of the destination IP address. This is required if a destination IP address is entered.

dscp-value: Specify the DSCP value between 0 and 63.

tos-value: Specify an IP ToS value to be matched between 0 and 15.

pre-value: Specify an IP Precedence value to be matched between 0 and 7.

frag {enable | disable}**:** Enable or disable matching of fragmented packets. The default is disable. When enabled, the rule will apply to all fragmented packets and always permit to forward the last fragment of a packet.
Note: **frag** {enable | disable} is only available on certain devices.

protocol: Specify a protocol number between 0 and 255.

s-port-number: With TCP or UDP configured as the protocol, specify the source port number.

s-port-mask: With TCP or UDP configured as the protocol, specify the source port mask with 4 hexadacimal numbers.

d-port-number: With TCP or UDP configured as the protocol, specify the destination port number.

d-port-mask: With TCP or UDP configured as the protocol, specify the destination port mask with 4 hexadacimal numbers.

tcpflag: With TCP configured as the protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched.

The flags are URG (Urgent flag), ACK (Acknowledge Flag), PSH (Push Flag), RST (Reset Flag), SYN (Synchronize Flag) and FIN (Finish Flag).

time-range-name: The name of the time-range. The default is No Limit.

Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create IP ACL 600, and configure Rule 1 to permit packets with source IP address 192.168.1.100:

Switch#configure

Switch(config)#access-list create 600

Switch(config)#access-list ip 600 **rule** 1 **permit logging** disable **sip** 192.168.1.100 **sip-mask** 255.255.255.255

Switch(config)#show access-list 600

IP access list 600 name: ACL_600

rule 1 permit logging disable sip 192.168.1.100 smask 255.255.255.255

Switch(config)#end

Switch#copy running-config startup-config

Combined ACL

Follow these steps to configure Combined ACL:

Step 1	**configure** Enter global configuration mode
Step 2	**access-list create** *acl-id* **[name** *acl-name***]** Create a Combined ACL. *acl-id:* Enter an ACL ID. The ID ranges from 1000 to 1499. *acl-name:* Enter a name to identify the ACL.

Step 3 **access-list combined** *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**smac** *source-mac-address* **smask** *source-mac-mask*] [**dmac** *dest-mac-address* **dmask** *dest-mac-mask*] [**vid** *vlan-id*] [**type** *ether-type*] [**pri** *priority*] [**sip** *sip-address* **sip-mask** *sip-address-mask*] [**dip** *dip-address* **dip-mask** *dip-address-mask*] [**dscp** *dscp-value*] [**tos** *tos-value*] [**pre** *pre-value*] [**protocol** *protocol* [**s-port** *s-port-number* **s-port-mask** *s-port-mask*] [**d-port** *d-port-number* **d-port-mask** *d-port-mask*] [**tcpflag** *tcpflag*]] [**tseg** *time-range-name*]

Add rules to the ACL.

acl-id-or-name: Enter the ID or name of the ACL that you want to add a rule for.

auto: The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id: Assign an ID to the rule.

deny | permit: Specify the action to be taken with the packets that match the rule. Deny means to discard; permit means to forward. By default, it is set to permit.

logging {enable | disable}: Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

source-mac-address: Enter the source MAC address.

source-mac-mask: Enter the source MAC address mask.

dest-mac-address: Enter the destination MAC address.

dest-mac-mask: Enter the destination MAC address mask. This is required if a destination MAC address is entered.

vlan-id: The VLAN ID ranges from 1 to 4094.

ether-type: Specify the Ethernet-type with 4 hexadecimal numbers.

priority: The user priority ranges from 0 to 7. The default is No Limit.

sip-address: Enter the source IP address.

sip-address-mask: Enter the mask of the source IP address. It is required if source IP address is entered.

dip-address: This is required if a source IP address is entered.

dip-address-mask: Enter the destination IP address mask. This is required if a destination IP address is entered.

dscp-value: Specify the DSCP value between 0 and 63.

tos-value: Specify an IP ToS value to be matched between 0 and 15.

pre-value: Specify an IP Precedence value to be matched between 0 and 7.

	protocol: Specify a protocol number between 0 and 255. *s-port-number:* With TCP or UDP configured as the protocol, specify the source port number. *s-port-mask:* With TCP or UDP configured as the protocol, specify the source port mask with 4 hexadacimal numbers. *d-port-number:* With TCP or UDP configured as the protocol, specify the destination port number. *d-port-mask:* With TCP or UDP configured as the protocol, specify the destination port mask with 4 hexadacimal numbers. *tcpflag:* With TCP configured as the protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched. The flags are URG (Urgent flag), ACK (Acknowledge Flag), PSH (Push Flag), RST (Reset Flag), SYN (Synchronize Flag), and FIN (Finish Flag). *time-range-name*: The name of the time-range. The default is No Limit.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create Combined ACL 1100 and configure Rule 1 to deny packets with source IP address 192.168.3.100 in VLAN 2:

Switch#configure

Switch(config)#access-list create 1100

Switch(config)#access-list combined 1100 **logging** disable **rule** 1 **permit vid** 2 **sip** 192.168.3.100 **sip-mask** 255.255.255.255

Switch(config)#show access-list 2600

Combined access list 2600 name: ACL_2600

rule 1 permit logging disable vid 2 sip 192.168.3.100 sip-mask 255.255.255.255

Switch(config)#end

Switch#copy running-config startup-config

IPv6 ACL

Follow these steps to configure IPv6 ACL:

Step 1	**configure** Enter global configuration mode

Step 2	**access-list create** *acl-id* **[name** *acl-name***]** Create an IPv6 ACL. *acl-id:* Enter an ACL ID. The ID ranges from 1500 to 1999. *acl-name:* Enter a name to identify the ACL.
Step 3	**access-list ipv6** *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**class** *class-value*] [**flow-label** *flow-label-value*] [**sip** *source-ip-address* **sip-mask** *source-ip-mask*] [**dip** *destination-ip-address* **dip-mask** *destination-ip-mask*] [**s-port** *source-port-number*] [**d-port** *destination-port-number*] [**tseg** *time-range-name*] Add rules to the ACL. *acl-id-or-name*: Enter the ID or name of the ACL that you want to add a rule for. *auto:* The rule ID will be assigned automatically and the interval between rule IDs is 5. *rule-id*: Assign an ID to the rule. deny | permit: Specify the action to be taken with the packets that match the rule. Deny means to discard; permit means to forward. By default, it is set to permit. **logging** {enable | disable}: Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes. *class-value*: Specify a class value to be matched. It ranges from 0 to 63. *flow-label-value*: Specify a Flow Label value to be matched. *source-ip-address:* Enter the source IP address. Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid. *source-ip-mask:* Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule. *destination-ip-address*: Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 addresses but only the first 64 bits will be valid. *destination-ip-mask:* Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule. *source-port-number*: Enter the TCP/UDP source port if TCP/UDP protocol is selected. *destination-port-number*: Enter the TCP/UDP destination port if TCP/UDP protocol is selected. *time-range-name*: The name of the time-range. The default is No Limit.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create IPv6 ACL 1600 and configure Rule 1 to deny packets with source IPv6 address CDCD:910A:2222:5498:8475:1111:3900:2020:

Switch#configure

Switch(config)#access-list create 1600

Switch(config)#access-list ipv6 1600 **rule** 1 **deny logging** disable **sip** CDCD:910A:2222:5498:8475:1111:3900:2020 **sip-mask** ffff:ffff:ffff:ffff

Switch(config)#show access-list 1600

IPv6 access list 1600 name: ACL_1600

rule 1 deny logging disable sip cdcd:910a:2222:5498:8475:1111:3900:2020 sip-mask ffff:ff

ff:ffff:ffff

Switch(config)#end

Switch#copy running-config startup-config

Packet Content ACL

Note:

Packet Content ACL is only available on certain devices.

Step 1	**configure** Enter global configuration mode
Step 2	**access-list create** *acl-id* **[name** *acl-name***]** Create a Packet Content ACL. *acl-id*:Enter an ACL ID. The ID ranges from 2000 to 2499. *acl-name*: Enter a name to identify the ACL.
Step 3	**access-list packet-content profile chunk-offset0** *offset0* **chunk-offset1** *offset1* **chunk-offset2** *offset2* **chunk-offset3** *offset3* Specify the offset of each chunk, all the 4 chunks must be set at the same time. *offset0* **-***offset3*: Specify the offset of each chunk, the value ranges from 0 to 31. When the offset is set as 31, it matches the first 127,128, 1, 2 bytes of the packet; when the offset is set as 0, it matches the 3, 4, 5, 6 bytes, and so on, for the rest of the offset value.

Step 4	**access-list packet-content config** *acl-id-or-name* **rule** { auto | *rule-id* } {deny | permit} **logging** { enable | disable } [**chunk0** *value* **mask0** *mask*] [**chunk1** *value* **mask1** *mask*] [**chunk2** *value* **mask2** *mask*] [**chunk3** *value* **mask3** *mask*] [**tseg** *time-range-name*] Add rules to the ACL. *acl-id-or-name*: Enter the ID or name of the ACL that you want to add a rule for. auto: The rule ID will be assigned automatically and the interval between rule IDs is 5. *rule-id*: Assign an ID to the rule. deny | permit: Specify the action to be taken with the packets that match the rule. Deny means to discard; permit means to forward. By default, it is set to permit. **logging** { enable | disable} : Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes. *value*: Enter the 4-byte value in hexadecimal for the desired chunk, like '0000ffff'. The Packet Content ACL will check this chunk of packets to examine if the packets match the rule or not. *mask*: Enter the 4-byte mask in hexadecimal for the desired chunk. The mask must be written completely in 4-byte hex mode, like '0000ffff'. The mask specifies which bits to match the rule. *time-range-name*: The name of the time-range. The default is No Limit.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create Packet Content ACL 2000, and deny the packets with the value of its chunk1 0x58:

Switch#configure

Switch(config)#access-list create 2000

Switch(config)#access-list packet-content profile chunk-offset0 offset0 **chunk-offset1** offset1 **chunk-offset2** offset2 **chunk-offset3** offset3

Switch(config)#packet-content config 2000 **rule** 10 deny **logging** disable **chunk**1 58 **mask1** ffffffff

Switch(config)#show access-list 2000

Packet content access list 2000 name: ACL_2000

rule 10 deny logging disable chunk1 value 0x58 mask 0xffffffff

Switch(config)#end

Switch#copy running-config startup-config

Resequencing Rules

Note:

Resequencing Rules is only available on certain devices.

You can resequence the rules by providing a Start Rule ID and Step value.

Step 1	**configure** Enter global configuration mode.
Step 2	**access-list resequence** *acl-id-or-name* **start** *start-rule-id* **step** *rule-id-step-value* Resequence the rules of the specific ACL. *acl-id-or-name*: Enter the ID or name of the ACL. *start-rule-id*: Enter the start rule ID. *rule-id-step-value*: Enter the Step value.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to resequence the rules of MAC ACL 100: set the start rule ID as 1 and the step value as 10:

Switch#configure

Switch(config)#access-list resequence 100 **start** 1 **step** 10

Switch(config)#show access-list 100

MAC access list 100 name: “ACL_100”

rule 1 deny logging disable smac aa:bb:cc:dd:ee:ff smask ff:ff:ff:ff:ff:ff

rule 11 permit logging disable vid 18

rule 21 permit logging disable dmac aa:cc:ee:ff:dd:33 dmask ff:ff:ff:ff:ff:ff

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring Policy

Policy allows you to further process the matched packets through operations such as mirroring, rate-limiting, redirecting, or changing priority.

Follow the steps below to configure the policy actions for an ACL rule.

Step 1	**configure** Enter global configuration mode.
Step 2	**access-list action** *acl-id-or-name* **rule** *rule-id* Configure the policy actions for an ACL rule. *acl-id-or-name*: Enter the ID or name of the ACL. *rule-id*: Enter the ID of the ACL rule.
Step 3	**redirect interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } (Optional) Define the policy to redirect the matched packets to the desired port. *port*: The destination port to which the packets will be redirected. The default is All. **s-mirror interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } (Optional) Define the policy to mirror the matched packets to the desired port. *port*: The destination port to which the packets will be mirrored. **s-condition rate** *rate* **burst** *burst-size* **osd** { **none | discard | remark dscp** *dscp* } (Optional) Define the policy to monitor the rate of the matched packets. *rate*: Specify a rate from 1 to 1000000 kbps. *burst-size*: Specify the number of bytes allowed in one second ranging from 1 to 128. **osd**: Select either “none”, “discard” or “remark dscp” as the action to be taken for the packets whose rate is beyond the specified rate. The default is None. When “remark dscp” is selected, you also need to specify the DSCP value for the matched packets. The DSCP value ranges from 0 to 63. Note: Remark DSCP is only available on certain devices. **qos-remark** [**dscp** *dscp*] [**priority** *pri*] [**dot1p** *pri*] (Optional) Define the policy to remark priority for the matched packets. *dscp*: Specify the DSCP region for the data packets. The value ranges from 0 to 63. **priority** *pri*: Specify the local priority for the data packets. The value ranges from 0 to 7. **dot1p** *pri*: Specify the 802.1p priority for the data packets. The value ranges from 0 to 7.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

Redirect the matched packets to port 1/0/4 for rule 1 of MAC ACL 10:

Switch#configure

Switch(config)#access-list action 10 rule 1

Switch(config-action)#redirect interface gigabitEthernet 1/0/4

Switch(config-action)#exit

Switch(config)#show access-list 10

MAC access list 10 name: ACL_10

rule 5 permit logging disable action redirect Gi1/0/4

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Configuring ACL Binding

You can bind the ACL to a port or a VLAN. The received packets on the port or in the VLAN will then be matched and processed according to the ACL rules. An ACL takes effect only after it is bound to a port or VLAN.

Note:

- Different types of ACLs cannot be bound to the same port or VLAN.
- Multiple ACLs of the same type can be bound to the same port or VLAN. The switch matches the received packets using the ACLs in order. The ACL that is bound earlier has a higher priority.

Follow the steps below to bind ACL to a port or a VLAN:

Step 1	**configure** Enter global configuration mode
Step 2	**access-list bind** *acl-id-or-name* **interface** { [**vlan** *vlan-list*] | [**fastEthernet** *port-list*] | [**gigabitEthernet** *port-list*] | [**ten-gigabitEthernet** *port-list*] } Bind the ACL to a port or a VLAN. *acl-id-or-name*: Enter the ID or name of the ACL that you want to add a rule for. *vlan-list*: Specify the ID or the ID list of the VLAN(s) that you want to bind the ACL to. The valid values are from 1 to 4094, for example, 2-3,5. *port-list*: Specify the number or the list of the Ethernet port that you want to bind the ACL to.
Step 3	**show access-list bind** View the ACL binding configuration.
Step 4	**end** Return to privileged EXEC mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind ACL 1 to port 3 and VLAN 4:

Switch#configure

Switch(config)#access-list bind 1 **interface vlan** 4 **gigabitEthernet** 1/0/3

SSwitch(config)#show access-list bind

ACL ID	ACL NAME	Interface/VID	Direction	Type
---	---	---	---	---
1	ACL_1	Gi1/0/3	Ingress	Port
1	ACL_1	4	Ingress	VLAN

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Viewing ACL Counting

You can use the following command to view the number of matched packets of each ACL in the privileged EXEC mode and any other configuration mode:

show access-list *acl-id-or-name* **counter**

View the number of matched packets of the specific ACL.

acl-id-or-name: Specify the ID or name of the ACL to be viewed.

3 Configuration Example for ACL

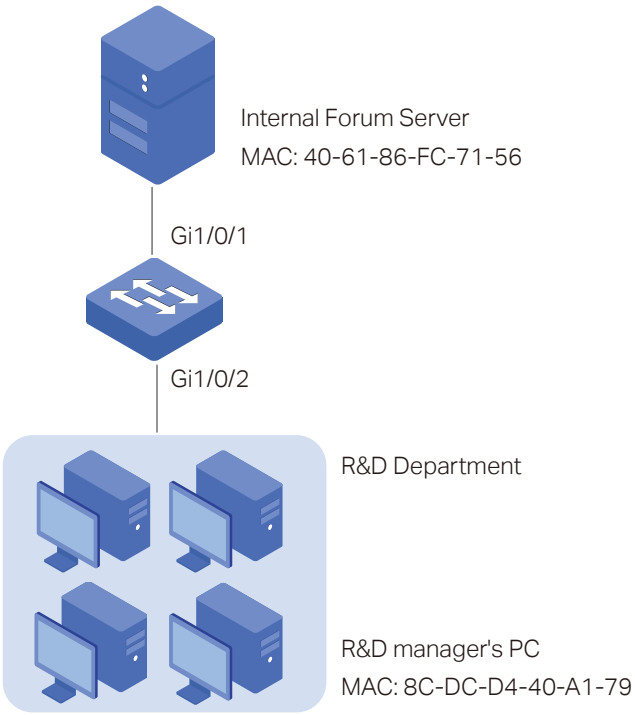
3.1 Configuration Example for MAC ACL

3.1.1 Network Requirements

A company forbids the employees in the R&D department to visit the internal forum during work hours. While the manager of the R&D department can get access to the internal forum without limitation.

As shown below, the internal forum server is connected to the switch via port 1/0/1, and computers in the R&D department are connected to the switch via port 1/0/2.

Figure 3-1 Network Topology



3.1.2 Configuration Scheme

To meet the requirements above, you can set up packet filtering by creating an MAC ACL and configuring rules for it.

- Time Range Configuration

Create a time range entry for the work hour of the company. Apply the time range to the ACL rule which blocks the access to internal forum server.

- ACL Configuration

Create a MAC ACL and configure the following rules for it:

- Configure a permit rule to match packets with source MAC address 8C-DC-D4-40-A1-79 and destination MAC address 40-61-86-FC-71-56. This rule allows the manager of R&D department to visit internal forum at any time.
- Configure a deny rule to match packets with destination MAC address 40-61-86-FC-71-56 and apply the time range of work hours. This rule forbids the employees in the R&D department to visit the internal forum during work hours.
- Configure a permit rule to match all the packets that do not match neither of the above rules.

- Binding Configuration

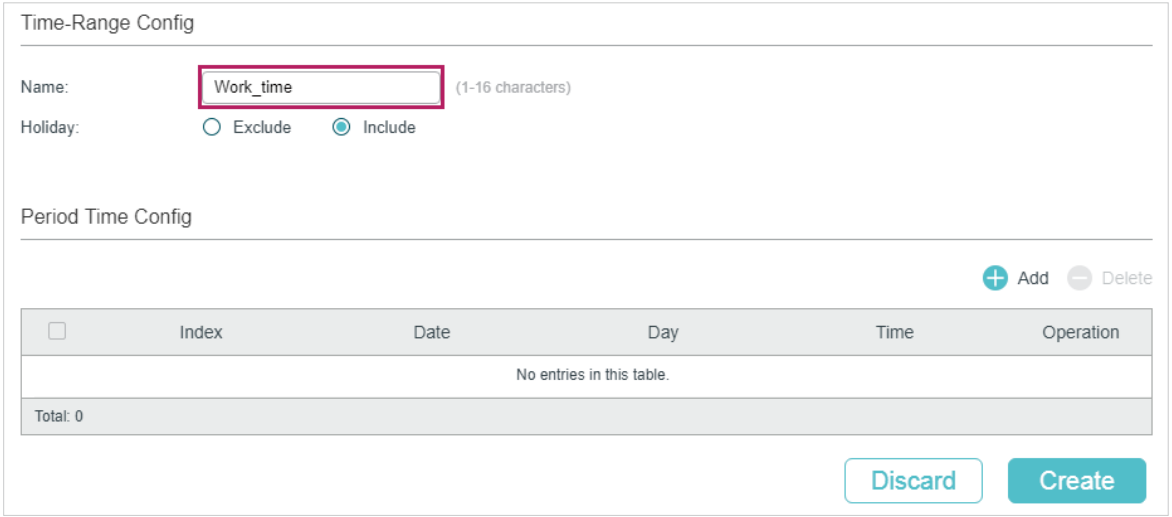
Bind the MAC ACL to port 1/0/2 so that the ACL rules will be applied to the computer of the devices in the R&D department which are restricted to the internal forum during work hours.

Demonstrated with T1600G-28TS, the following sections explain the configuration procedure in two ways: using the GUI and using the CLI.

3.1.3 Using the GUI

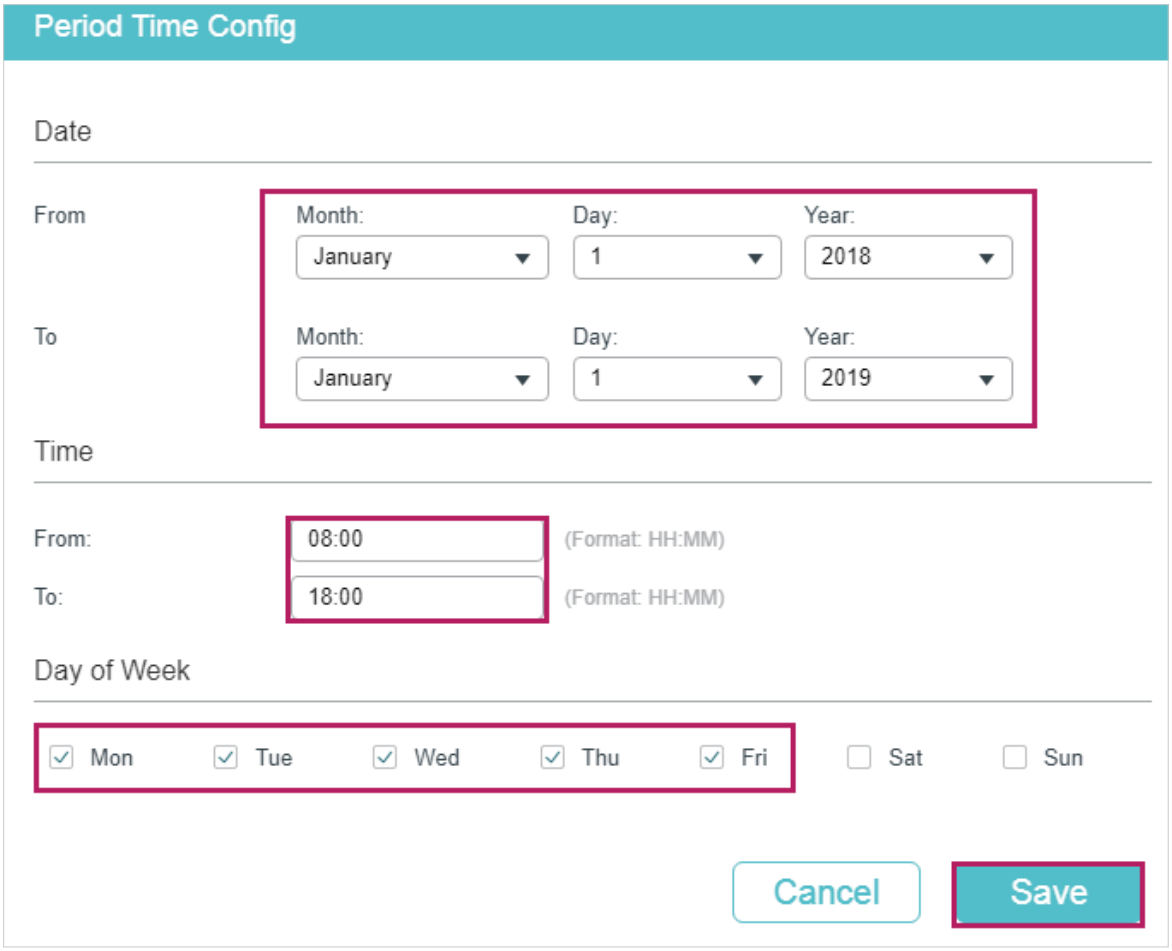
1) Choose the menu **SYSTEM** > **Time Range > Time Range Config** and click Add to load the following page. Create a time range named Work_time.

Figure 3-2 Configuring Time Range



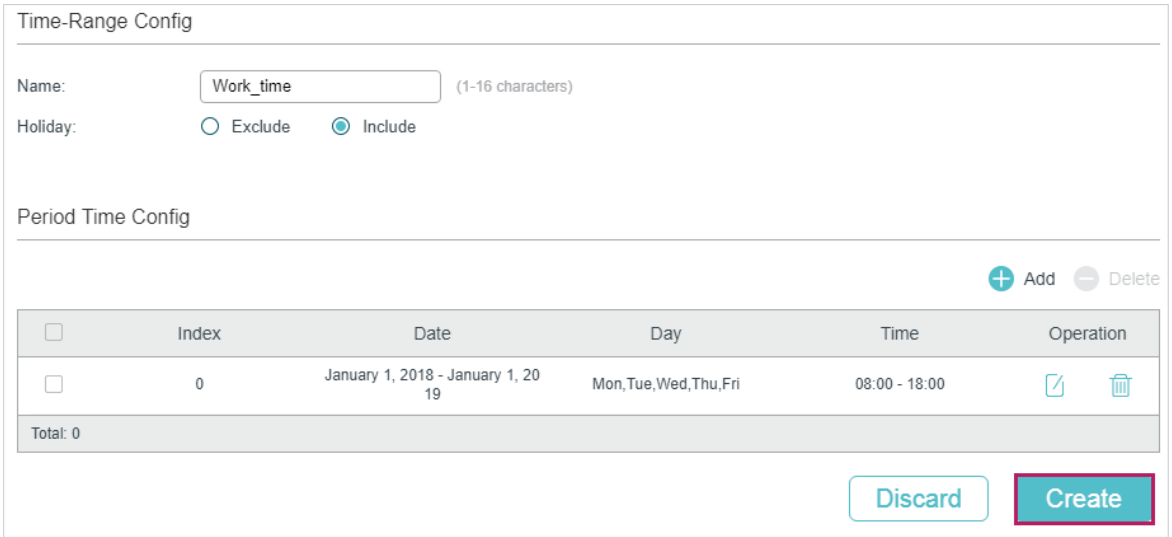
2) In the **Period Time Config** section, click Add and the following window will pop up. Add the work hour of the company in the **Period Time** and click **Save**.

Figure 3-3 Adding Period Time



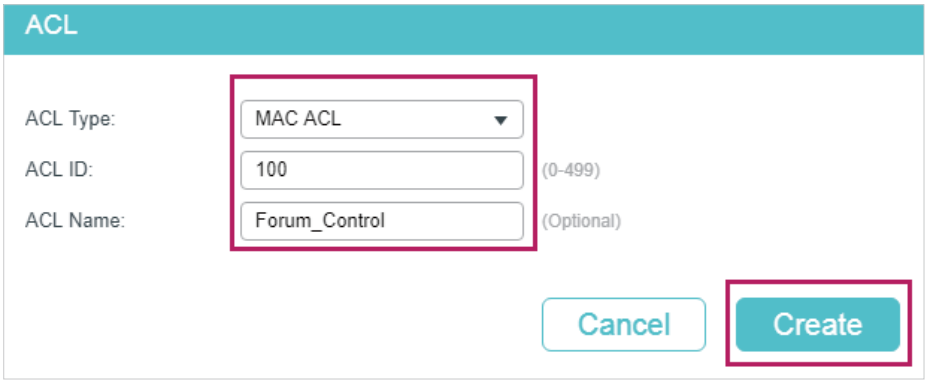
3) After adding the Period Time, click **Create** to save the time range entry.

Figure 3-4 Creating Time Range



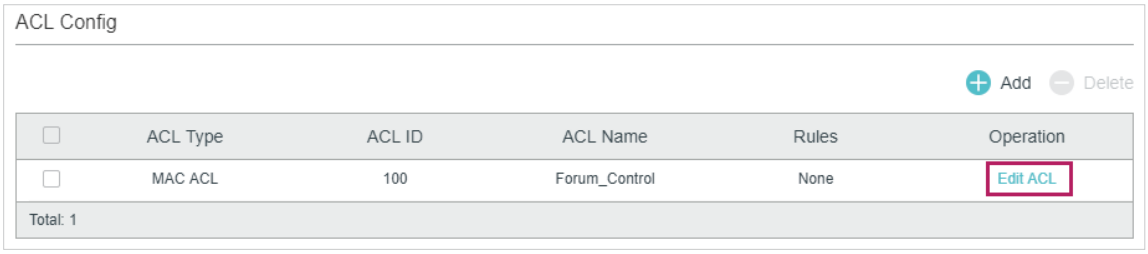
4) Choose the menu **SECURITY > ACL > ACL Config** and click Add to load the following page. Then create a MAC ACL for the marketing department.

Figure 3-5 Creating a MAC ACL



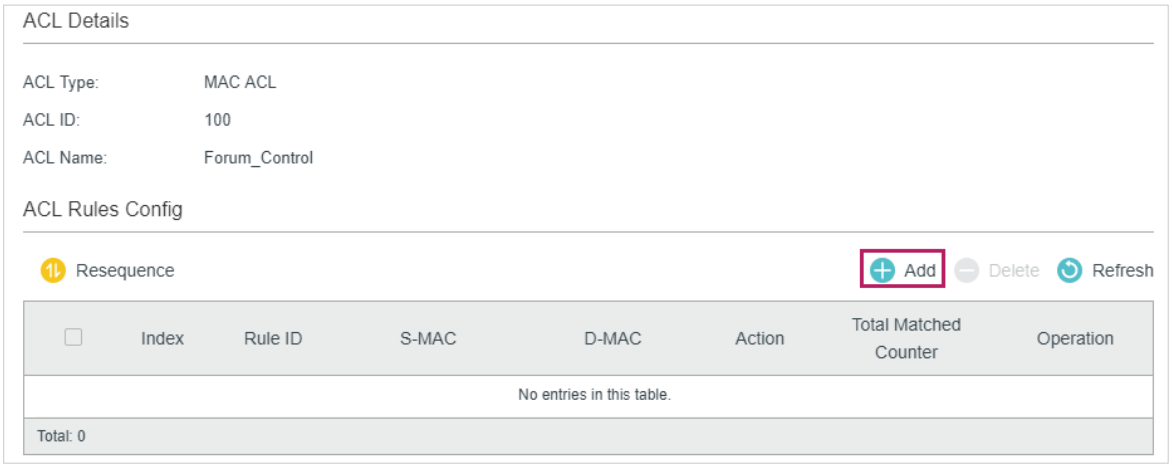
5) Click **Edit ACL** in the Operation column.

Figure 3-6 Editing the MAC ACL



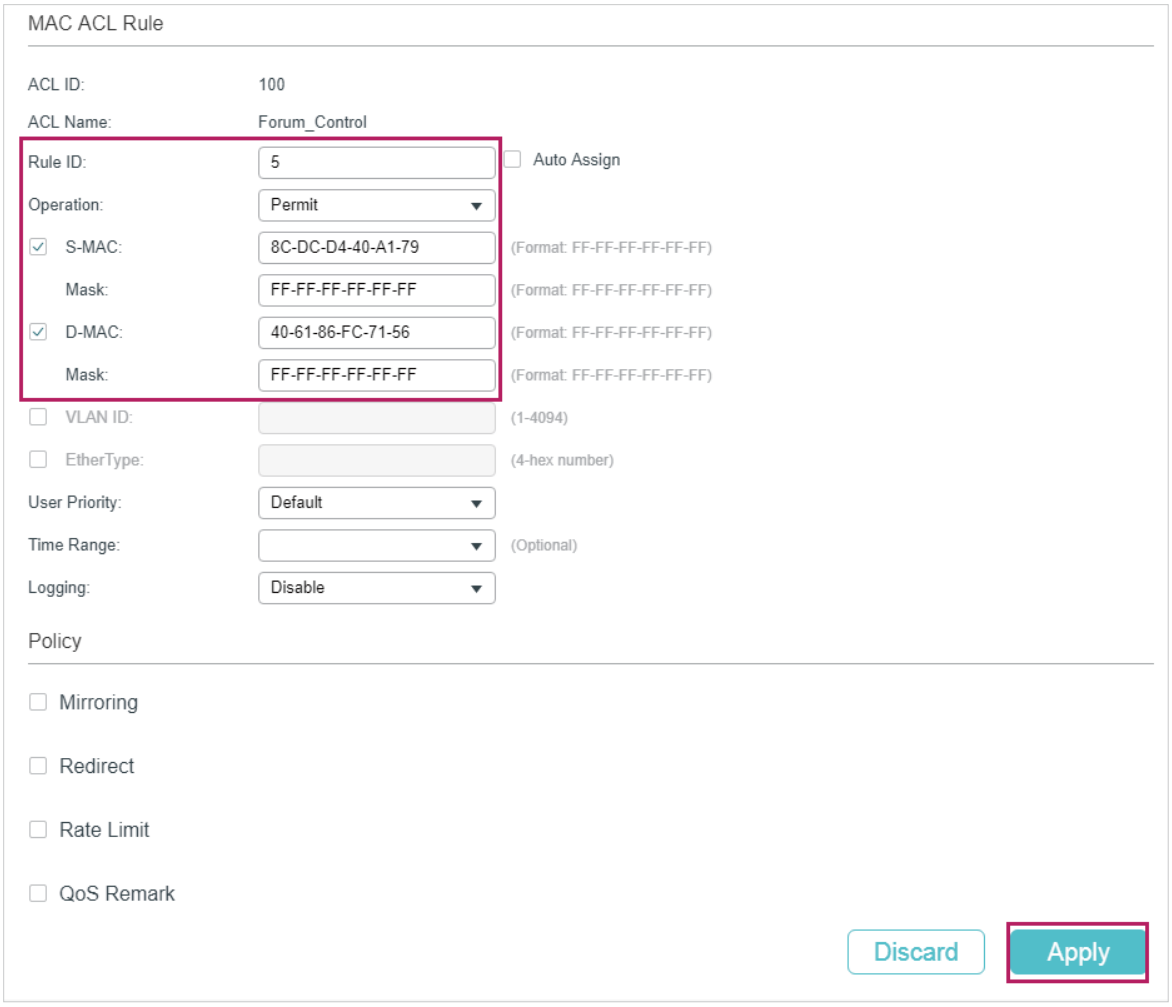
6) On the ACL configuration page, click Add.

Figure 3-7 Editing the MAC ACL



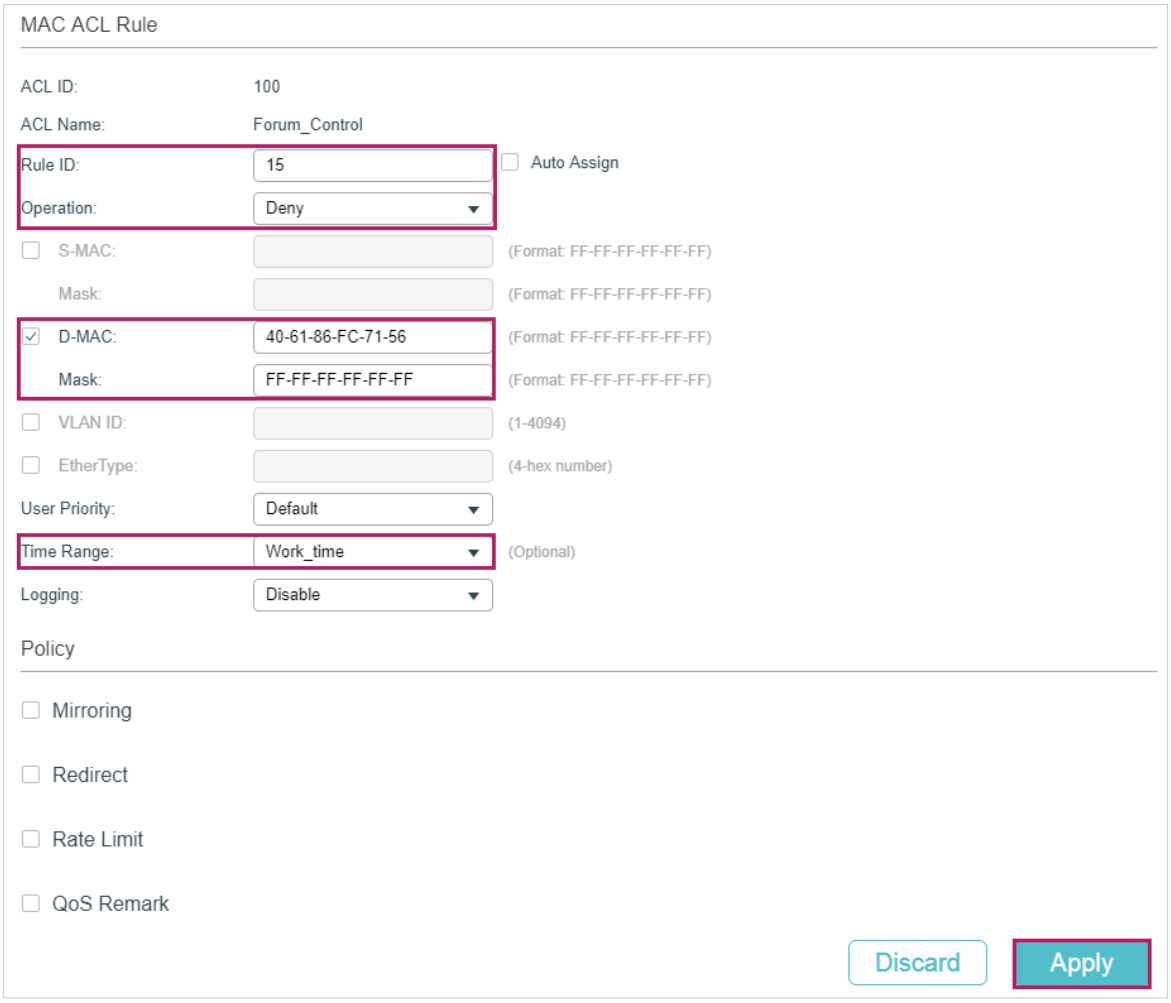
7) Configure rule 5 to permit packets with the source MAC address 8C-DC-D4-40-A1-79 and destination MAC address 40-61-86-FC-71-56.

Figure 3-8 Configuring Rule 5



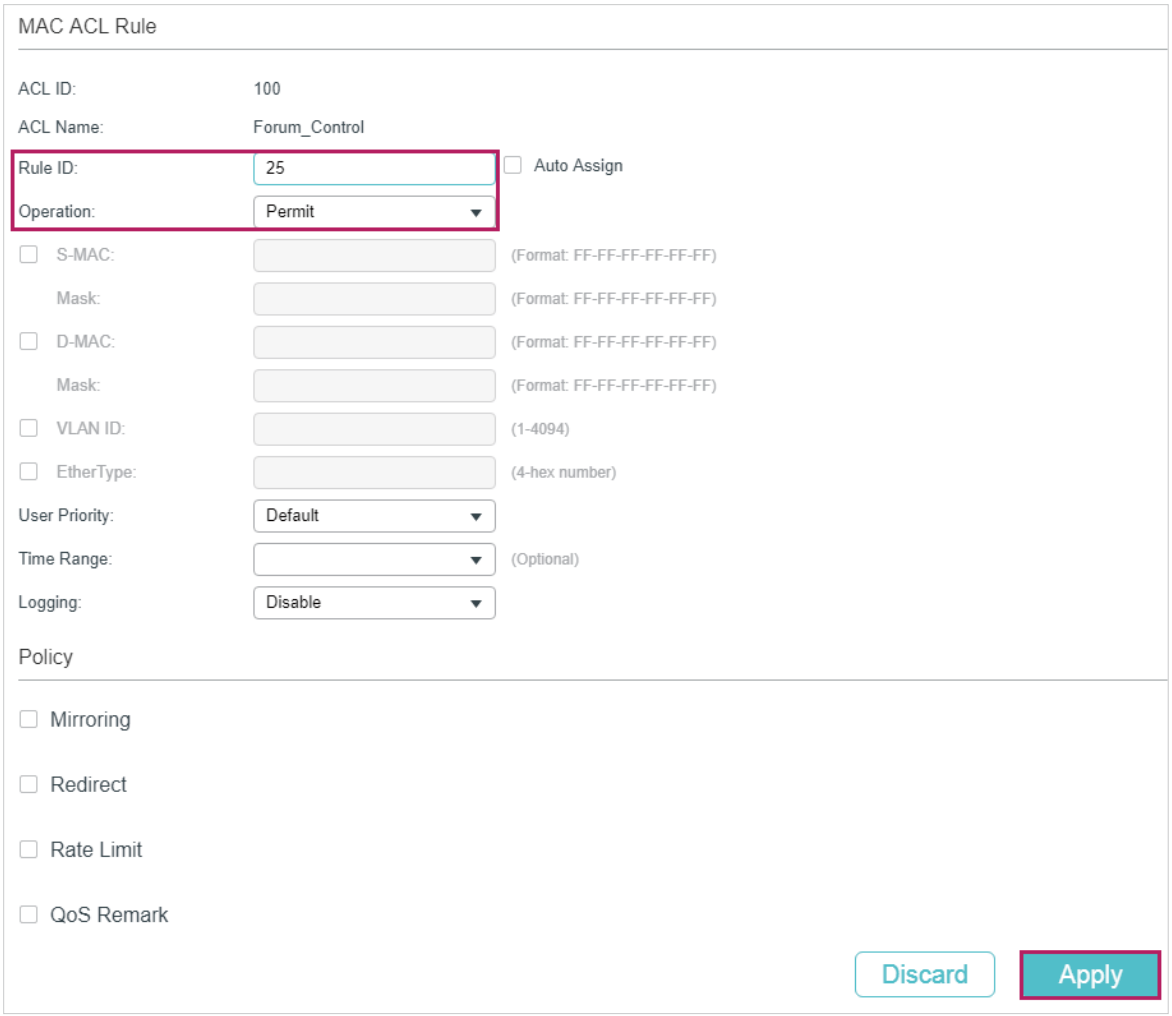
8) In the same way, configure rule 15 to deny packets with destination MAC address 40-61-86-FC-71-56 and apply the time range of work hours.

Figure 3-9 Configuring Rule 15



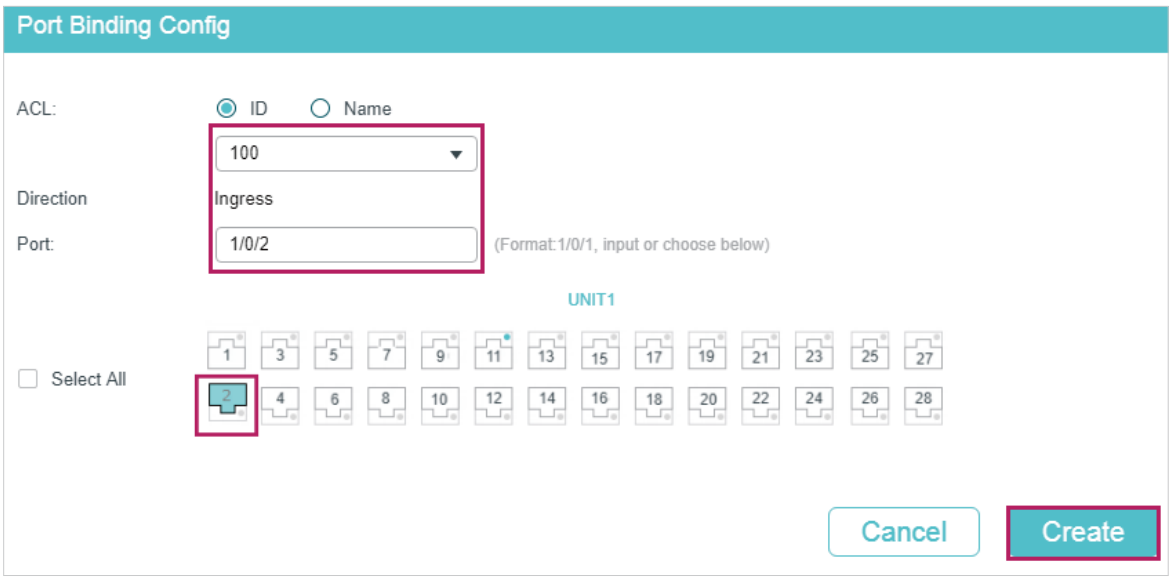
9) Configure rule 25 to permit all the packets that do not match neither of the above rules.

Figure 3-10 Configuring Rule 25



10) Choose the menu **SECURITY > ACL > ACL Binding** and click Add to load the following page. Bind ACL 100 to port 1/0/2 to make it take effect.

Figure 3-11 Binding the ACL to Port 1/0/2



11) Click to save the settings.

3.1.4 Using the CLI

1) Create a time range entry .

   Switch#config

   Switch(config)#time-range Work_time

   Switch(config-time-range)#holiday include

   Switch(config-time-range)#absolute from 01/01/2018 to 01/01/2019

   Switch(config-time-range)#periodic start 08:00 end 18:00 day-of-the-week 1,2,3,4,5

   Switch(config-time-range)#end

   Switch#copy running-config startup-config

2) Create a MAC ACL.

   Switch#configure

   Switch(config)#access-list create 100 name Forum_Control

3) Configure rule 5 to permit packets with source MAC address 8C-DC-D4-40-A1-79 and destination MAC address 40-61-86-FC-71-56.

   Switch(config)#access-list mac 100 rule 5 permit logging disable smac 8C:DC:D4:40:A1:79 smask FF: FF: FF: FF: FF: FF dmac 40:61:86:FC:71:56 dmask FF: FF: FF: FF: FF: FF

4) Configure rule 15 to deny packets with destination MAC address 40-61-86-FC-71-56.

   Switch(config)#access-list mac 100 rule 15 deny logging disable dmac 40:61:86:FC:71:56 dmask FF: FF: FF: FF: FF: FF tseg Work_time

5) Configure rule 25 to permit all the packets. The rule makes sure that the traffic to other network resources will not be blocked by the switch.

   Switch(config)#access-list mac 100 rule 25 permit logging disable

6) Bind ACL100 to port 1/0/2.

   Switch(config)#access-list bind 100 interface gigabitEthernet 1/0/2

   Switch(config)#end

   Switch#copy running-config startup-config

Verify the Configurations

Verify the MAC ACL 100:

Switch#show access-list 100

MAC access list 100 name: “Forum_Control”

rule 5 permit logging disable smac 8c:dc:d4:40:a1:79 smask ff:ff:ff:ff:ff:ff dmac 40:61:86:fc:71:56 dmask ff:ff:ff:ff:ff:ff

rule 15 deny logging disable dmac 40:61:86:fc:71:56 dmask ff:ff:ff:ff:ff:ff tseg “Work_time”

rule 25 permit logging disable

Switch#show access-list bind

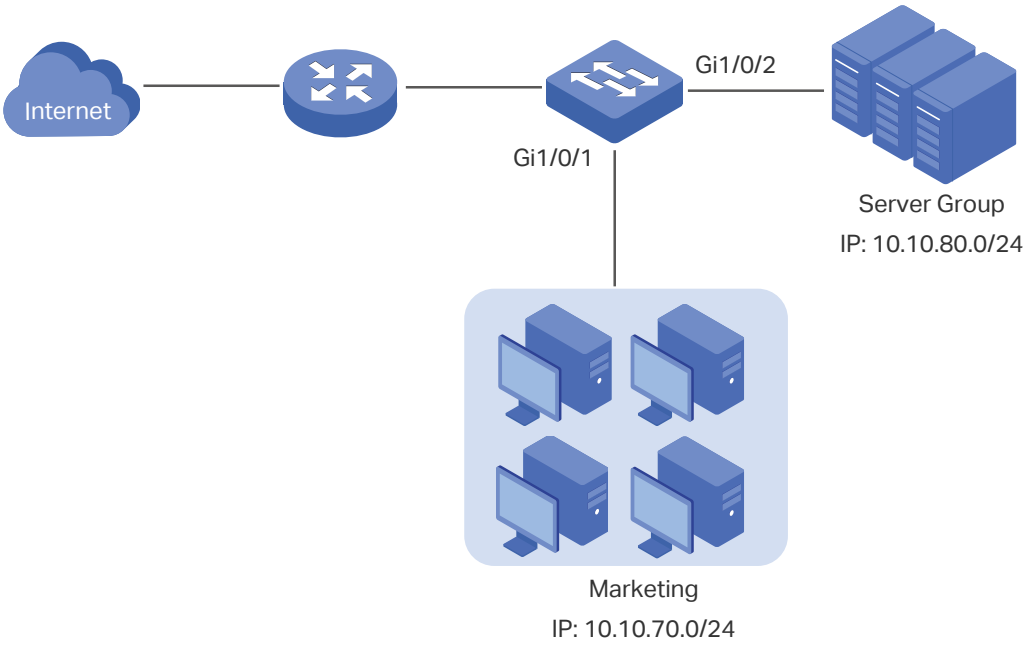
ACL ID	ACL NAME	Interface/VID	Direction	Type
100	Forum_Control	Gi1/0/2	Ingress	Port

3.2 Configuration Example for IP ACL

3.2.1 Network Requirements

As shown below, a company's internal server group can provide different types of services. Computers in the Marketing department are connected to the switch via port 1/0/1, and the internal server group is connected to the switch via port 1/0/2.

Figure 3-12 Network Topology



It is required that:

- The Marketing department can only access internal server group in the intranet.
- The Marketing department can only visit http and https websites on the internet.

3.2.2 Configuration Scheme

To meet the requirements above, you can set up packet filtering by creating an IP ACL and configuring rules for it.

- ACL Configuration

Create an IP ACL and configure the following rules for it:

- Configure a permit rule to match packets with source IP address 10.10.70.0/24, and destination IP address 10.10.80.0/24. This rule allows the Marketing department to access internal network servers from intranet.

- Configure four permit rules to match the packets with source IP address 10.10.70.0/24, and destination ports TCP 80, TCP 443 and TCP/UDP 53. These allow the Marketing department to visit http and https websites on the internet.

The switch matches the packets with the rules in order, starting with Rule 1. If a packet matches a rule, the switch stops the matching process and initiates the action defined in the rule.

- Binding Configuration

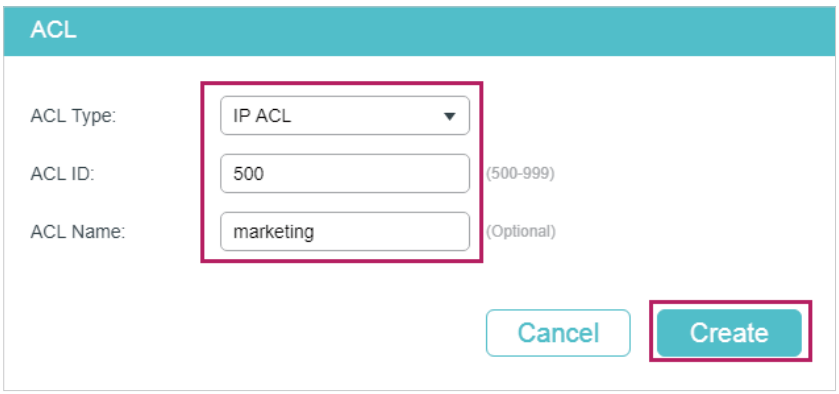
Bind the IP ACL to port 1/0/1 so that the ACL rules will apply to the Marketing department only.

Demonstrated with T1600G-28TS, the following sections explain the configuration procedure in two ways: using the GUI and using the CLI.

3.2.3 Using the GUI

1) Choose the menu **SECURITY > ACL > ACL Config** and click Add to load the following page. Then create an IP ACL for the marketing department.

Figure 3-13 Creating an IP ACL

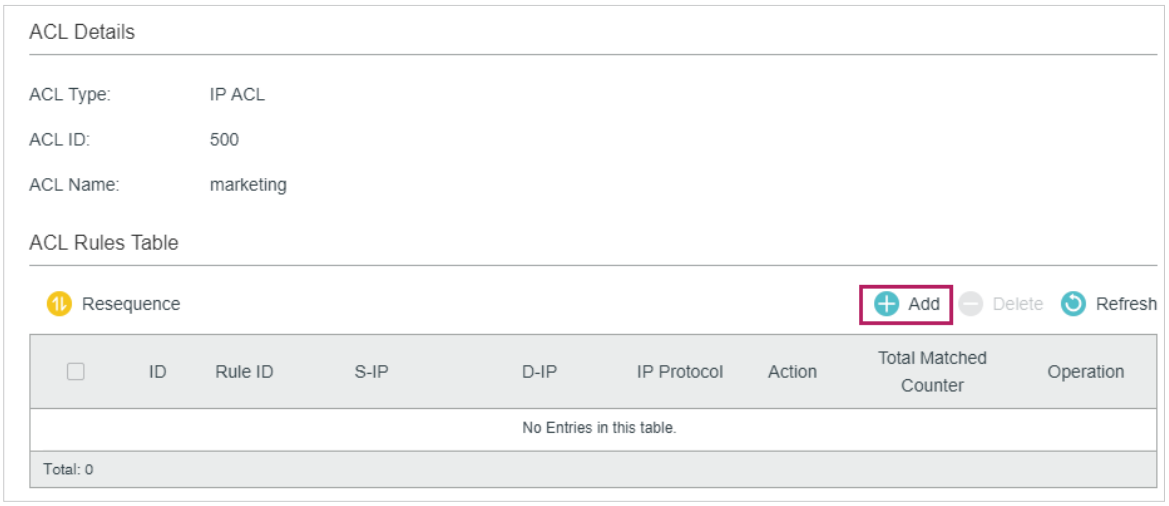


2) Click **Edit ACL** in the Operation column.

Figure 3-14 Editing IP ACL

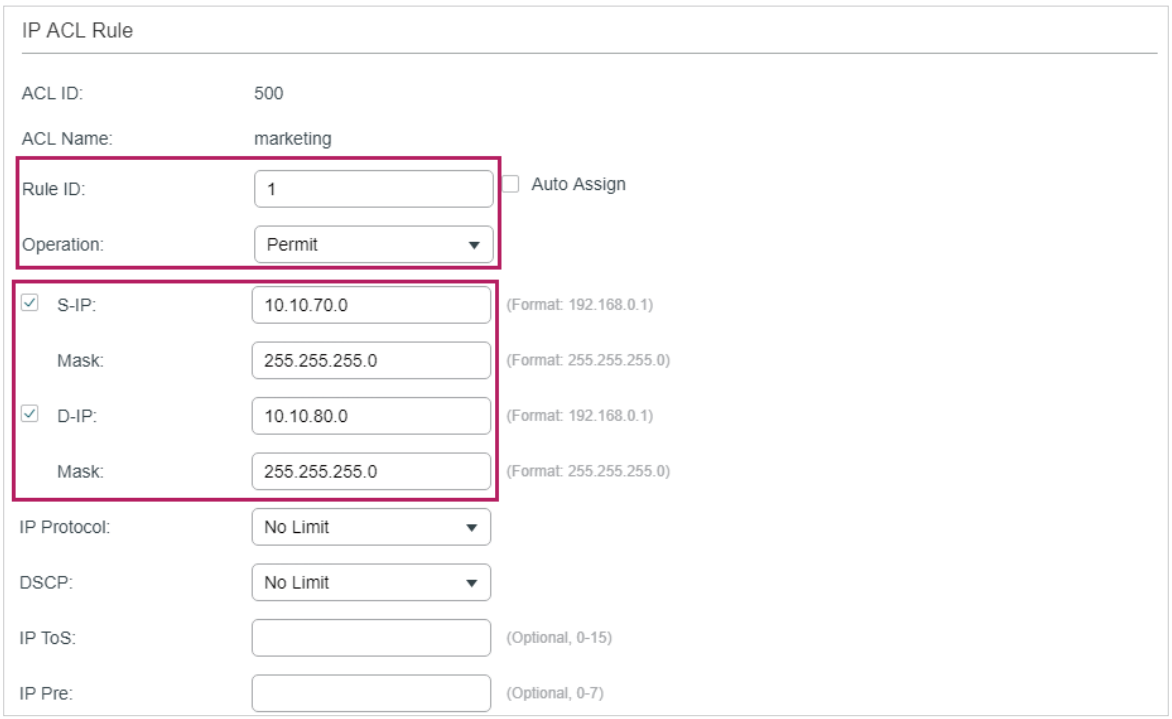
3) On the ACL configuration page, click Add.

Figure 3-15 Editing IP AC



4) Configure rule 1 to permit packets with the source IP address 10.10.70.0/24 and destination IP address 10.10.80.0/24.

Figure 3-16 Configuring Rule 1



5) In the same way, configure rule 2 and rule 3 to permit packets with source IP 10.10.70.0 and destination port TCP 80 (http service port) and TCP 443 (https service port).

Figure 3-17 Configuring Rule 2

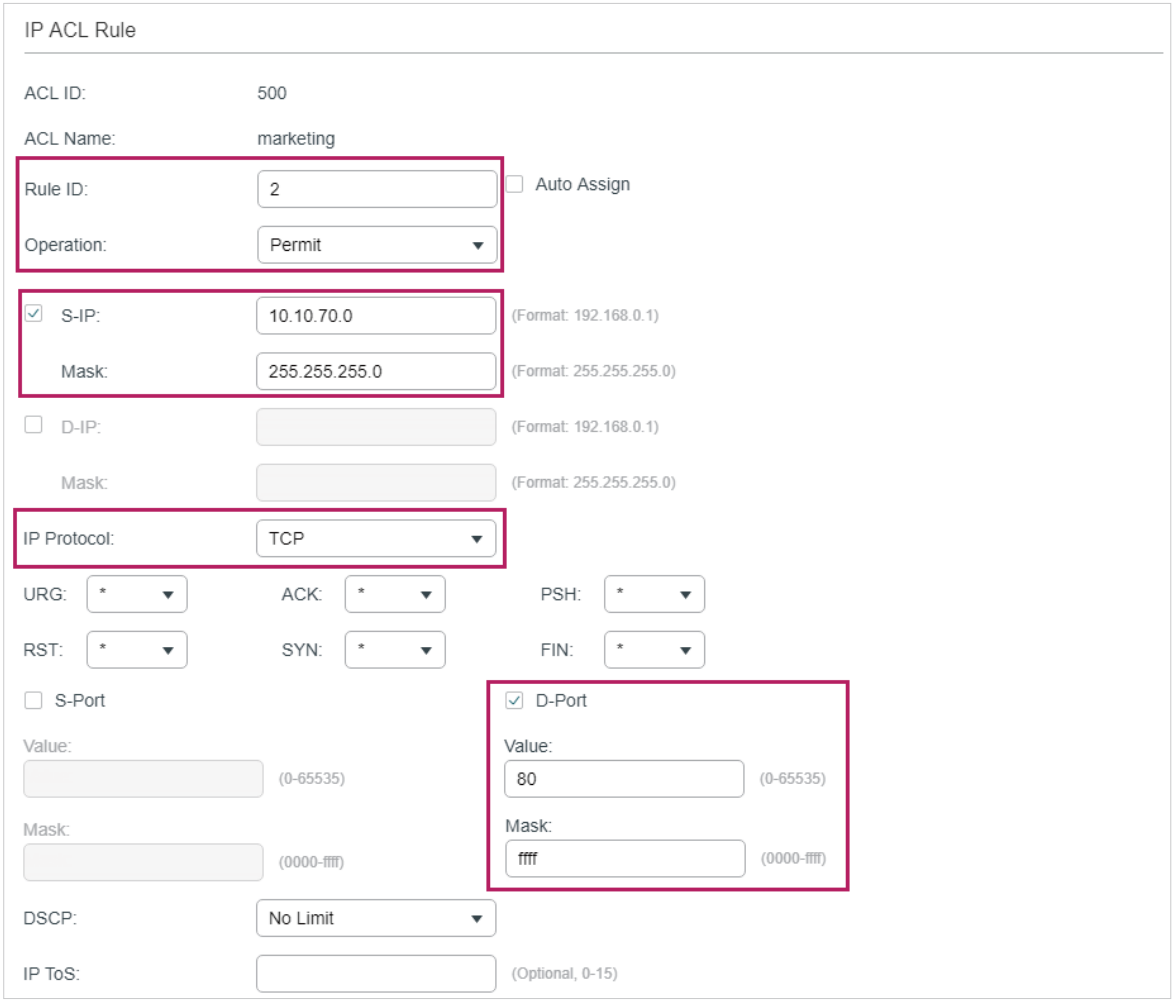
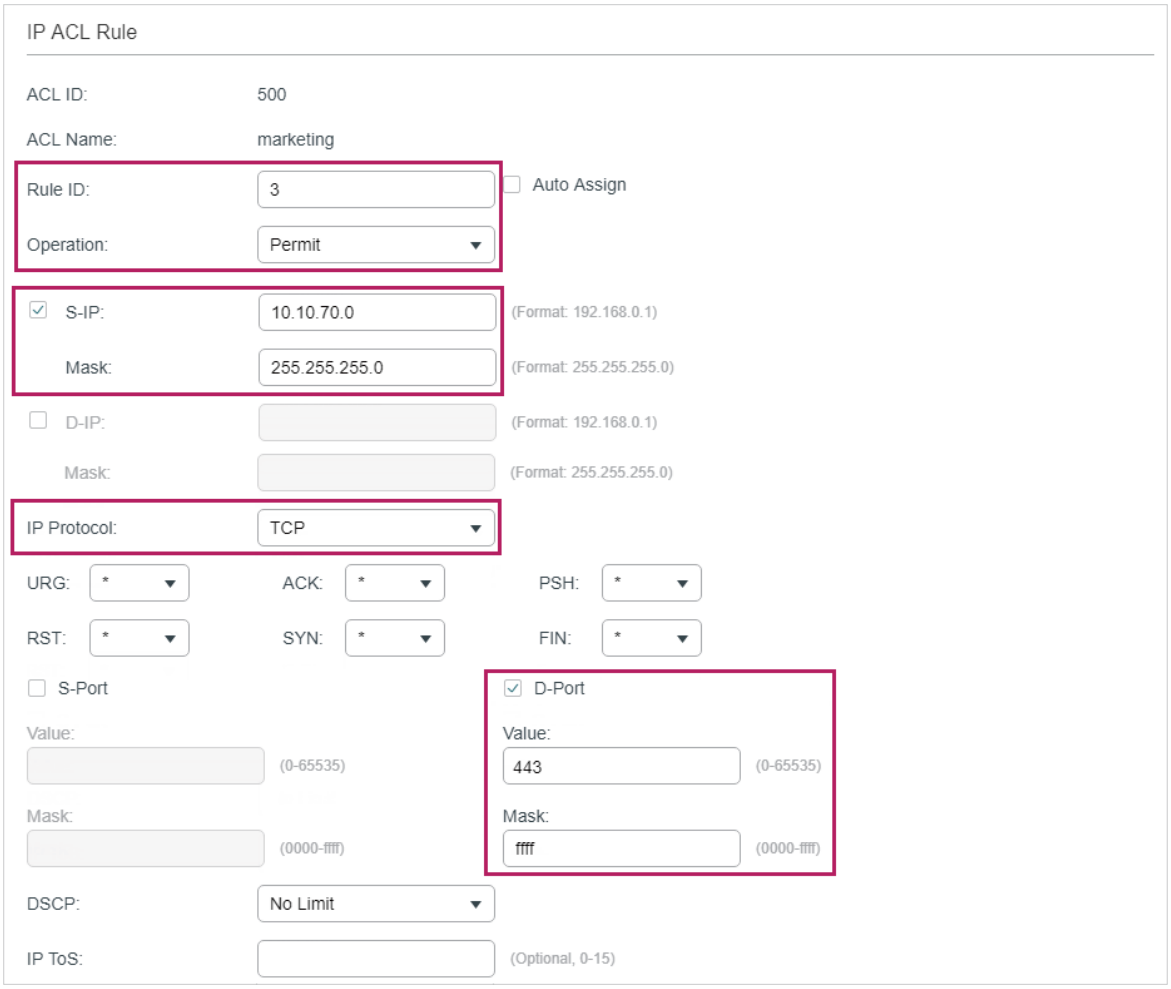


Figure 3-18 Configuring Rule 3



6) In the same way, configure rule 4 and rule 5 to permit packets with source IP 10.10.70.0 and with destination port TCP 53 or UDP 53 (DNS service port).

Figure 3-19 Configuring Rule 4

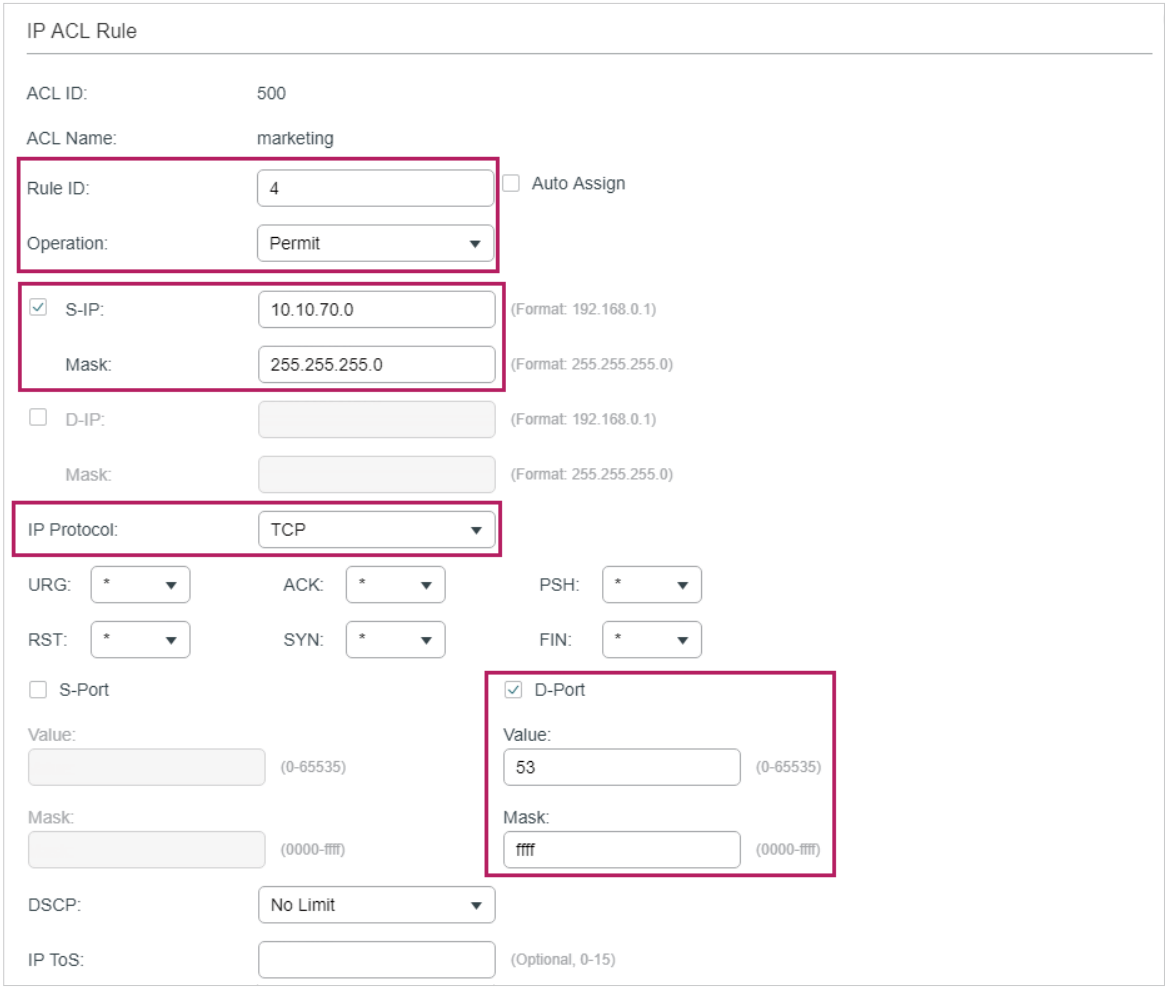
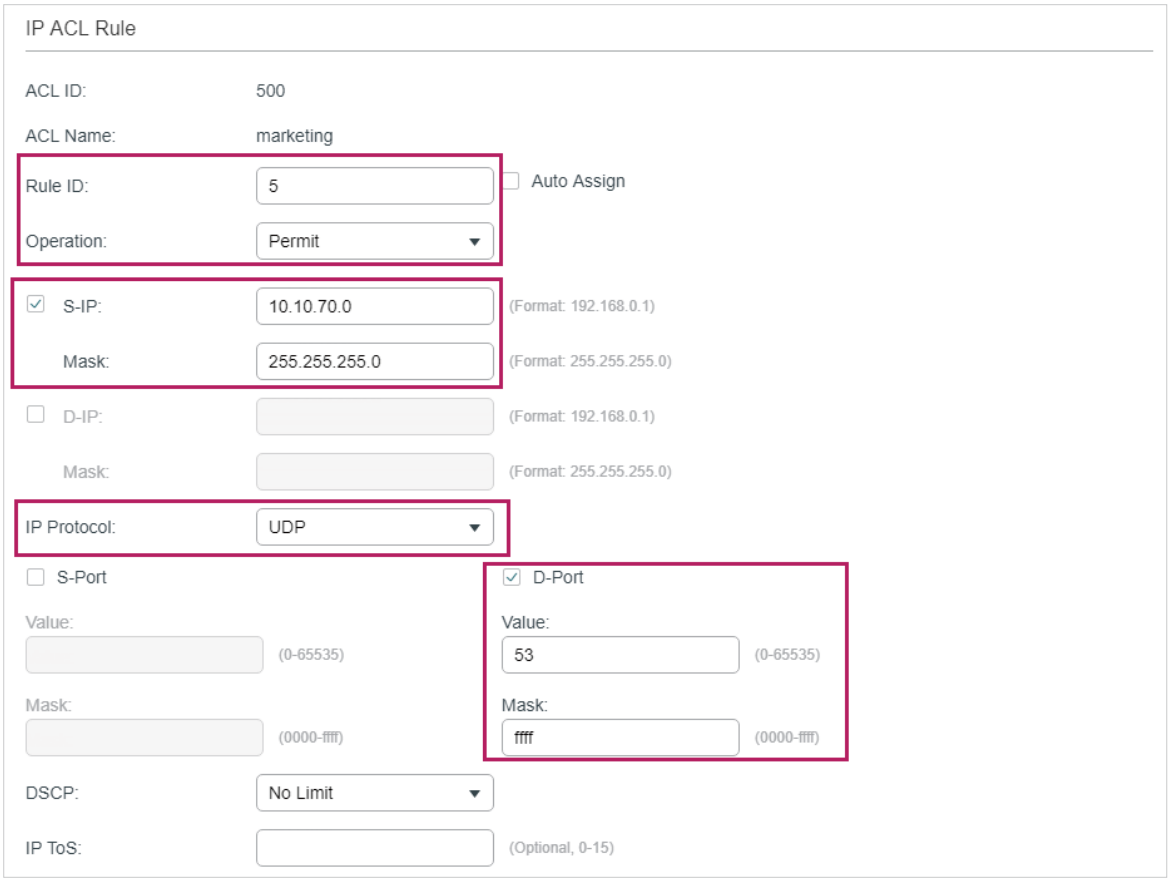
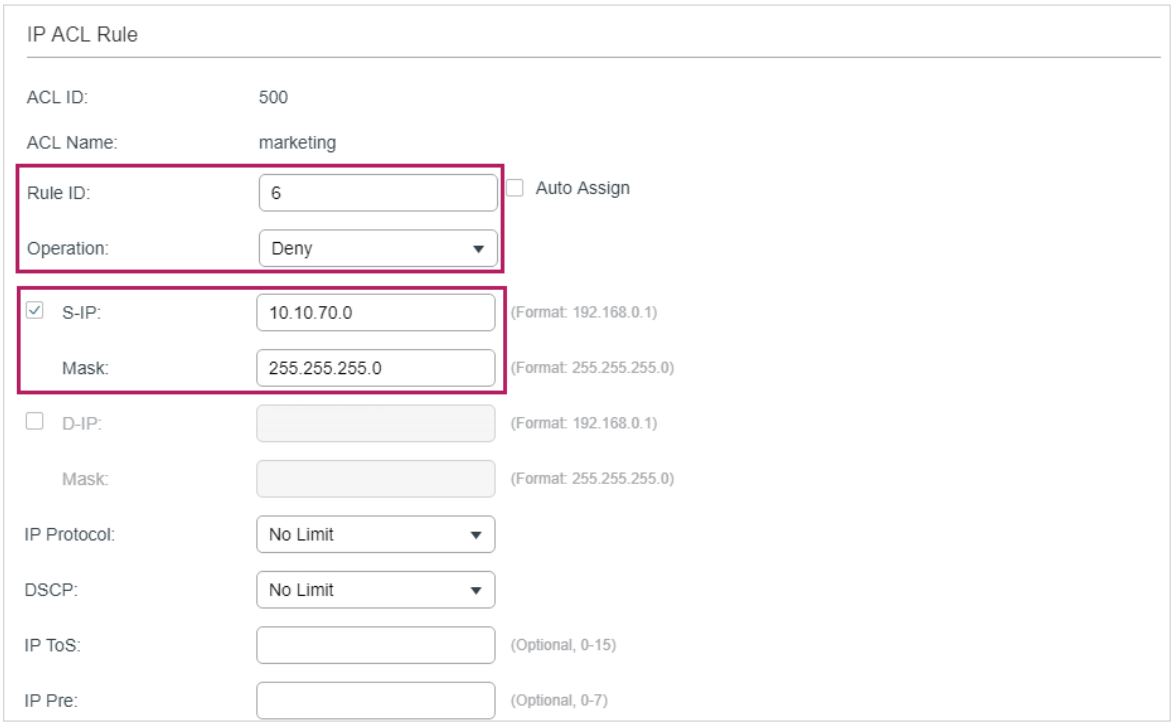


Figure 3-20 Configuring Rule 5



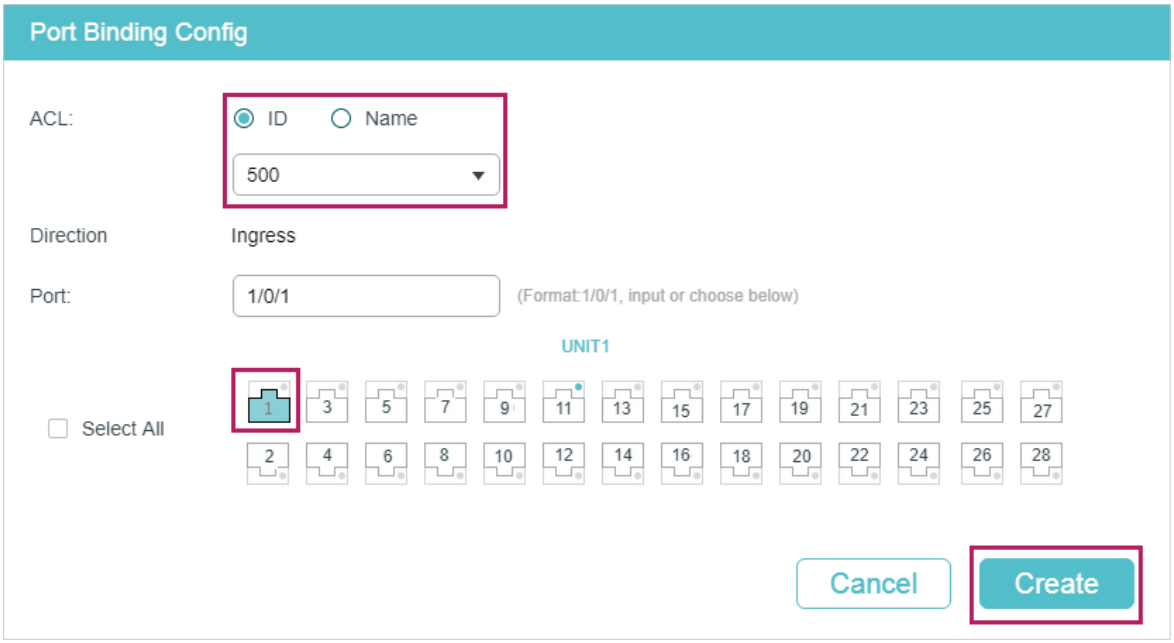
7) In the same way, configure rule 6 to deny packets with source IP 10.10.70.0.

Figure 3-21 Configuring Rule 6



8) Choose the menu **SECURITY > ACL > ACL Binding** and click Add to load the following page. Bind ACL Marketing to port 1/0/1 to make it take effect.

Figure 3-22 Binding the ACL to Port 1/0/1



9) Click Save to save the settings.

3.2.4 Using the CLI

1) Create an IP ACL.

   Switch#configure

   Switch(config)#access-list create 500 name marketing

2) Configure rule 1 to permit packets with source IP 10.10.70.0/24 and destination IP 10.10.80.0/24.

   Switch(config)#access-list ip 500 rule 1 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 dip 10.10.80.0 dmask 255.255.255.0

3) Configure rule 2 and Rule 3 to permit packets with source IP 10.10.70.0/24, and destination port TCP 80 (http service port) or TCP 443 (https service port).

   Switch(config)#access-list ip 500 rule 2 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 protocol 6 d-port 80 d-port-mask ffff

   Switch(config)#access-list ip 500 rule 3 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 protocol 6 d-port 443 d-port-mask ffff

4) Configure rule 4 and rule 5 to permit packets with source IP 10.10.70.0/24, and destination port TCP53 or UDP 53.

   Switch(config)#access-list ip 500 rule 4 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 protocol 6 d-port 53 d-port-mask ffff

   Switch(config)#access-list ip 500 rule 5 permit logging disable sip 10.10.70.0 sip-amask 255.255.255.0 protocol 17 d-port 53 d-port-mask ffff

5) Configure rule 6 to deny packets with source IP 10.10.70.0/24.

Switch(config)#access-list ip 500 rule 2 deny logging disable sip 10.10.70.0 sip-mask 255.255.255.0

6) Bind ACL500 to port 1.

Switch(config)#access-list bind 500 interface gigabitEthernet 1/0/1

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configurations

Verify the IP ACL 500:

Switch#show access-list 500

rule 1 permit logging disable sip 10.10.70.0 smask 255.255.255.0 dip 10.10.80.0 dmask 255.255.255.0

rule 2 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 80

rule 3 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 443

rule 4 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 53

rule 5 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 17 d-port 53

rule 6 deny loggin disable sip 10.10.70.0 smask 255.255.255.0

Switch#show access-list bind

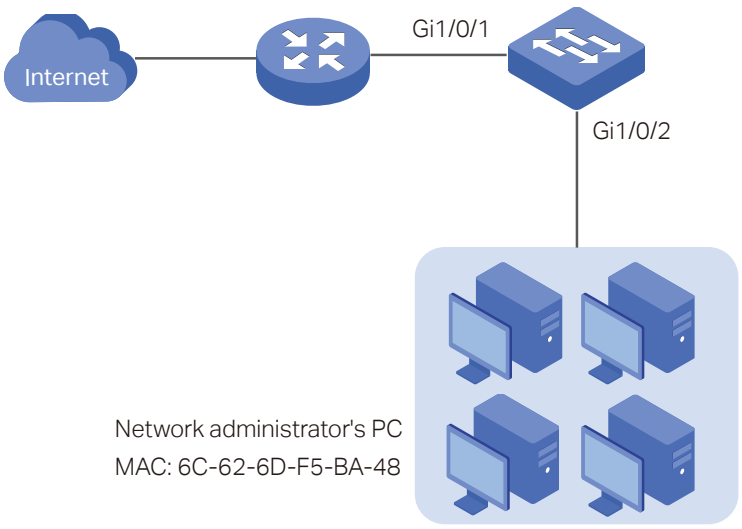
ACL ID	ACL NAME	Interface/VID	Direction	Type
500	marketing	Gi1/0/1	Ingress	Port

3.3 Configuration Example for Combined ACL

3.3.1 Network Requirements

To enhance network security, a company requires that only the network administrator can log in to the switch through Telnet connection. The computers are connected to the switch via port 1/0/2. The network topology is shown as below.

Figure 3-23 Network Topology



3.3.2 Configuration Scheme

To meet the requirements above, you can set up packet filtering by creating a Combined ACL and configuring rules for it.

- ACL Configuration

Create a Combined ACL and configure the following rules for it:

- Configure a permit rule to match packets with source MAC address 6C-62-6D-F5-BA-48, and destination port TCP 23. This rule allows the computer of the network administrator to access the switch through Telnet connection.
- Configure a deny rule to match all the packets except the packets with source MAC address 6C-62-6D-F5-BA-48 and destination port TCP 23. This rule blocks the Telnet connection to the switch of other computers.
- Configure a permit rule to match all the packets. This rule allows that other devices are given the network services except Telnet connection.

The switch matches the packets with the rules in order, starting with Rule 1. If a packet matches a rule, the switch stops the matching process and initiates the action defined in the rule.

- Binding Configuration

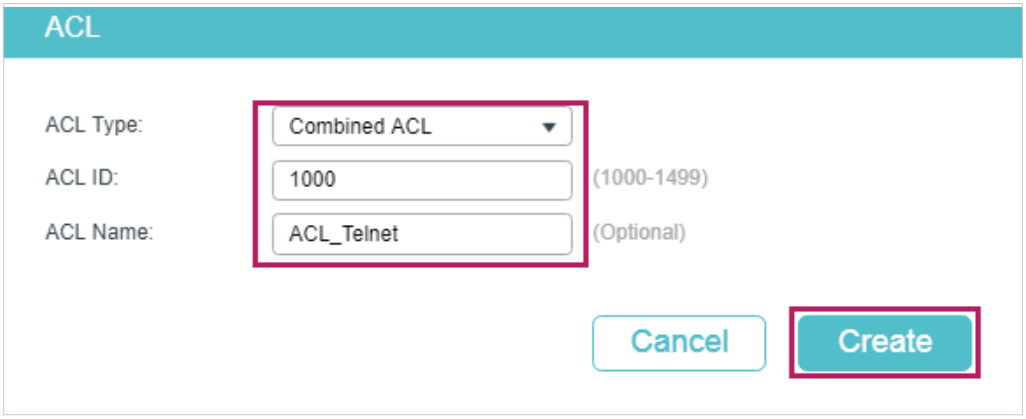
Bind the Combined ACL to port 1/0/2 so that the ACL rules will be applied to the computer of the network administrator and the devices which are restricted to Telnet connection.

Demonstrated with T1600G-28TS, the following sections explain the configuration procedure in two ways: using the GUI and using the CLI.

3.3.3 Using the GUI

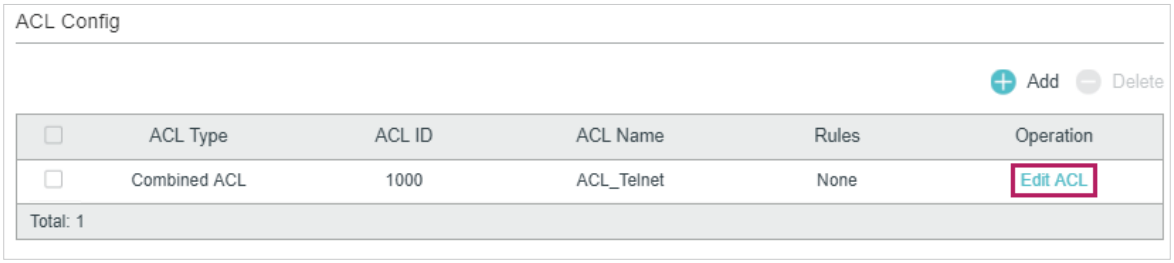
1) Choose the menu **SECURITY > ACL > ACL Config** and click Add to load the following page. Then create a Combined ACL for the marketing department.

Figure 3-24 Creating an Combined ACL



2) Click **Edit ACL** in the Operation column.

Figure 3-25 Editing Combined ACL

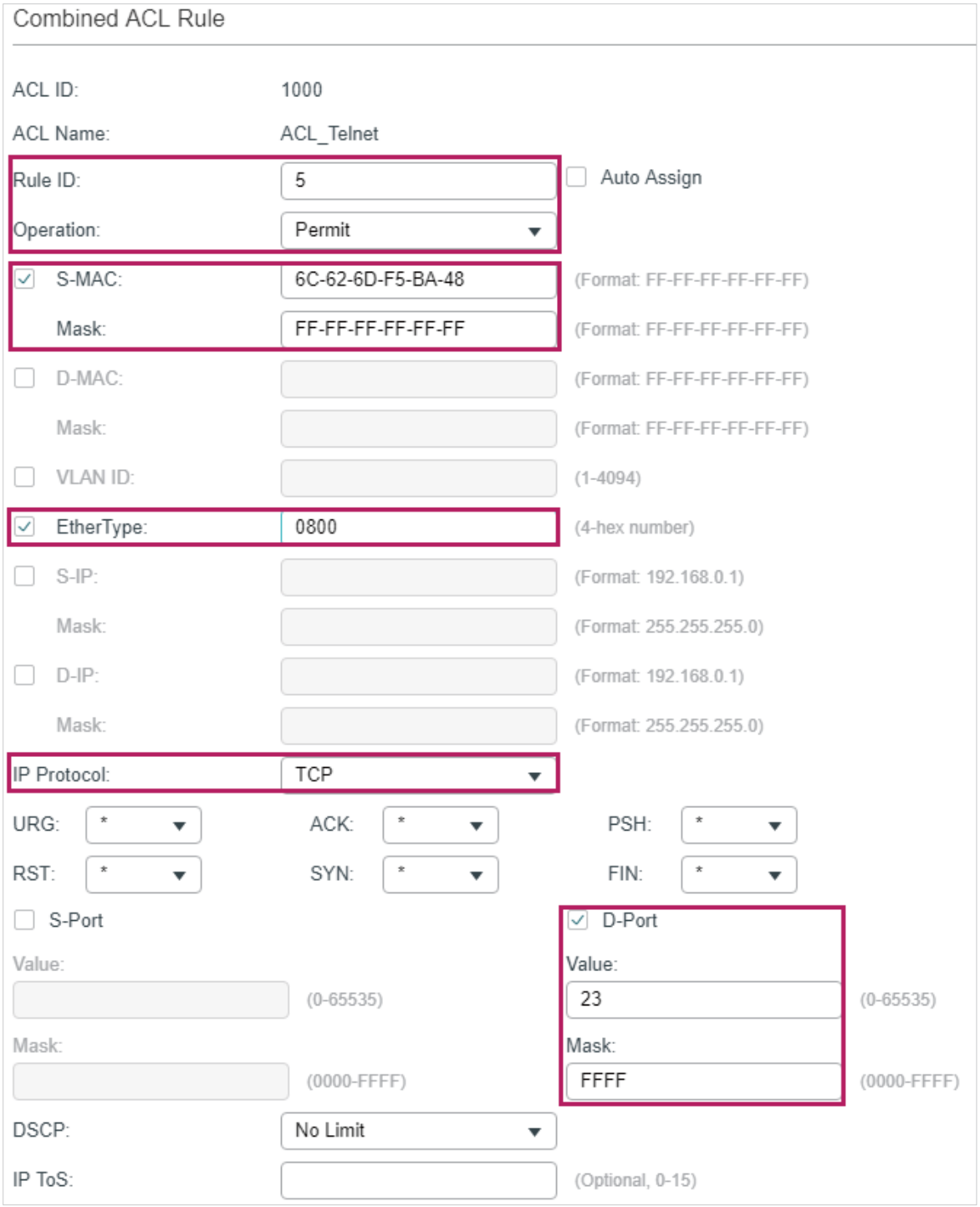


3) On the ACL configuration page, click Add.

Figure 3-26 Editing Combined ACL

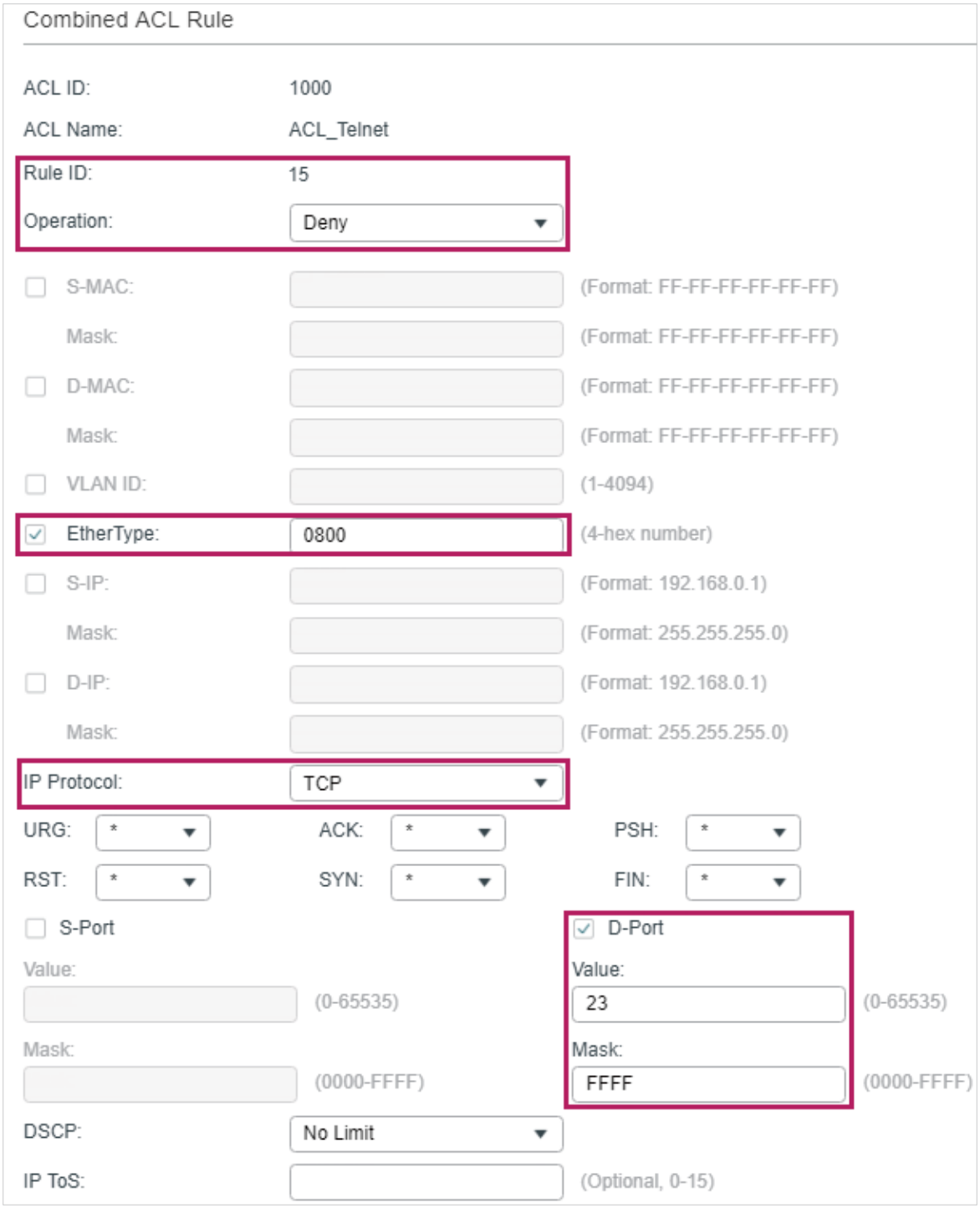
4) Configure rule 5 to permit packets with the source MAC address 6C-62-6D-F5-BA-48 and destination port TCP 23 (Telnet service port).

Figure 3-27 Configuring Rule 5



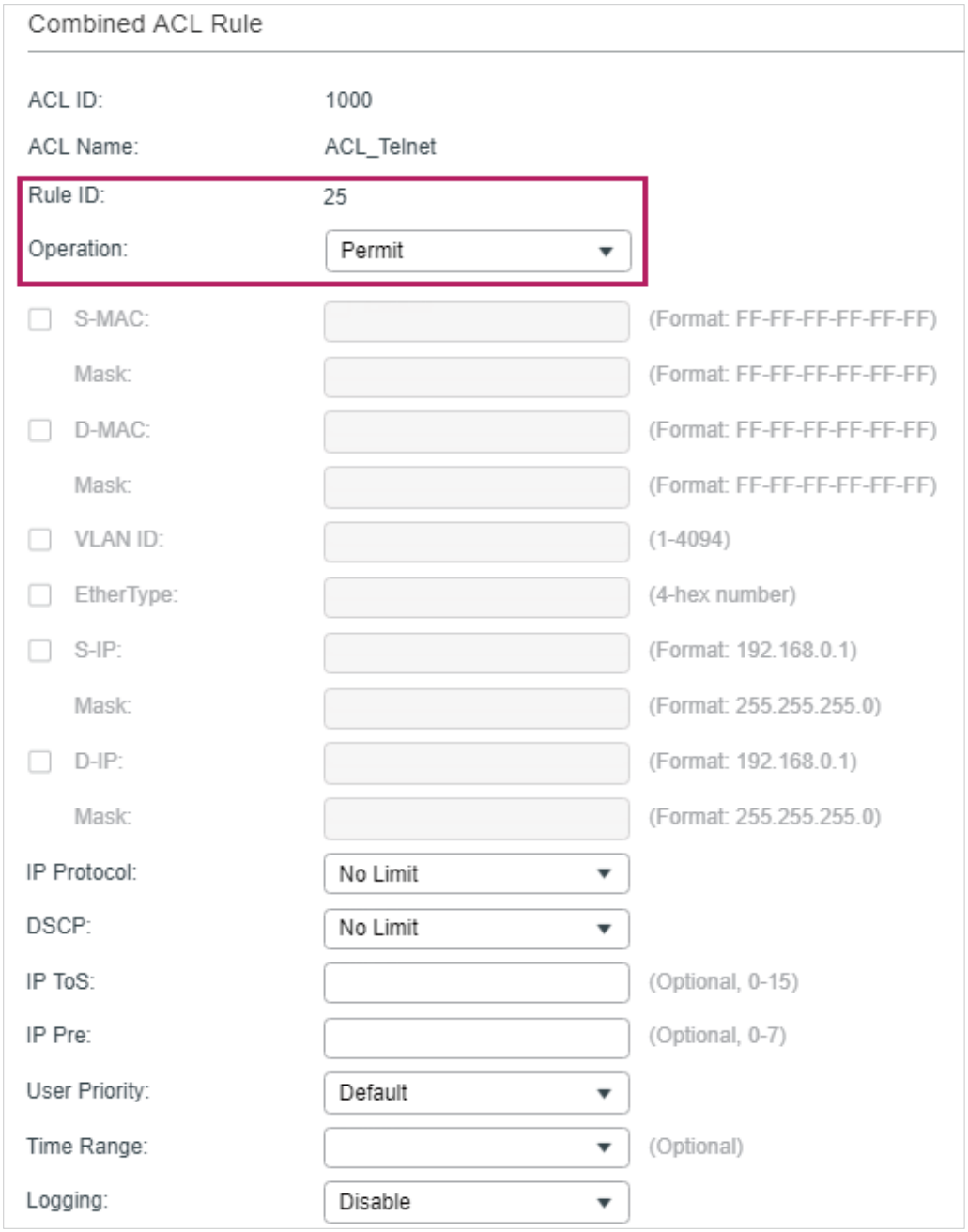
5) Configure rule 15 to deny all the packets except the packet with source MAC address 6C-62-6D-F5-BA-48, and destination port TCP 23 (Telnet service port).

Figure 3-28 Configuring Rule 15



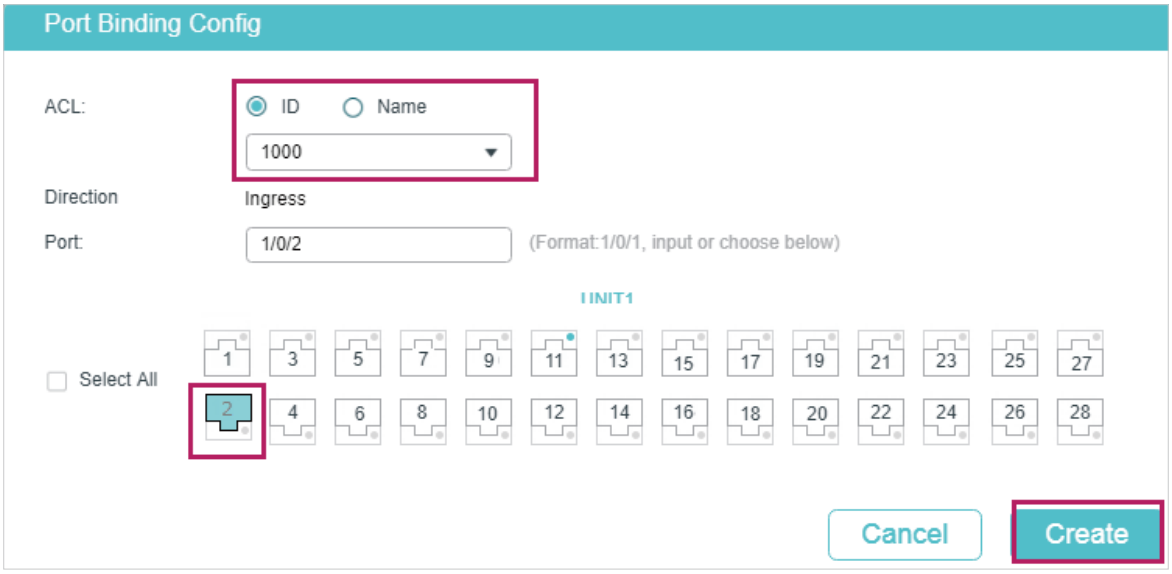
6) In the same way, configure rule 25 to permit all the packets. The rule makes sure that all devices can get other network services normally.

Figure 3-29 Configuring Rule 25



7) Choose the menu **SECURITY > ACL > ACL Binding** and click Add to load the following page. Bind the Policy ACL_Telnet to port 1/0/2 to make it take effect.

Figure 3-30 Binding the ACL to Port 1/0/2



8) Click Save to save the settings.

3.3.4 Using the CLI

1) Create a Combined ACL.

   Switch#configure

   Switch(config)#access-list create 1000 name ACL_Telnet

2) Configure rule 5 to permit packets with the source MAC address 6C-62-6D-F5-BA-48 and destination port TCP 23 (Telnet service port).

   Switch(config)#access-list combined 1000 rule 5 permit logging disable smac 6C:62:6D:F5:BA: 48 smask FF: FF: FF: FF: FF: FF type 0800 protocol 6 d-port 23 d-port-mask FFFF

3) Configure rule 15 to deny all the packets except the packet with source MAC address 6C-62-6D-F5-BA-48, and destination port TCP 23 (Telnet service port).

   Switch(config)#access-list combined 1000 rule 15 deny logging disable type 0800 protocol 6 d-port 23 d-port-mask FFFF

4) Configure rule 25 to permit all the packets. The rule makes sure that all devices can get other network services normally.

   Switch(config)#access-list combined 1000 rule 25 permit logging disable type 0800 protocol 6 d-port 23 d-port-mask FFFF

5) Bind ACL500 to port 1/0/2.

   Switch(config)#access-list bind 500 interface gigabitEthernet 1/0/2

   Switch(config)#end

   Switch#copy running-config startup-config

Verify the Configurations

Verify the Combined ACL 1000:

Switch#show access-list 1000

Combined access list 1000 name: "ACL_Telnet"

rule 5 permit logging disable smac 6c:62:6d:f5:ba:48 smask ff:ff:ff:ff:ff:ff type 0800 protocol 6 d-port 23

rule 15 deny logging disable type 0800 protocol 6 d-port 23

rule 25 permit logging disable

Switch#show access-list bind

ACL ID	ACL NAME	Interface/VID	Direction	Type
1000	ACL_Telnet	Gi1/0/2	Ingress	Port

4 Appendix: Default Parameters

The default settings of ACL are listed in the following tables:

Table 4-1 MAC ACL

Parameter	Default Setting
Operation	Permit
User Priority	No Limit
Time-Range	No Limit

Table 4-2 IP ACL

Parameter	Default Setting
Operation	Permit
IP Protocol	All
DSCP	No Limit
IP ToS	No Limit
IP Pre	No Limit
Time-Range	No Limit

Table 4-3 IPv6 ACL

Parameter	Default Setting
Operation	Permit
Time-Range	No Limit

Table 4-4 Combined ACL

Parameter	Default Setting
Operation	Permit
Time-Range	No Limit

Table 4-5 Policy

Parameter	Default Setting
Mirroring	Disabled
Redirect	Disabled
Rate Limit	Disabled
QoS Remark	Disabled

Part 28

Configuring IPv4 IMPB

CHAPTERS

1. IPv4 IMPB
2. IP-MAC Binding Configuration
3. ARP Detection Configuration
4. IPv4 Source Guard Configuration
5. Configuration Examples
6. Appendix: Default Parameters

1 IPv4 IMPB

1.1 Overview

IPv4 IMPB (IP-MAC-Port Binding) is used to bind the IP address, MAC address, VLAN ID and the connected port number of the specified host. Basing on the binding table, the switch can prevent the ARP cheating attacks with the ARP Detection feature and filter the packets that don't match the binding entries with the IP Source Guard feature.

1.2 Supported Features

IP-MAC Binding

This feature is used to add binding entries. The binding entries can be manually configured, or learned by ARP scanning or DHCP snooping. The features ARP Detection and IPv4 Source Guard are based on the IP-MAC Binding entries.

ARP Detection

In an actual complex network, there are high security risks during ARP implementation procedure. The cheating attacks against ARP, such as imitating gateway, cheating gateway, cheating terminal hosts and ARP flooding attack, frequently occur to the network. ARP Detection can prevent the network from these ARP attacks.

- Prevent ARP Cheating Attacks

Based on the IP-MAC Binding entries, the ARP Detection can be configured to detect the ARP packets and filter the illegal ones so as to prevent the network from ARP cheating attacks.

- Prevent ARP Flooding Attack

You can limit the receiving speed of the legal ARP packets on the port to avoid ARP flooding attack.

IPv4 Source Guard

IPv4 Source Guard is used to filter the IPv4 packets based on the IP-MAC Binding table. Only the packets that match the binding rules are forwarded.

2 IP-MAC Binding Configuration

You can add IP-MAC Binding entries in three ways:

- Manual Binding
- Via ARP Scanning
- Via DHCP Snooping

Additionally, you can view, search and edit the entries in the Binding Table.

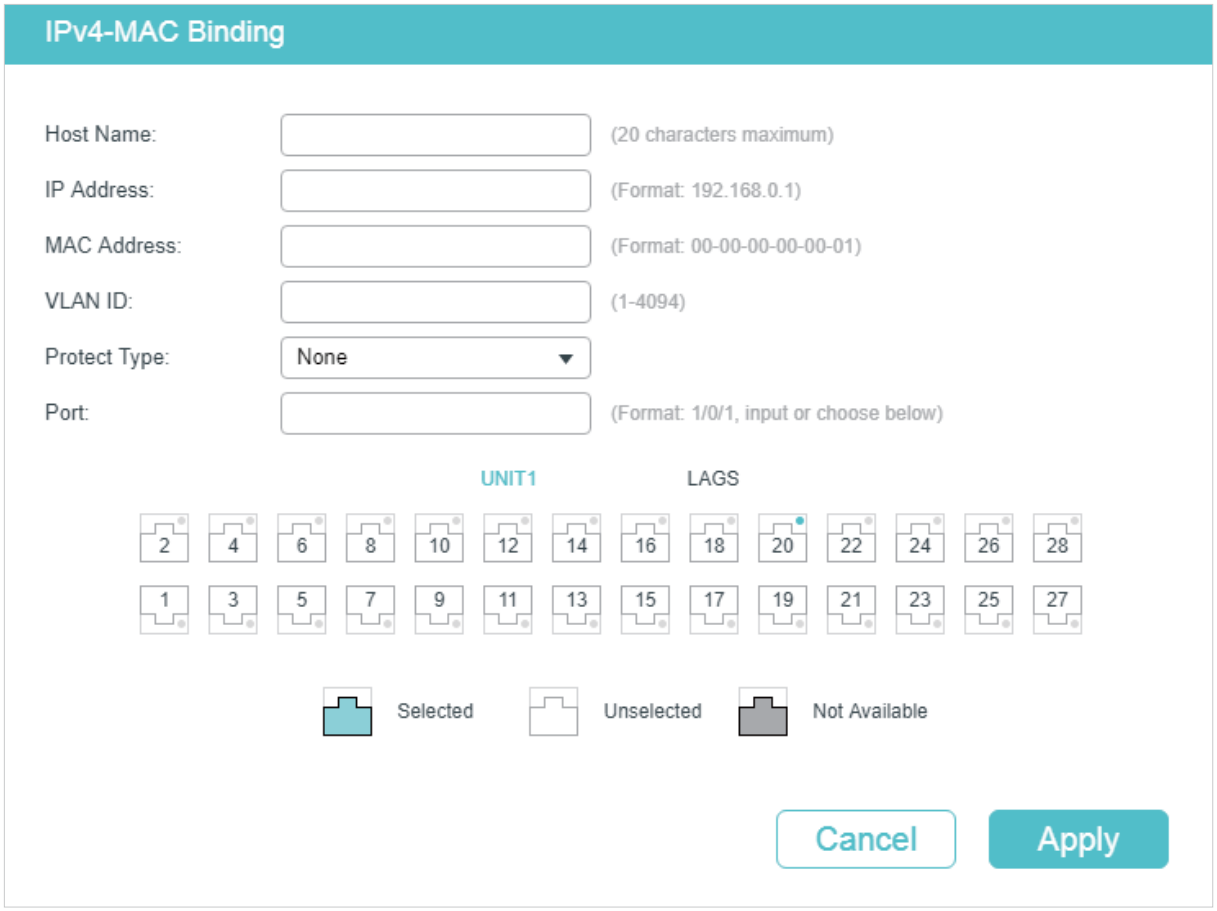
2.1 Using the GUI

2.1.1 Binding Entries Manually

You can manually bind the IP address, MAC address, VLAN ID and the Port number together on the condition that you have got the detailed information of the hosts.

Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Manual Binding** and click Add to load the following page.

Figure 2-1 Manual Binding



Follow these steps to manually create an IP-MAC Binding entry:

1) Enter the following information to specify a host.

Host Name	Enter the host name for identification.
IP Address	Enter the IP address.
MAC Address	Enter the MAC address.
VLAN ID	Enter the VLAN ID.

2) Select protect type for the entry.

Protect Type	Select the protect type for the entry. The entry will be applied to to the specific feature. The following options are provided: **None**: This entry will not be applied to any feature. **ARP Detection**: This entry will be applied to the ARP Detection feature. **IP Source Guard**: This entry will be applied to the IPv4 Source Guard feature. **Both**: This entry will be applied to both of the features.

3) Enter or select the port that is connected to this host.
4) Click **Apply**.

2.1.2 Binding Entries via ARP Scanning

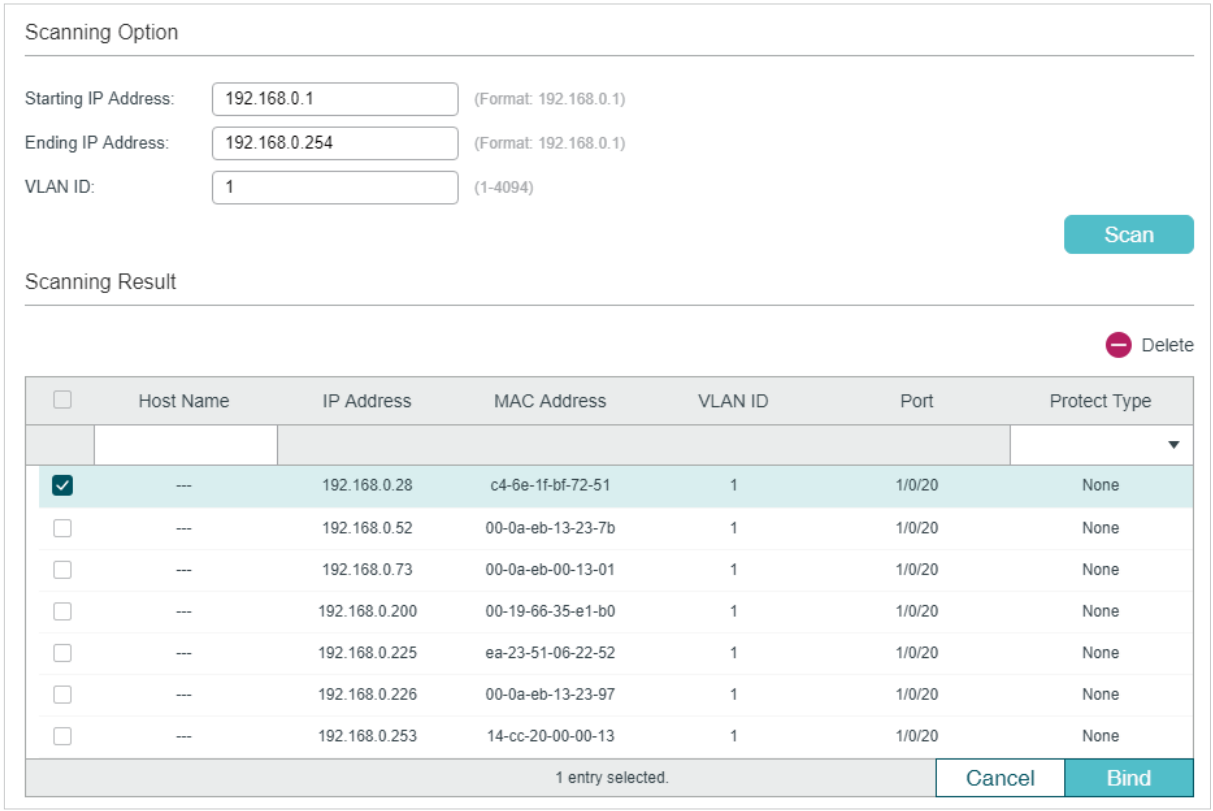
With ARP Scanning, the switch sends the ARP request packets of the specified IP field to the hosts. Upon receiving the ARP reply packet, the switch can get the IP address, MAC address, VLAN ID and the connected port number of the host. You can bind these entries conveniently.

Note:

Before using this feature, make sure that your network is safe and the hosts are not suffering from ARP attacks at present; otherwise, you may obtain incorrect IP-MAC Binding entries. If your network is being attacked, it's recommended to bind the entries manually.

Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > ARP Scanning** to load the following page.

Figure 2-2 ARP Scanning



Follow these steps to configure IP-MAC Binding via ARP scanning:

1) In the **Scanning Option** section, specify an IP address range and a VLAN ID. Then click **Scan** to scan the entries in the specified IP address range and VLAN.

Starting IP Address/Ending IP Address	Specify an IP range by entering a start and end IP address.

VLAN ID	Specify a VLAN ID.

2) In the **Scanning Result** section, select one or more entries and configure the relevant parameters. Then click **Bind**.

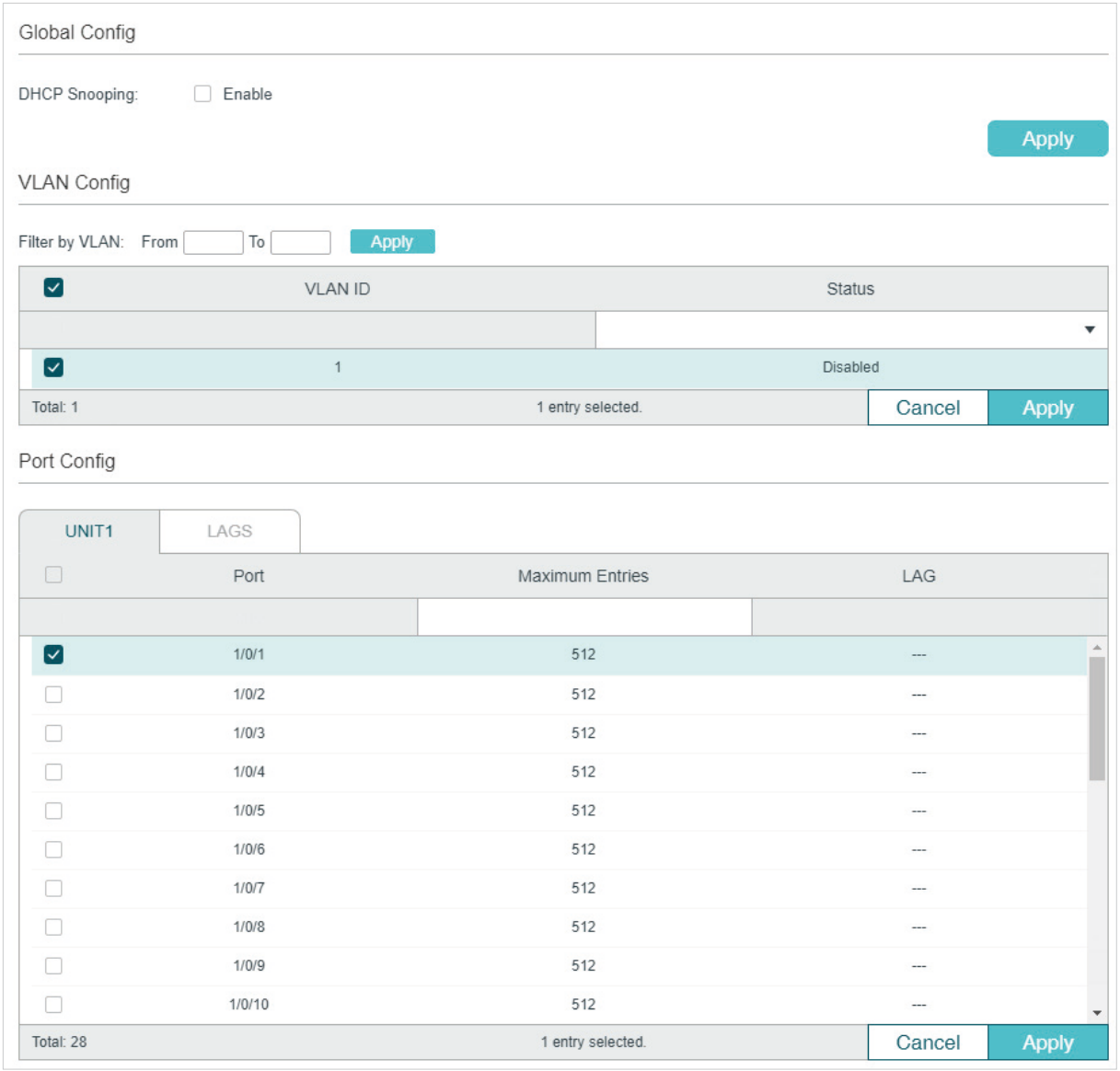
Host Name	Enter a host name for identification.
IP Address	Displays the IP address.
MAC Address	Displays the MAC address.
VLAN ID	Displays the VLAN ID.
Port	Displays the port number.
Protect Type	Select the protect type for the entry. The entry will be applied to to the specific feature. The following options are provided: **None**: This entry will not be applied to any feature. **ARP Detection**: This entry will be applied to the ARP Detection feature. **IP Source Guard**: This entry will be applied to the IP Source Guard feature. **Both** This entry will be applied to both of the features.

2.1.3 Binding Entries via DHCP Snooping

With DHCP Snooping enabled, the switch can monitor the IP address obtaining process of the host, and record the IP address, MAC address, VLAN ID and the connected port number of the host.

Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > DHCP Snooping** to load the following page.

Figure 2-3 DHCP Snooping



Follow these steps to configure IP-MAC Binding via DHCP Snooping:

1) In the **Global Config** section, globally enable DHCP Snooping. Click **Apply**.

2) In the **VLAN Config** section, enable DHCP Snooping on a VLAN or range of VLANs. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable DHCP Snooping on the VLAN.

3) In the **Port Config** section, configure the maximum number of binding entries a port can learn via DHCP snooping. Click **Apply**.

Port	Displays the port number.

Maximum Entries	Configure the maximum number of binding entries a port can learn via DHCP snooping
LAG	Displays the LAG that the port is in.

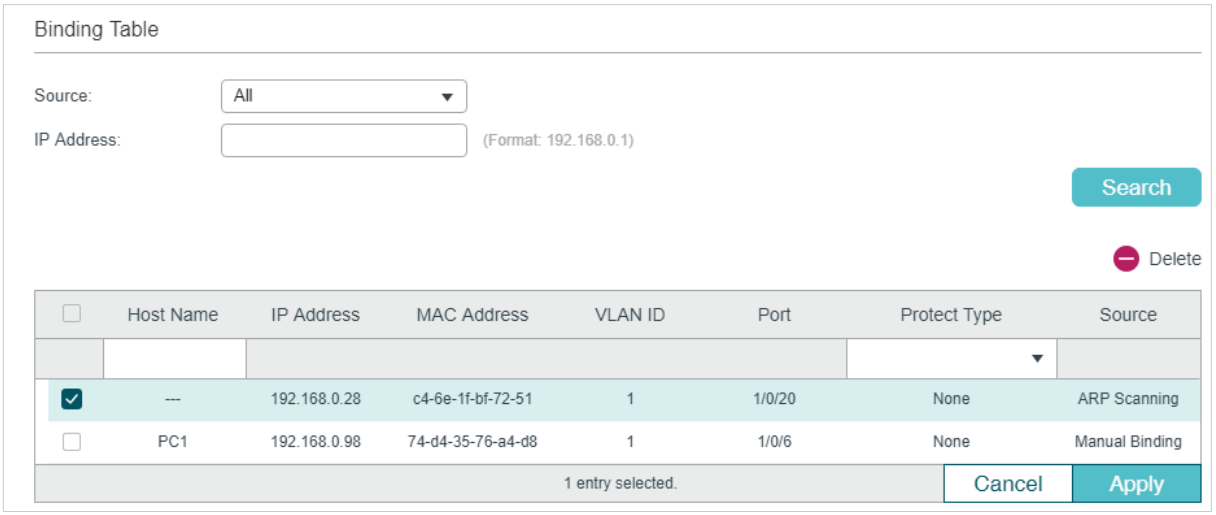
4) The learned entries will be displayed in the Binding Table. You can go to **SECURITY > IPv4 IMPB > IP-MAC Binding > Binding Table** to view or edit the entries.

2.1.4 Viewing the Binding Entries

In the Binding Table, you can view, search and edit the specified binding entries.

Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Binding Table** to load the following page.

Figure 2-4 Binding Table



You can specify the search criteria to search your desired entries.

Source	Select the source of the entry and click **Search**. **All**: Displays the entries from all sources. **Manual Binding**: Displays the manually bound entries. **ARP Scanning**: Displays the binding entries learned from ARP Scanning. **DHCP Snooping**: Displays the binding entries learned from DHCP Snooping.
IP	Enter an IP address and click **Search** to search the specific entry.

Additionally, you select one or more entries to edit the host name and protect type and click **Apply**.

Host Name	Enter a host name for identification.
IP Address	Displays the IP address.
MAC Address	Displays the MAC address.

VLAN ID	Displays the VLAN ID.
Port	Displays the port number.
Protect Type	Select the protect type for the entry. The entry will be applied to to the specific feature. The following options are provided: **None**: This entry will not be applied to any feature. **ARP Detection**: This entry will be applied to the ARP Detection feature. **IP Source Guard**: This entry will be applied to the IP Source Guard feature. **Both**: This entry will be applied to both of the features.
Source	Displays the source of the entry.

2.2 Using the CLI

Binding entries via ARP scanning is not supported by the CLI. The following sections introduce how to bind entries manually and via DHCP Snooping and view the binding entries.

2.2.1 Binding Entries Manually

You can manually bind the IP address, MAC address, VLAN ID and the Port number together on the condition that you have got the detailed information of the hosts.

Follow these steps to manually bind entries:

Step 1	**configure** Enter global configuration mode.

Step 2	**ip source binding** *hostname ip-addr mac-addr* **vlan** *vlan-id* **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **} {** none | arp-detection | ip-verify-source | both **}** Manually bind the host name, IP address, MAC address, VLAN ID and port number of the host, and configure the protect type for the host. *hostname*: Specify a name for the host. It contains 20 characters at most. *ip-addr*: Enter the IP address of the host. *mac-addr*: Enter the MAC address of the host, in the format of xx:xx:xx:xx:xx:xx. *vlan-id*: Enter the VLAN ID of the host. *port*: Enter the number of the port on which the host is connected. none | arp-detection | ip-verify-source | both: Specify the protect type for the entry. None indicates this entry will not be applied to any feature; arp-detection indicates this entry will be applied to ARP Detection; ip-verify-source indicates this entry will be applied to IPv4 Source Guard.
Step 3	**show ip source binding** Verify the binding entry.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind an entry with the hostname host1, IP address 192.168.0.55, MAC address 74:d4:35:76:a4:d8, VLAN ID 10, port number 1/0/5, and enable this entry for the ARP detection feature.

Switch#configure

Switch(config)#ip source binding host1 192.168.0.55 74:d4:35:76:a4:d8 **vlan** 10 **interface gigabitEthernet** 1/0/5 arp-detection

Switch(config)#show ip source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	host1	192.168.0.55	74:d4:35:76:a4:d8	10	Gi1/0/5	ARP-D	Manual

Notice:

1.Here, 'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Binding Entries via DHCP Snooping

Follow these steps to bind entries via DHCP Snooping:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp snooping** Globally enable DHCP Snooping.
Step 3	**ip dhcp snooping vlan** *vlan-range* Enable DHCP Snooping on the specified VLAN. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 5	**ip dhcp snooping max-entries** *value* Configure the maximum number of binding entries the port can learn via DHCP snooping. *value:* Enter the value of maximum number of entries. The valid values are from 0 to 512.
Step 6	**show ip dhcp snooping** Verify global configuration of DHCP Snooping.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Snooping globally and on VLAN 5, and set the maximum number of binding entries port 1/0/1 can learn via DHCP snooping as 100:

Switch#configure

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 5

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip dhcp snooping max-entries 100

Switch(config-if)#show ip dhcp snooping

Global Status: Enable

VLAN ID: 5

Switch(config-if)#show ip dhcp snooping interface gigabitEthernet 1/0/1

Interface max-entries LAG

--- --- ---

Gi1/0/1 100 N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Viewing Binding Entries

On privileged EXEC mode or any other configuration mode, you can use the following command to view binding entries:

show ip source binding

View the information of binding entries, including the host name, IP address, MAC address, VLAN ID, port number and protect type.

3 ARP Detection Configuration

To complete ARP Detection configuration, follow these steps:

1) Add IP-MAC Binding entries.
2) Enable ARP Detection.
3) Configure ARP Detection on ports.
4) View ARP statistics.

3.1 Using the GUI

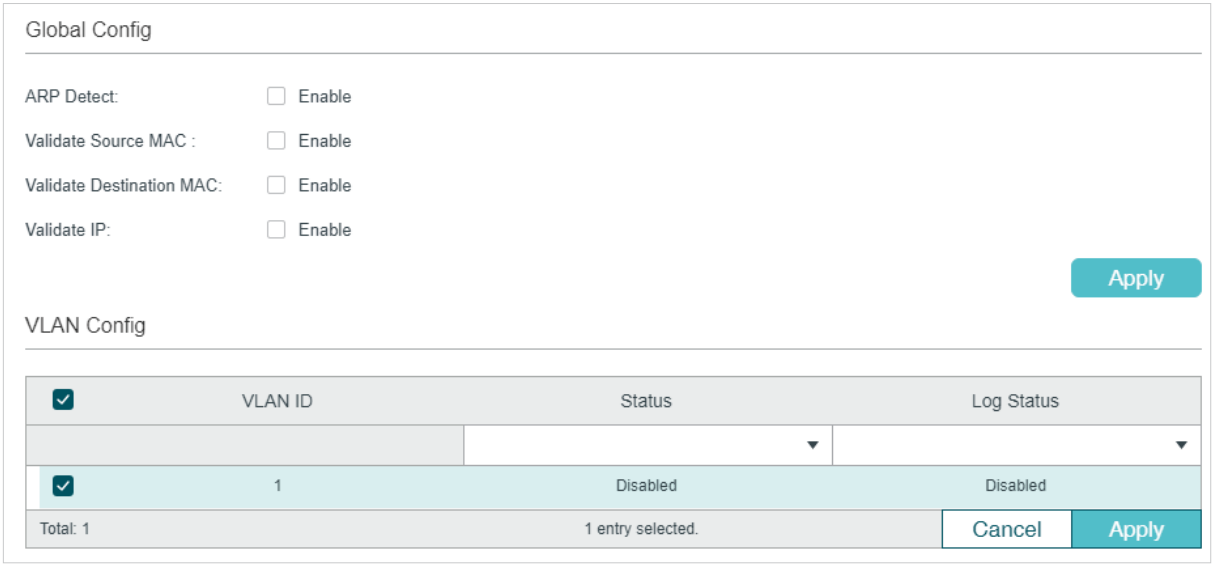
3.1.1 Adding IP-MAC Binding Entries

In ARP Detection, the switch detects the ARP packets based on the binding entries in the IP-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration. For details, refer to IP-MAC Binding Configuration.

3.1.2 Enabling ARP Detection

Choose the menu **SECURITY > IPv4 IMPB > ARP Detection > Global Config** to load the following page.

Figure 3-1 ARP Detection Global Config



Follow these steps to enable ARP Detection:

1) In the **Global Config** section, enable ARP Detection and configure the related parameters. Click **Apply**.

ARP Detect	Enable or disable ARP Detection globally.
Validate Source MAC	Enable or disable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded.
Validate Destination MAC	Enable or disable the switch to check whether the destination MAC address and the target MAC address are the same when receiving an ARP reply packet. If not, the ARP packet will be discarded.
Validate IP	Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal ARP packets will be discarded, including broadcast addresses, multicast addresses, Class E addresses, loopback addresses (127.0.0.0/8) and the following address: 0.0.0.0.

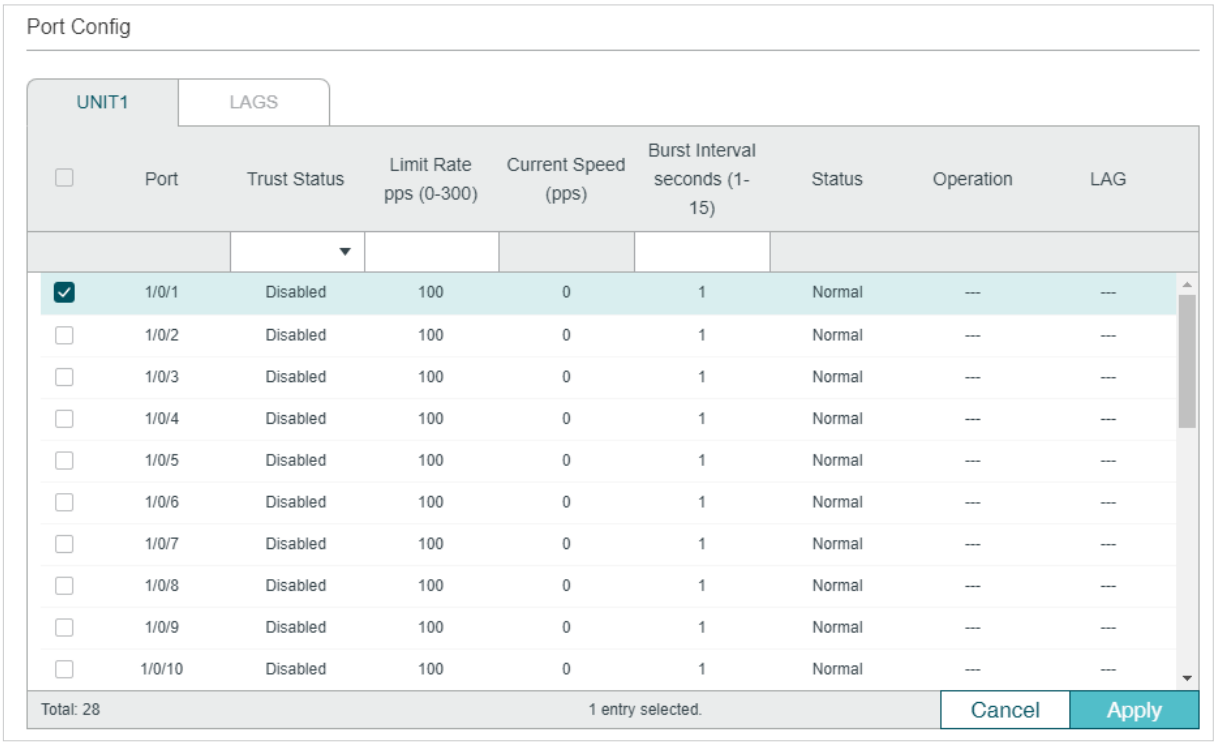
2) In the **VLAN Config** section, enable ARP Detection on the selected VLANs. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable ARP Detection on the VLAN.
Log Status	Enable or disable Log feature on the VLAN. With this feature enabled, the switch generates a log when an illegal ARP packet is discarded.

3.1.3 Configuring ARP Detection on Ports

Choose the menu **SECURITY > IPv4 IMPB > ARP Detection >Port Config** to load the following page.

Figure 3-2 ARP Detection on Port



Follow these steps to configure ARP Detection on ports:

1) Select one or more ports and configure the parameters.

Trust Status	Enable or disable this port to be a trusted port. On a trusted port, the ARP packets are forwarded directly without checked. The specific ports, such as up-link ports and routing ports are suggested to be set as trusted.
Limit Rate	Specify the maximum number of the ARP packets that can be received on the port per second.
Current Speed	Displays the current speed of receiving the ARP packets on the port.
Burst Interval	Specify a time range. If the speed of received ARP packets reaches the limit for this time range, the port will be shut down.
Status	Displays the status of the ARP attack: **Normal**: The forwarding of ARP packets on the port is normal. **Down:** The transmission speed of the legal ARP packet exceeds the defined value. The port will be shut down for 300 seconds. You can also click the Recovery button to recover
Operation	If Status is changed to Down, there will be a **Recover** button. You can click the button to restore the port to the normal status.
LAG	Displays the LAG that the port is in.

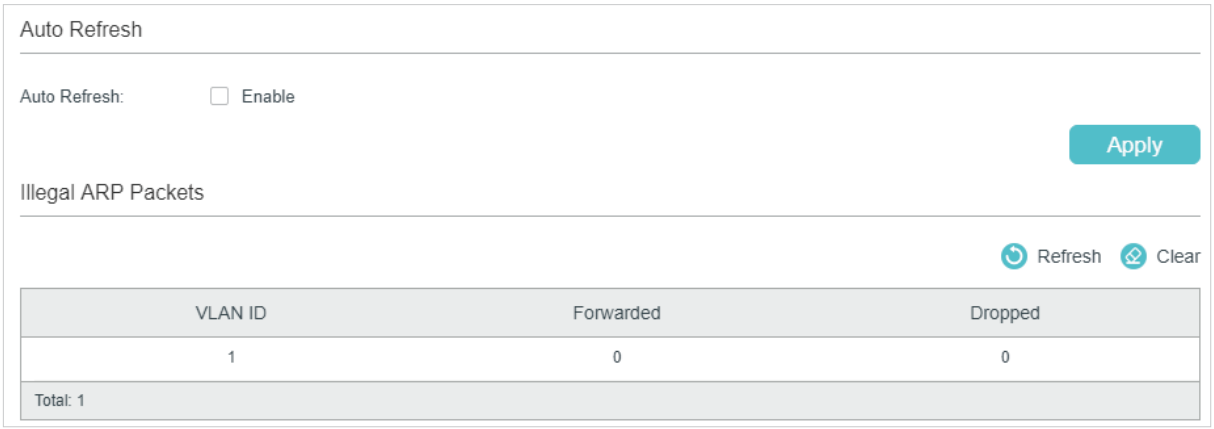
2) Click **Apply**.

3.1.4 Viewing ARP Statistics

You can view the number of the illegal ARP packets received on each port, which facilitates you to locate the network malfunction and take the related protection measures.

Choose the menu **SECURITY > IPv4 IMPB > ARP Detection > ARP Statistics** to load the following page.

Figure 3-3 View ARP Statistics



In the **Auto Refresh** section, you can enable the auto refresh feature and specify the refresh interval, and thus the web page will be automatically refreshed.

In the **Illegal ARP Packet** section, you can view the number of illegal ARP packets in each VLAN.

VLAN ID	Displays the VLAN ID.
Forwarded	Displays the number of forwarded ARP packets in this VLAN.
Dropped	Displays the number of dropped ARP packets in this VLAN.

3.2 Using the CLI

3.2.1 Adding IP-MAC Binding Entries

In ARP Detection, the switch detects the ARP packets based on the binding entries in the IP-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration. For details, refer to IP-MAC Binding Configuration.

3.2.2 Enabling ARP Detection

Follow these steps to enable ARP Detection:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip arp inspection** Globally enable the ARP Detection feature.
Step 3	**ip arp inspection validate {** src-mac | dst-mac | ip **}** Configure the switch to check the IP address or MAC address of the received packets. src-mac: Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded. dst-mac: Enable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded. ip: Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal ARP packets will be discarded, including broadcast addresses, multicast addresses, Class E addresses, loopback addresses (127.0.0.0/8) and the following address: 0.0.0.0.
Step 4	**ip arp inspection vlan** *vlan-list* Enable ARP Detection on one or more 802.1Q VLANs that already exist. *vlan-list*: Enter the VLAN ID. The format is 1,5-9.

Step 5	**ip arp inspection vlan** *vlan-list* **logging** (Optional) Enable the Log feature to make the switch generate a log when an ARP packet is discarded. *vlan-list*: Enter the VLAN ID. The format is 1,5-9.
Step 6	**show ip arp inspection** Verify the ARP Detection configuration.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable ARP Detection globally and on VLAN 2, and enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet:

Switch#configure

Switch(config)#ip arp inspection

Switch(config)#ip arp inspection validate src-mac

Switch(config)#ip arp inspection vlan 2

Switch(config)#show ip arp inspection

Global Status: Enable

Verify SMAC: Enable

Verify DMAC: Disable

Verify IP: Disable

Switch(config)#show ip arp inspection vlan

VID	Enable status	Log Status
----	----------	----------
1	Disable	Disable
2	Enable	Disable

Switch(config)#end

Switch#copy running-config startup-config

3.2.3 Configuring ARP Detection on Ports

Follow these steps to configure ARP Detection on ports:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ip arp inspection trust** Configure the port as a trusted port, on which the ARP Detection function will not take effect. The specific ports, such as up-linked ports and routing ports are suggested to be set as trusted ports.
Step 4	**ip arp inspection limit-rate** *value* Specify the maximum number of the ARP packets can be received on the port per second. *value:* Specify the limit rate value. The valid values are from 0 to 300 pps (packets/second), and the default value is 100.
Step 5	**ip arp inspection burst-interval** *value* Specify a time range. If the speed of received ARP packets reaches the limit for this time range, the port will be shut down. *value:* Specify the time range. The valid values are from 1 to 15 seconds, and the default value is 1 second.
Step 6	**show ip arp inspection interface** View the configurations and status of the ports.
Step 7	**show ip arp inspection vlan** View the configurations and status of the VLANs.
Step 8	**ip arp inspection recover** (Optional) For ports on which the speed of receiving ARP packets has exceeded the limit, use this command to restore the port from Down status to Normal status.
Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set port 1/02 as a trusted port, and set limit-rate as 20 pps and burst interval as 2 seconds on port 1/0/2:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ip arp inspection trust

Switch(config-if)#ip arp inspection limit-rate 20

Switch(config-if)#ip arp inspection burst-interval 2

Switch(config-if)#show ip arp inspection interface gigabitEthernet 1/0/2

Interface	Trust state	limit Rate(pps)	Current speed(pps)	Burst Interval	Status	LAG
---	---	---	---	---	---	---
Gi1/0/2	Enable	20	0	2	---	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

The following example shows how to restore the port 1/0/1 that is in Down status to Normal status:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip arp inspection recover

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.4 Viewing ARP Statistics

On privileged EXEC mode or any other configuration mode, you can use the following command to view ARP statistics:

show ip arp inspection statistics

View the ARP statistics on each port, including the number of forwarded ARP packets and the number of dropped ARP packets.

4 IPv4 Source Guard Configuration

To complete IPv4 Source Guard configuration, follow these steps:

1) Add IP-MAC Binding entries.
2) Configure IPv4 Source Guard.

4.1 Using the GUI

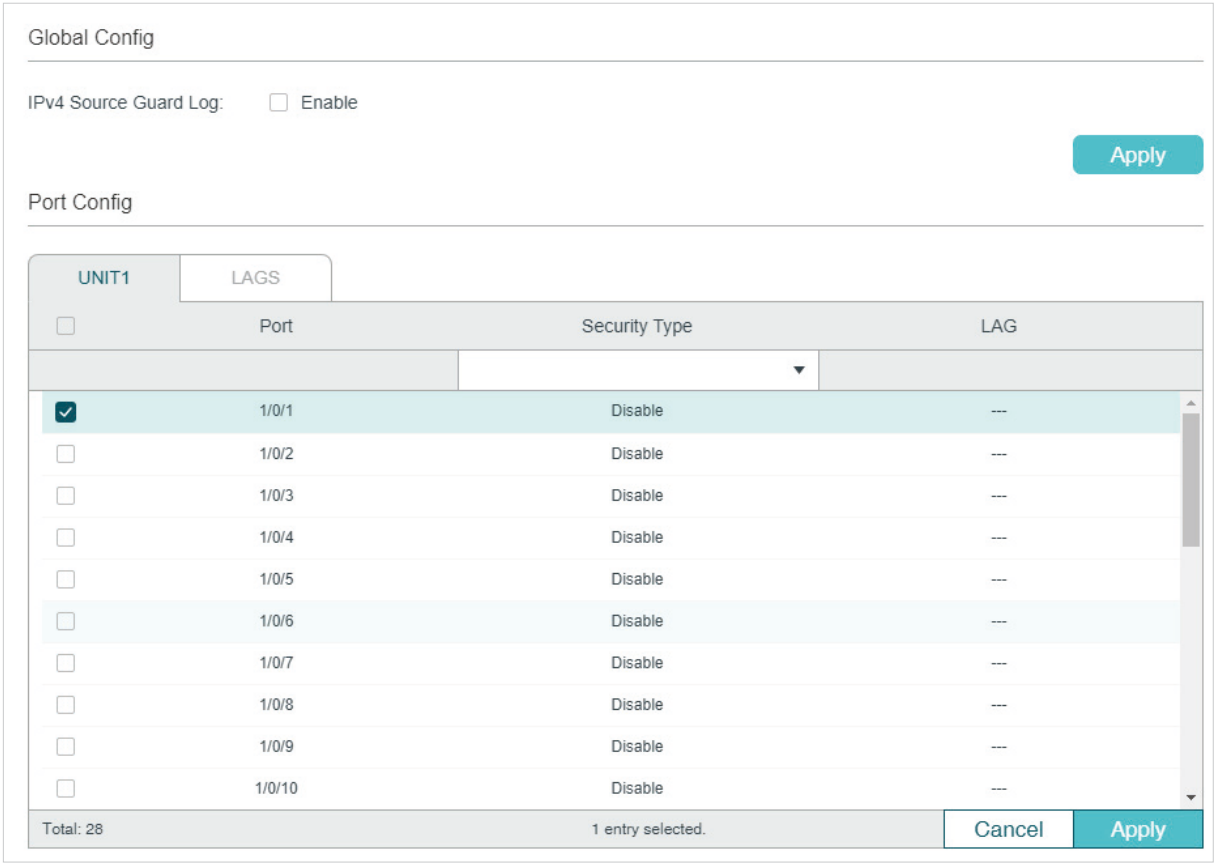
4.1.1 Adding IP-MAC Binding Entries

In IPv4 Source Guard, the switch filters the packets that do not match the rules of IPv4-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration. For details, refer to IP-MAC Binding Configuration.

4.1.2 Configuring IPv4 Source Guard

Choose the menu **SECURITY > IPv4 IMPB > IPv4 Source Guard** to load the following page.

Figure 4-1 IPv4 Source Guard Config



Follow these steps to configure IPv4 Source Guard:

1) In the **Global Config** section, choose whether to enable the Log feature. Click **Apply**.

IPv4 Source Guard Log	Enable or disable IPv4 Source Guard Log feature. With this feature enabled, the switch generates a log when illegal packets are received.

2) In the **Port Config** section, configure the protect type for ports and click **Apply**.

Port	Displays the port number.
Security Type	Select Security Type on the port for IPv4 packets. The following options are provided: **Disable:** The IP Source Guard feature is disabled on the port. **SIP+MAC**: Only the packet with its source IP address, source MAC address and port number matching the IPv4-MAC binding rules can be processed, otherwise the packet will be discarded. **SIP**: Only the packet with its source IP address and port number matching the IPv4-MAC binding rules can be processed, otherwise the packet will be discarded. Note: SIP is only available on certain devices.
LAG	Displays the LAG that the port is in.

4.2 Using the CLI

4.2.1 Adding IP-MAC Binding Entries

In IPv4 Source Guard, the switch filters the packets that do not match the rules of IPv4-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration. For details, refer to IP-MAC Binding Configuration.

4.2.2 Configuring IPv4 Source Guard

Follow these steps to configure IPv4 Source Guard:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.

Step 3	**ip verify source {** sip+mac | sip **}** Enable IP Source Guard for IPv4 packets. sip+mac: Only the packet with its source IP address, source MAC address and port number matching the IP-MAC binding rules can be processed, otherwise the packet will be discarded. sip: Only the packet with its source IP address and port number matching the IP-MAC binding rules can be processed, otherwise the packet will be discarded. Note: SIP is only available on certain devices.
Step 4	**show ip verify source [interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}]** Verify the IP Source Guard configuration for IPv4 packets.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IPv4 Source Guard on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip verify source sip+mac

Switch(config-if)#show ip verify source interface gigabitEthernet 1/0/1

```
Port       Security-Type     LAG
----       -------------     ----
Gi1/0/1    SIP+MAC           N/A
```

Switch(config-if)#end

Switch#copy running-config startup-config

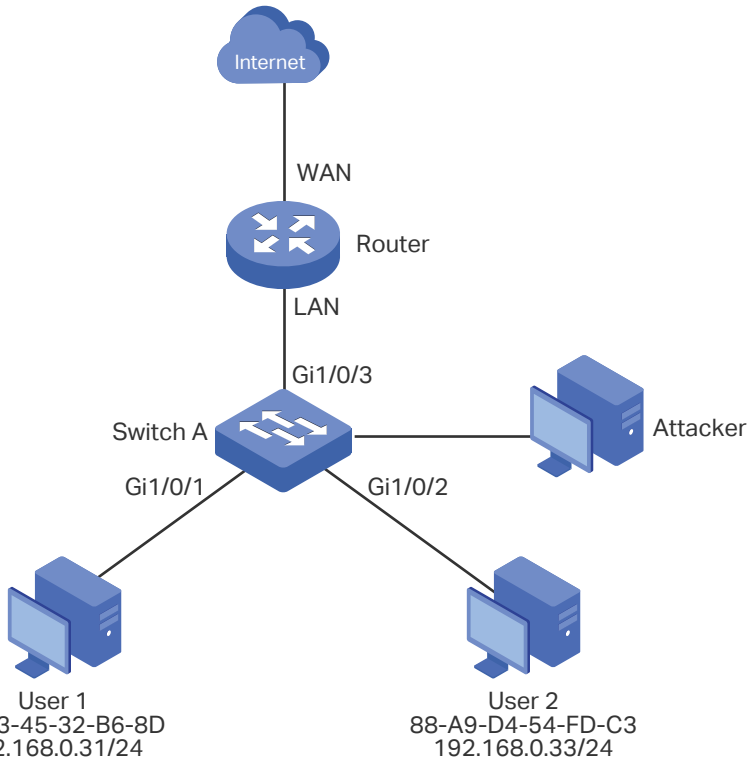
5 Configuration Examples

5.1 Example for ARP Detection

5.1.1 Network Requirements

As shown below, User 1 and User 2 are legal users in the LAN and connected to port 1/0/1 and port 1/0/2. Both of them are in the default VLAN 1. The router has been configured with security feature to prevent attacks from the WAN. Now the network administrator wants to configure Switch A to prevent ARP attacks from the LAN.

Figure 5-1 Network Topology



5.1.2 Configuration Scheme

To meet the requirement, you can configure ARP Detection to prevent the network from ARP attacks in the LAN.

The overview of configurations on the switch is as follows:

1) Configure IP-MAC Binding. The binding entries for User 1 and User 2 should be manually bound.
2) Configure ARP Detection globally.

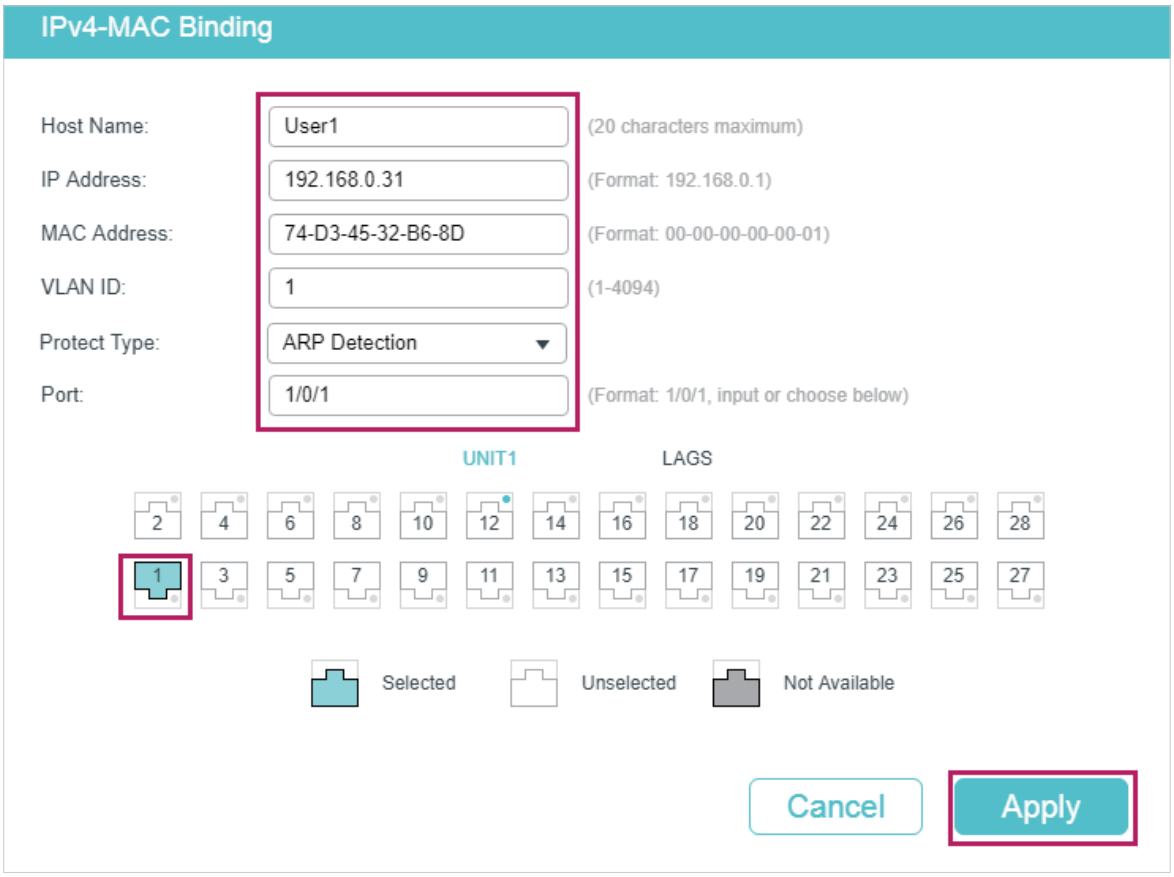
3) Configure ARP Detection on ports. Since port 1/0/3 is connected to the gateway router, set port 1/0/3 as trusted port. To prevent ARP flooding attacks, limit the speed of receiving the legal ARP packets on all ports.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.1.3 Using the GUI

1) Choose the menu **SECURITY > IPv4 IMBP > IP-MAC Binding > Manual Binding** and click Add to load the following page. Enter the host name, IP address, MAC address and VLAN ID of User 1, select the protect type as ARP Detection, and select port 1/0/1 on the panel. Click **Apply**.

Figure 5-2 Binding Entry for User 1



2) On the same page, add a binding entry for User 2. Enter the host name, IP address, MAC address and VLAN ID of User 2, select the protect type as ARP Detection, and select port 1/0/2 on the panel. Click **Apply**.

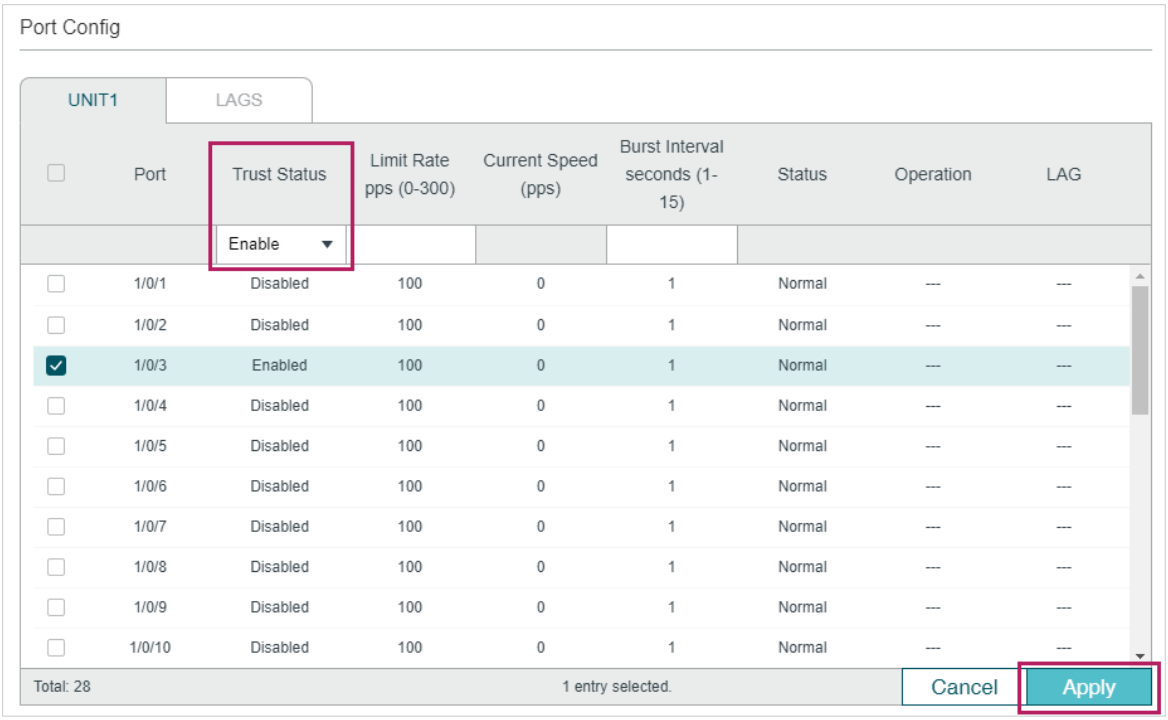
Figure 5-3 Binding Entry for User 2

3) Choose the menu **SECURITY > IPv4 IMBP > ARP Detection > Global Config** to load the following page. Enable APP Detect, Validate Source MAC, Validate Destination MAC and Validate IP, and click **Apply**. Select VLAN 1, change Status as Enabled and click **Apply**.

Figure 5-4 Enable ARP Detection

4) Choose the menu **SECURITY > IPv4 IMBP > ARP Detection > Port Config** to load the following page. By default, all ports are enabled with ARP Detection and ARP flooding defend. Configure port 1/0/3 as trusted port and keep other defend parameters as default. Click **Apply**.

Figure 5-5 Port Config



5) Click Save to save the settings.

5.1.4 Using the CLI

1) Manually bind the entries for User 1 and User 2.

Switch_A#configure

Switch_A(config)#ip source binding User1 192.168.0.31 74:d3:45:32:b6:8d vlan 1 interface gigabitEthernet 1/0/1 arp-detection

Switch_A(config)#ip source binding User1 192.168.0.32 88:a9:d4:54:fd:c3 vlan 1 interface gigabitEthernet 1/0/2 arp-detection

2) Enable ARP Detection globally and on VLAN 1.

Switch_A(config)#ip arp inspection

Switch_A(config)#ip arp inspection vlan 1

3) Configure port 1/0/3 as trusted port.

Switch_A(config)#interface gigabitEthernet 1/0/3

Switch_A(config-if)#ip arp inspection trust

Switch_A(config-if)#end

Switch_A#copy running-config startup-config

Verify the Configuration

Verify the IP-MAC Binding entries:

Switch_A#show ip source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	User1	192.168.0.31	74:d3:45:32:b6:8d	1	Gi1/0/1	ARP-D	Manual
1	User2	192.168.0.33	88:a9:d4:54:fd:c3	1	Gi1/0/2	ARP-D	Manual

Notice:

1.Here, 'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Verify the global configuration of ARP Detection:

Switch_A#show ip arp inspection

Global Status: Enable

Verify SMAC: Enable

Verify DMAC: Enable

Verify IP: Enable

Verify the ARP Detection configuration on VLAN:

Switch_A#show ip arp inspection vlan

VID	Enable status	Log Status
----	----------	----------
1	Enable	Disable

Verify the ARP Detection configuration on ports:

Switch_A#show ip arp inspection interface

Interface	Trust state	limit Rate(pps)	Current speed(pps)	Burst Interval	Status	LAG
---	---	---	---	---	---	---
Gi1/0/1	Disable	100	0	1	---	N/A
Gi1/0/2	Disable	100	0	1	---	N/A
Gi1/0/3	Enable	100	0	1	---	N/A

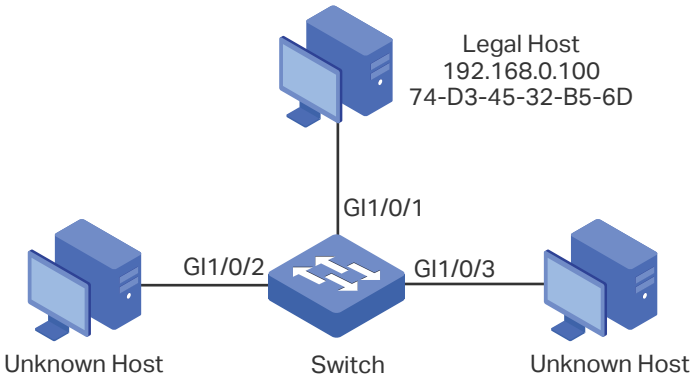
...

5.2 Example for IP Source Guard

5.2.1 Network Requirements

As shown below, the legal host connects to the switch via port 1/0/1 and belongs to the default VLAN 1. It is required that only the legal host can access the network via port 1/0/1, and other unknown hosts will be blocked when trying to access the network via ports 1/0/1-3.

Figure 5-6 Network Topology



5.2.2 Configuration Scheme

To implement this requirement, you can use IP-MAC Binding and IP Source Guard to filter out the packets received from the unknown hosts. The overview of configuration on the switch is as follows:

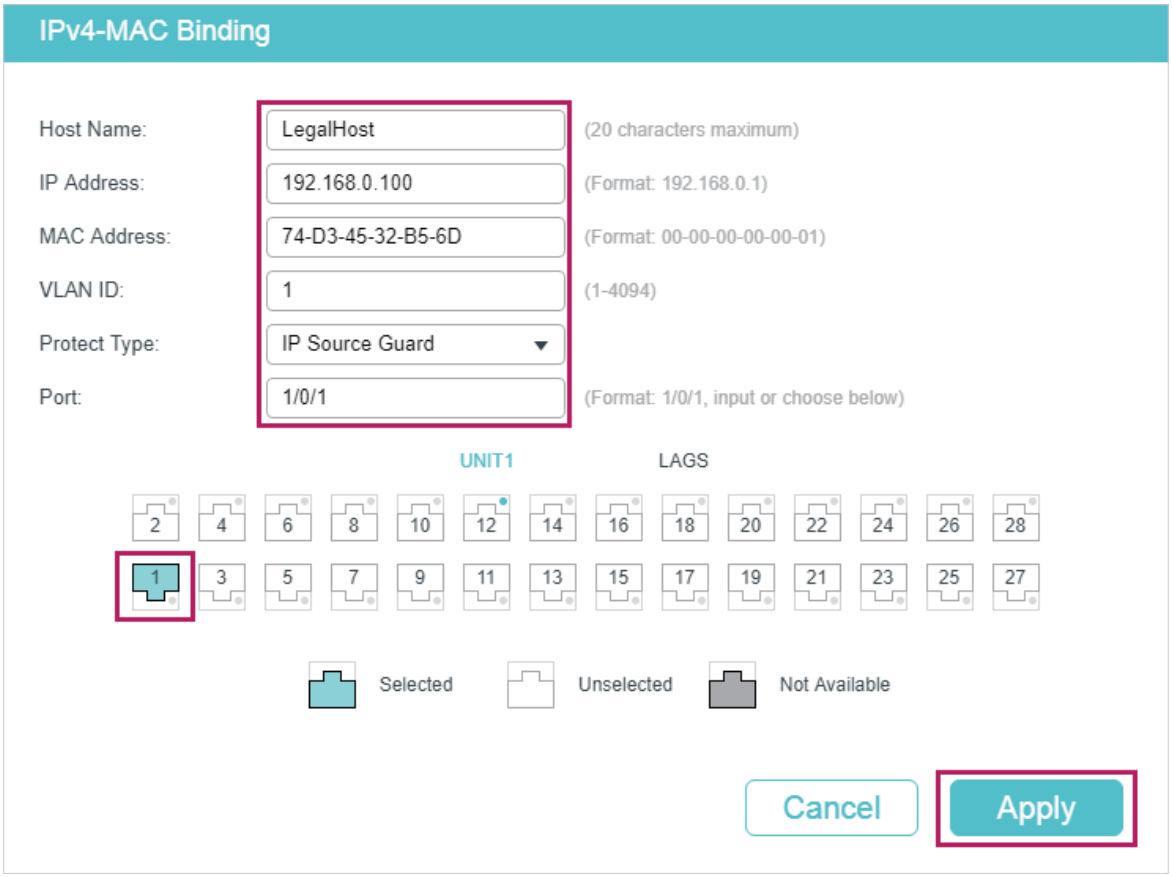
1) Bind the MAC address, IP address, connected port number and VLAN ID of the legal host with IP-MAC Binding.
2) Enable IP Source Guard on ports 1/0/1-3.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.2.3 Using the GUI

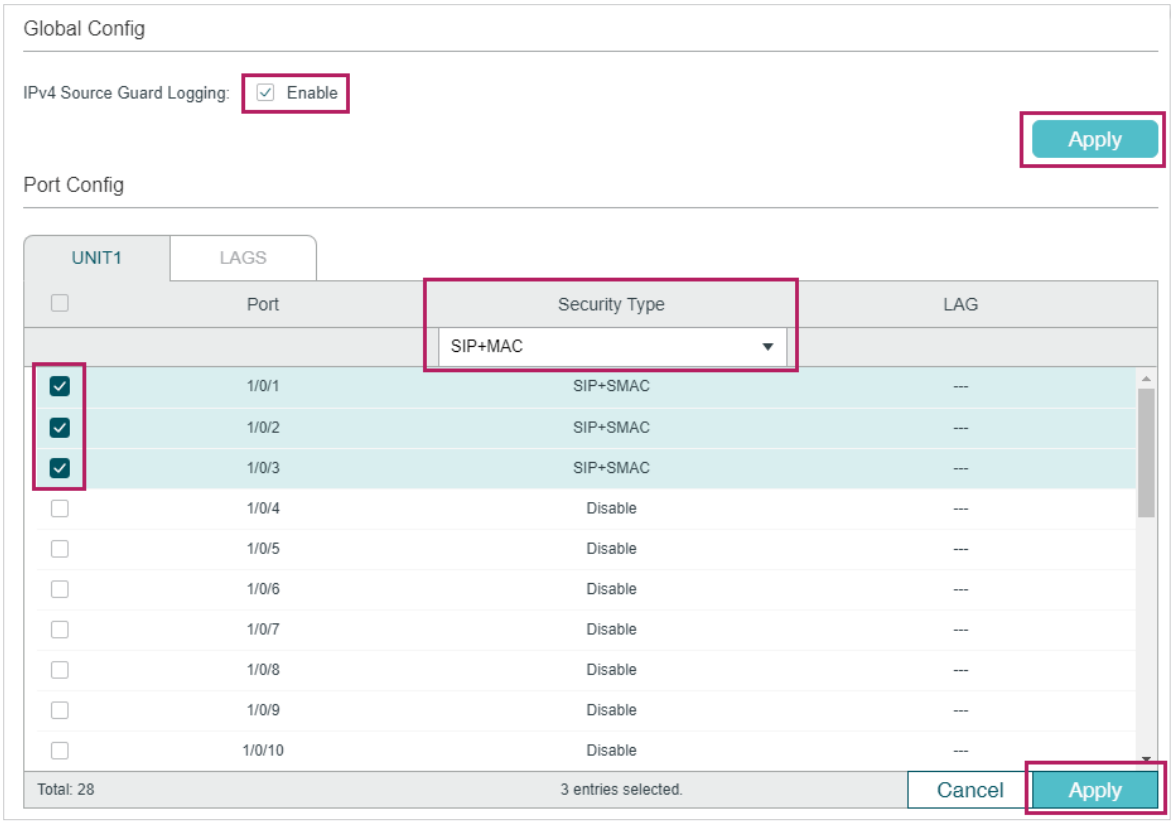
1) Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Manual Binding** and click Add to load the following page. Enter the host name, IP address, MAC address and VLAN ID of the legal host, select the protect type as , and select port 1/0/1 on the panel. Click **Apply**.

Figure 5-7 Manual Binding



2) Choose the menu **SECURITY > IPv4 IMPB > IPv4 Source Guard** to load the following page. Enable IPv4 Source Guard Logging to make the switch generate logs when receiving illegal packets, and click **Apply**. Select ports 1/0/1-3, configure the Security Type as SIP+MAC, and click **Apply**.

Figure 5-8 IPv4 Source Guard



3) Click Save to save the settings.

5.2.4 Using the CLI

1) Manually bind the IP address, MAC address, VLAN ID and connected port number of the legal host, and apply this entry to the IP Source Guard feature.

   Switch#configure

   Switch(config)#ip source binding legal-host 192.168.0.100 74:d3:45:32:b5:6d vlan 1 interface gigabitEthernet 1/0/1 ip-verify-source

2) Enable the log feature and IP Source Guard on ports 1/0/1-3.

   Switch(config)# ip verify source logging

   Switch(config)# interface range gigabitEthernet 1/0/1-3

   Switch(config-if-range)#ip verify source sip+mac

   Switch(config-if-range)#end

   Switch#copy running-config startup-config

Verify the Configuration

Verify the binding entry:

Switch#show ip source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	User1	192.168.0.100	74:d3:45:32:b5:6d	1	Gi1/0/1	IP-V-S	Manual

Notice:

1.Here, 'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Verify the configuration of IP Source Guard:

Switch#show ip verify source

IP Source Guard log: Enabled

Port	Security-Type	LAG
Gi1/0/1	SIP+MAC	N/A
Gi1/0/2	SIP+MAC	N/A
Gi1/0/3	SIP+MAC	N/A

...

6 Appendix: Default Parameters

Default settings of DHCP Snooping are listed in the following table:

Table 6-1 DHCP Snooping

Parameter	Default Setting
Global Config	
DHCP Snooping	Disabled
VLAN Config	
Status	Disabled
Port Config	
Maximum Entry	512

Default settings of ARP Detection are listed in the following table:

Table 6-2 ARP Detection

Parameter	Default Setting
Global Config	
ARP Detect	Disabled
Validate Source MAC	Disabled
Validate Destination MAC	Disabled
Validate IP	Disabled
VLAN Config	
Status	Disabled
Log Status	Disabled
Port Config	
Trust Status	Disabled
Limit Rate	100 pps

Parameter	Default Setting
Burst Interval	1 second
ARP Statistics	
Auto Refresh	Disabled
Refresh Interval	5 seconds

Default settings of IPv4 Source Guard are listed in the following table:

Table 6-3 ARP Detection

Parameter	Default Setting
Global Config	
IPv4 Source Guard Log:	Disabled
Port Config	
Security Type	Disabled

Part 29

Configuring IPv6 IMPB

CHAPTERS

1. IPv6 IMPB
2. IPv6-MAC Binding Configuration
3. ND Detection Configuration
4. IPv6 Source Guard Configuration
5. Configuration Examples
6. Appendix: Default Parameters

1 IPv6 IMPB

1.1 Overview

IPv6 IMPB (IP-MAC-Port Binding) is used to bind the IPv6 address, MAC address, VLAN ID and the connected port number of the specified host. Basing on the binding table, the switch can prevent ND attacks with the ND Detection feature and filter the packets that don't match the binding entries with the IPv6 Source Guard feature.

1.2 Supported Features

IPv6-MAC Binding

This feature is used to add binding entries. The binding entries can be manually configured, or learned by ND Snooping or DHCPv6 snooping. The features ND Detection and IPv6 Source Guard are based on the IPv6-MAC Binding entries.

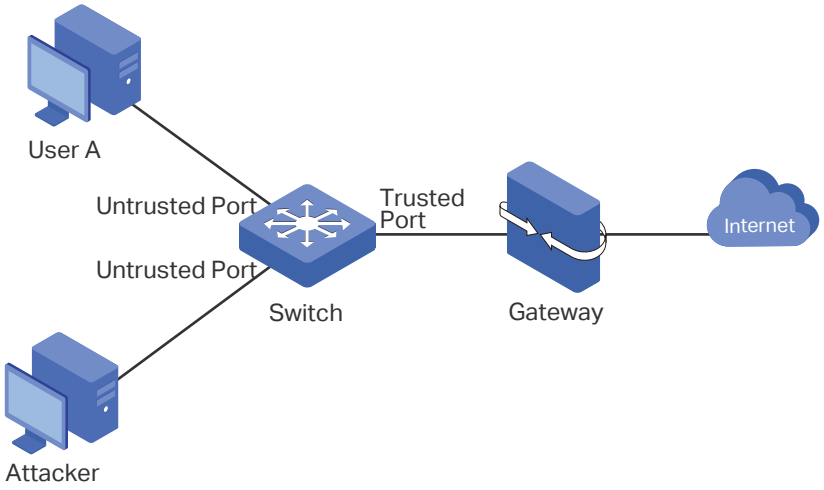
ND Detection

Because of the absence of security mechanism, IPv6 ND (Neighbor Discovery) protocol is easy to be exploited by attackers. ND detection feature uses the entries in the IPv6-MAC binding table to filter the forged ND packets and prevent the ND attacks.

The application topology of ND Detection is as the following figure shows. The port that is connected to the gateway should be configured as trusted port, and other ports should be configured as untrusted ports. The forwarding principles of ND packets are as follows:

- All ND packets received on the trusted port will be forwarded without checked.
- RS (Router Solicitation) and NS (Neighbor Solicitation) packets with their source IPv6 addresses unspecified, such as the RS packet for IPv6 address request and the NS packet for duplicate address detection, will not be checked on both kinds of ports.
- RA (Router Advertisement) and RR (Router Redirect) packets received on the untrusted port will be discarded directly, and other ND packets will be checked: The switch will use the IPv6-MAC binding table to compare the IPv6 address, MAC address, VLAN ID and receiving port between the entry and the ND packet. If a match is found, the ND packet is considered legal and will be forwarded; if no match is found, the ND packet is considered illegal and will be discarded.

Figure 1-1 Network Topology of ND Detection



IPv6 Source Guard

IPv6 Source Guard is used to filter the IPv6 packets based on the IPv6-MAC Binding table. Only the packets that match the binding rules are forwarded.

2 IPv6-MAC Binding Configuration

You can add IPv6-MAC Binding entries in three ways:

- Manual Binding
- Via ND Snooping
- Via DHCPv6 Snooping

Additionally, you can view, search and edit the entries in the Binding Table.

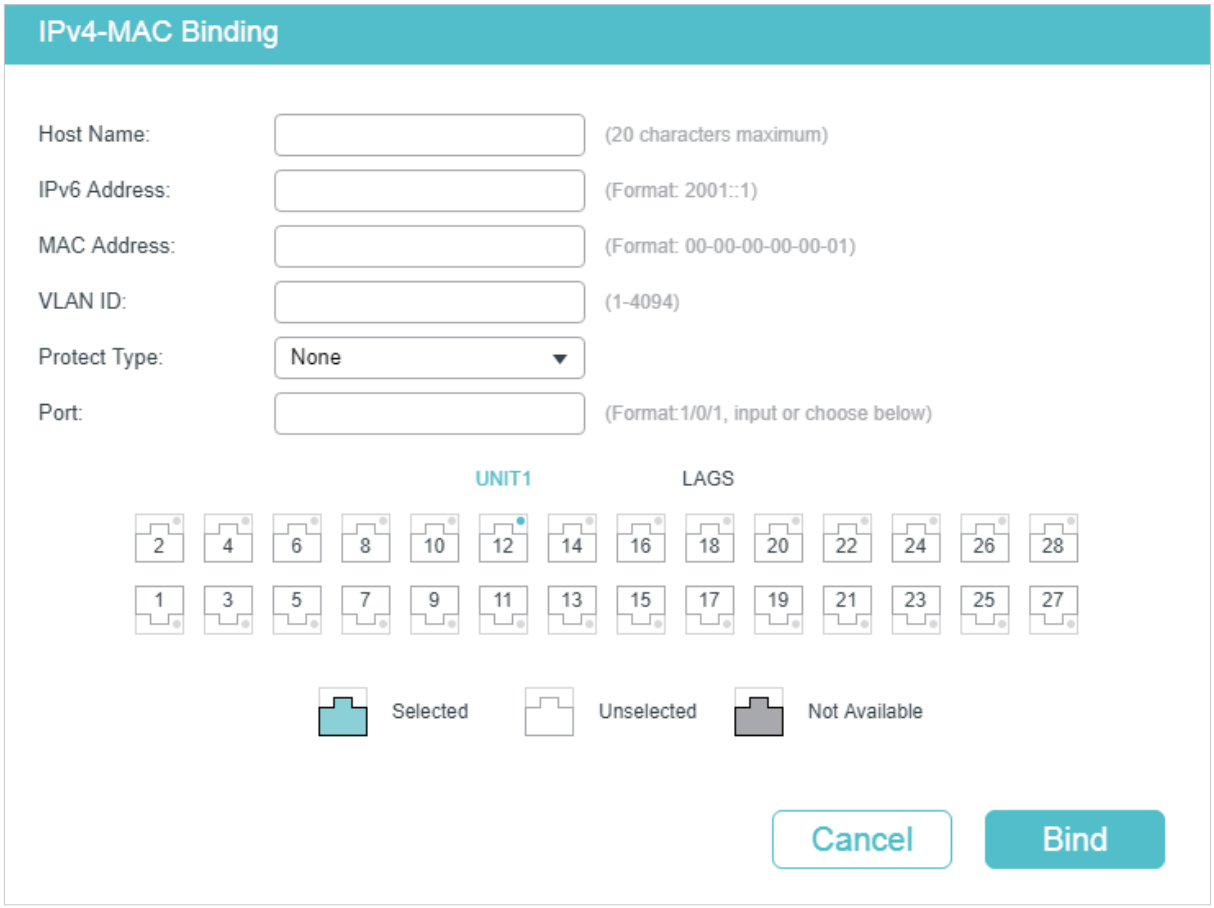
2.1 Using the GUI

2.1.1 Binding Entries Manually

You can manually bind the IPv6 address, MAC address, VLAN ID and the Port number together on the condition that you have got the detailed information of the hosts.

Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Manual Binding** and click Add to load the following page.

Figure 2-1 Manual Binding



Follow these steps to manually create an IPv6-MAC Binding entry:

1) Enter the following information to specify a host.

Host Name	Enter the host name for identification.
IPv6 Address	Enter the IPv6 address.
MAC Address	Enter the MAC address.
VLAN ID	Enter the VLAN ID.

2) Select protect type for the entry.

Protect Type	Select the protect type for the entry. The entry will be applied to to the specific feature. The following options are provided: **None**: This entry will not be applied to any feature. **ND Detection**: This entry will be applied to the ND Detection feature. **IPv6 Source Guard**: This entry will be applied to the IPv6 Source Guard feature. **Both**: This entry will be applied to both of the features.

3) Enter or select the port that is connected to this host.

4) Click **Apply**.

2.1.2 Binding Entries via ND Snooping

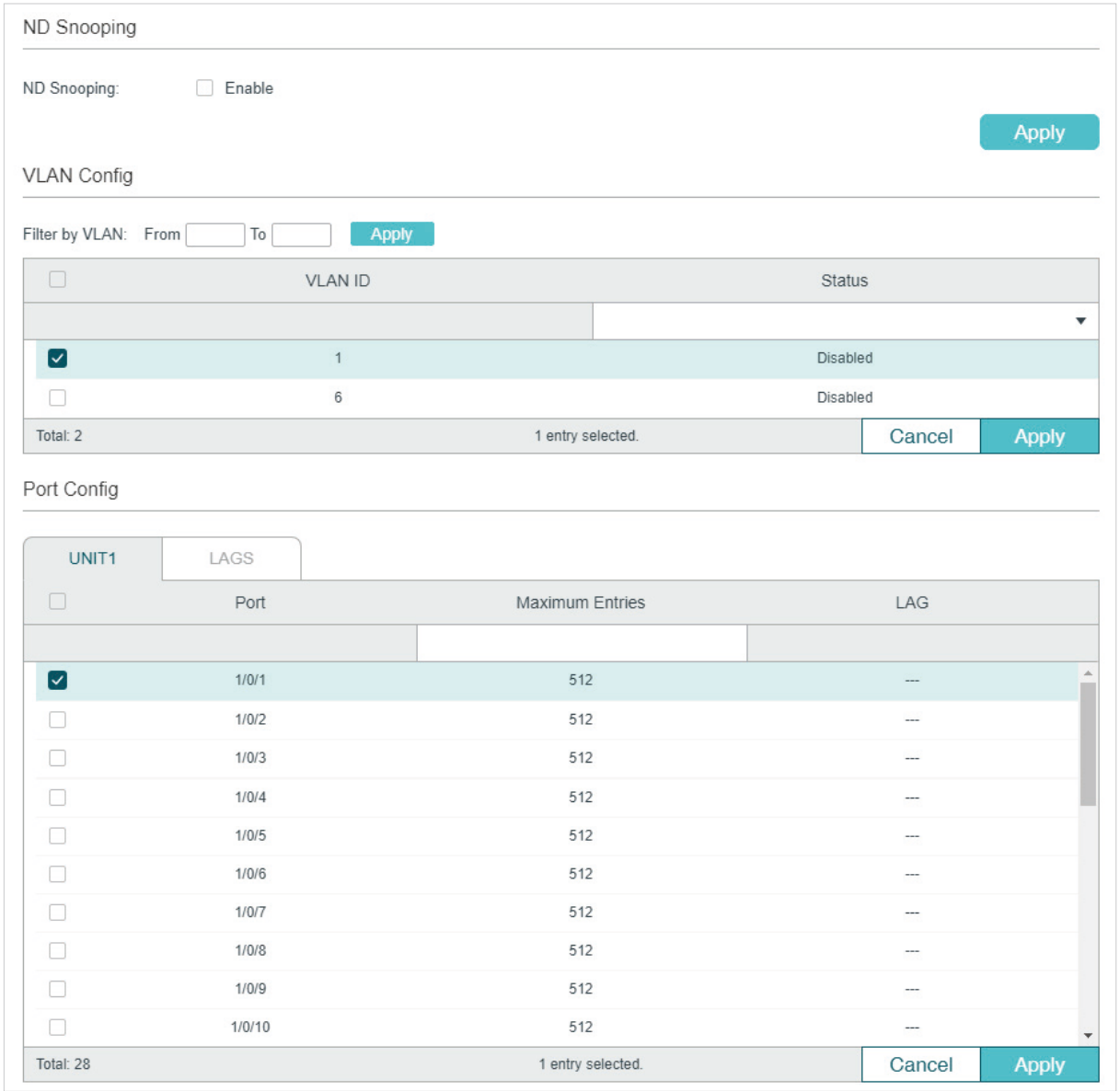
With ND Snooping, the switch monitors the ND packets, and records the IPv6 addresses, MAC addresses, VLAN IDs and the connected port numbers of the IPv6 hosts. You can bind these entries conveniently.

Note:

Before using this feature, make sure that your network is safe and the hosts are not suffering from ND attacks at present; otherwise, you may obtain incorrect IPv6-MAC Binding entries. If your network is being attacked, it's recommended to bind the entries manually.

Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > ND Snooping** to load the following page.

Figure 2-2 ND Snooping



Follow these steps to configure IPv6-MAC Binding via ND Snooping:

1) In the **ND Snooping** section, enable ND Snooping and click **Apply**.

2) In the **VLAN Config** section, select one or more VLANs and enable ND Snooping. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable ND Snooping on the VLAN.

3) In the **Port Config** section, configure the maximum number of entries a port can learn via ND snooping. Click **Apply**.

Port	Displays the port number.
Maximum Entries	Configure the maximum number of binding entries a port can learn via ND snooping.
LAG	Displays the LAG that the port is in.

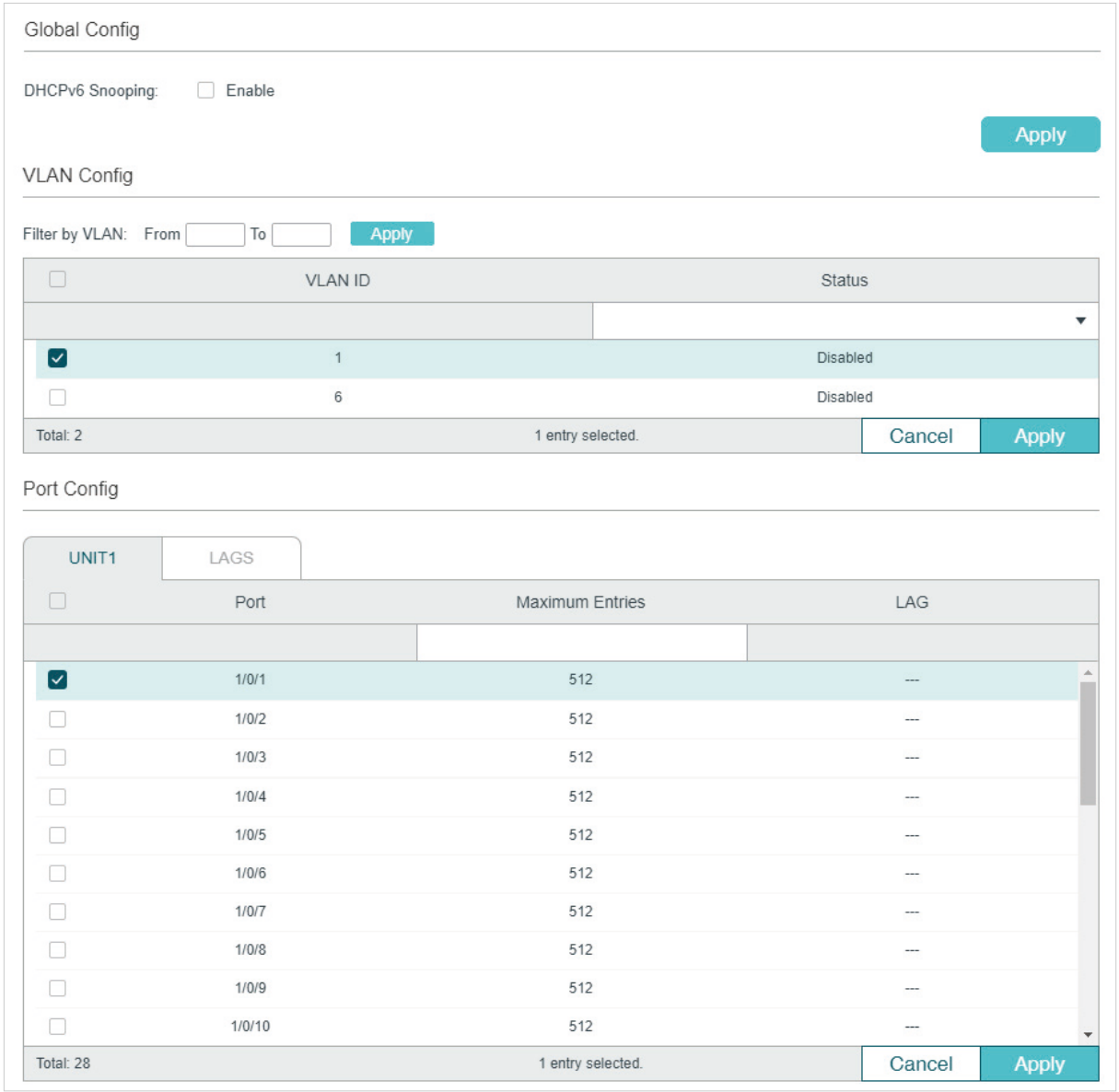
4) The learned entries will be displayed in the Binding Table. You can go to **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Binding Table** to view or edit the entries.

2.1.3 Binding Entries via DHCPv6 Snooping

With DHCPv6 Snooping enabled, the switch can monitor the IP address obtaining process of the host, and record the IPv6 address, MAC address, VLAN ID and the connected port number of the host.

Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > DHCPv6 Snooping** to load the following page.

Figure 2-3 DHCPv6 Snooping



Follow these steps to configure IPv6-MAC Binding via DHCPv6 Snooping:

1) In the **Global Config** section, globally enable DHCPv6 Snooping. Click **Apply**.

2) In the **VLAN Config** section, enable DHCPv6 Snooping on a VLAN or range of VLANs. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable DHCPv6 Snooping on the VLAN.

3) In the **Port Config** section, configure the maximum number of binding entries a port can learn via DHCPv6 snooping. Click **Apply**.

Port	Displays the port number.

Maximum Entries	Configure the maximum number of binding entries a port can learn via DHCPv6 snooping.
LAG	Displays the LAG that the port is in.

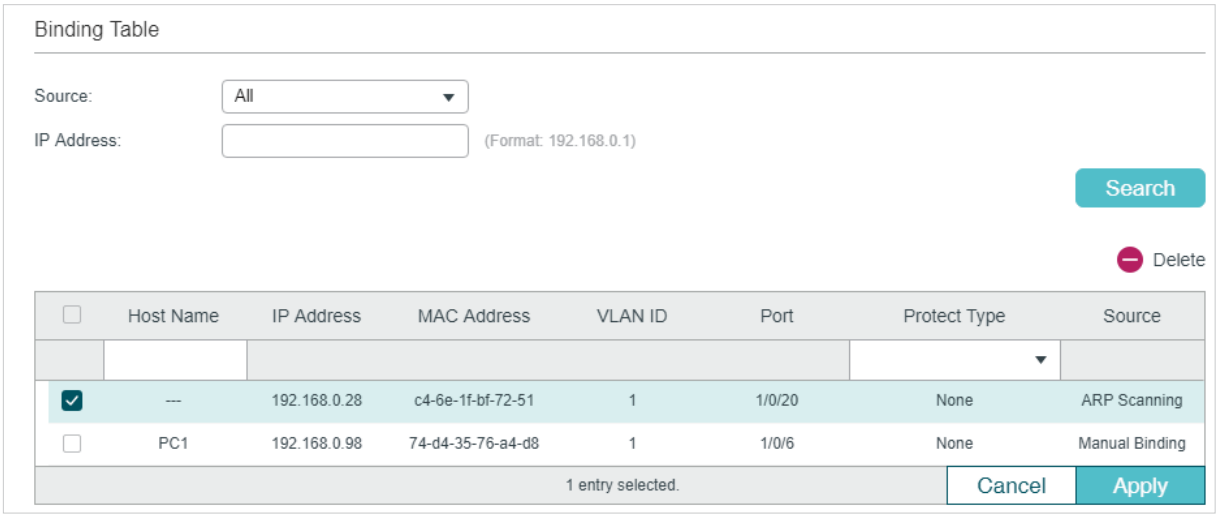
4) The learned entries will be displayed in the Binding Table. You can go to **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Binding Table** to view or edit the entries.

2.1.4 Viewing the Binding Entries

In the Binding Table, you can view, search and edit the specified binding entries.

Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Binding Table** to load the following page.

Figure 2-4 Binding Table



You can specify the search criteria to search your desired entries.

Source	Select the source of the entry and click **Search**. **All**: Displays the entries from all sources. **Manual Binding**: Displays the manually bound entries. **ND Snooping**: Displays the binding entries learned from ND Snooping. **DHCPv6 Snooping**: Displays the binding entries learned from DHCP Snooping.
IP	Enter an IP address and click **Search** to search the specific entry.

Additionally, you select one or more entries to edit the host name and protect type and click **Apply**.

Host Name	Enter a host name for identification.
IP Address	Displays the IPv6 address.
MAC Address	Displays the MAC address.

VLAN ID	Displays the VLAN ID.
Port	Displays the port number.
Protect Type	Select the protect type for the entry. The entry will be applied to to the specific feature. The following options are provided: **None**: This entry will not be applied to any feature. **ND Detection**: This entry will be applied to the ND Detection feature. **IPv6 Source Guard**: This entry will be applied to the IP Source Guard feature. **Both**: This entry will be applied to both of the features.
Source	Displays the source of the entry.

2.2 Using the CLI

The following sections introduce how to bind entries manually and via ND Snooping and DHCP Snooping, and how to view the binding entries.

2.2.1 Binding Entries Manually

You can manually bind the IPv6 address, MAC address, VLAN ID and the Port number together on the condition that you have got the detailed information of the hosts.

Follow these steps to manually bind entries:

Step 1	**configure** Enter global configuration mode.

Step 2	**ipv6 source binding** *hostname ipv6-addr mac-addr* **vlan** *vlan-id* **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **} {** none | nd-detection | ipv6-verify-source | both **}** Manually bind the host name, IP address, MAC address, VLAN ID and port number of the host, and configure the protect type for the host. *hostname*: Specify a name for the host. It contains 20 characters at most. *ipv6-addr*: Enter the IPv6 address of the host. *mac-addr*: Enter the MAC address of the host, in the format of xx:xx:xx:xx:xx:xx. *vlan-id*: Enter the VLAN ID of the host. *port*: Enter the number of the port on which the host is connected. none | nd-detection | ipv6-verify-source | both: Specify the protect type for the entry. None indicates this entry will not be applied to any feature; nd-detection indicates this entry will be applied to ND Detection; ipv6-verify-source indicates this entry will be applied to IP Source Guard; both indicates this entry will be applied to both ND Detection and IP Source Guard.
Step 3	**show ip source binding** Verify the binding entry.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind an entry with the hostname host1, IPv6 address 2001:0:9d38:90d5::34, MAC address AA-BB-CC-DD-EE-FF, VLAN ID 10, port number 1/0/5, and enable this entry for ND Detection.

Switch#configure

Switch(config)#ipv6 source binding host1 2001:0:9d38:90d5::34 aa:bb:cc:dd:ee:ff **vlan** 10 **interface gigabitEthernet** 1/0/5 nd-detection

Switch(config)#show ipv6 source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	Source
-	----	-------	--------	---	----	---	------
1	host1	2001:0:9d38:90d5::34	aa:bb:cc:dd:ee:ff	10	Gi1/0/5	ND-D	Manual

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Binding Entries via ND Snooping

Follow these steps to bind entries via ND Snooping:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 nd snooping** Globally enable ND Snooping.
Step 3	**ipv6 nd snooping vlan** *vlan-range* Enable ND Snooping on the specified VLAN. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 5	**ipv6 nd snooping max-entries** *value* Configure the maximum number of ND binding entries a port can learn via ND snooping. *value:* Enter the maximum number of ND binding entries a port can learn via ND snooping. The valid values are from 0 to 1024, and the default is 1024.
Step 6	**show ipv6 nd snooping** Verify the global configuration of IPv6 ND Snooping
Step 7	**show ipv6 nd snooping interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Verify the IPv6 ND Snooping configuration of the specific port.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable ND Snooping globally and on VLAN 1.

Switch#configure

Switch(config)#ipv6 nd snooping

Switch(config)#ipv6 nd snooping vlan 1

Switch(config)#show ipv6 nd snooping

Global Status: Enable

VLAN ID: 1

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to configure the maximum number of entries that can be learned on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 nd snooping max-entries 1000

Switch(config-if)#show ipv6 nd snooping interface gigabitEthernet 1/0/1

Interface	max-entries	LAG
---	---	---
Gi1/0/1	1000	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Binding Entries via DHCPv6 Snooping

Follow these steps to bind entries via DHCP Snooping:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 dhcp snooping** Globally enable DHCPv6 Snooping.
Step 3	**ipv6 dhcp snooping vlan** *vlan-range* Enable DHCPv6 Snooping on the specified VLAN. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 5	**ipv6 dhcp snooping max-entries** *value* Configure the maximum number of binding entries the port can learn via DHCPv6 snooping. *value:* Enter the value of maximum number of entries. The valid values are from 0 to 512.
Step 6	**show ip dhcp snooping** Verify global configuration of DHCPv6 Snooping.

Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCPv6 Snooping globally and on VLAN 5, and set the maximum number of binding entries port 1/0/1 can learn via DHCPv6 snooping as 100:

Switch#configure

Switch(config)#ipv6 dhcp snooping

Switch(config)#ipv6 dhcp snooping vlan 5

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 dhcp snooping max-entries 100

Switch(config-if)#show ipv6 dhcp snooping

Global Status: Enable

VLAN ID: 5

Switch(config-if)#show ipv6 dhcp snooping interface gigabitEthernet 1/0/1

Interface max-entries LAG

--- --- ---

Gi1/0/1 100 N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Viewing Binding Entries

On privileged EXEC mode or any other configuration mode, you can use the following command to view binding entries:

show ipv6 source binding View the information of binding entries, including the host name, IP address, MAC address, VLAN ID, port number and protect type.

3 ND Detection Configuration

To complete ND Detection configuration, follow these steps:

1) Add IPv6-MAC Binding entries.
2) Enable ND Detection.
3) Configure ND Detection on ports.
4) View ND statistics.

3.1 Using the GUI

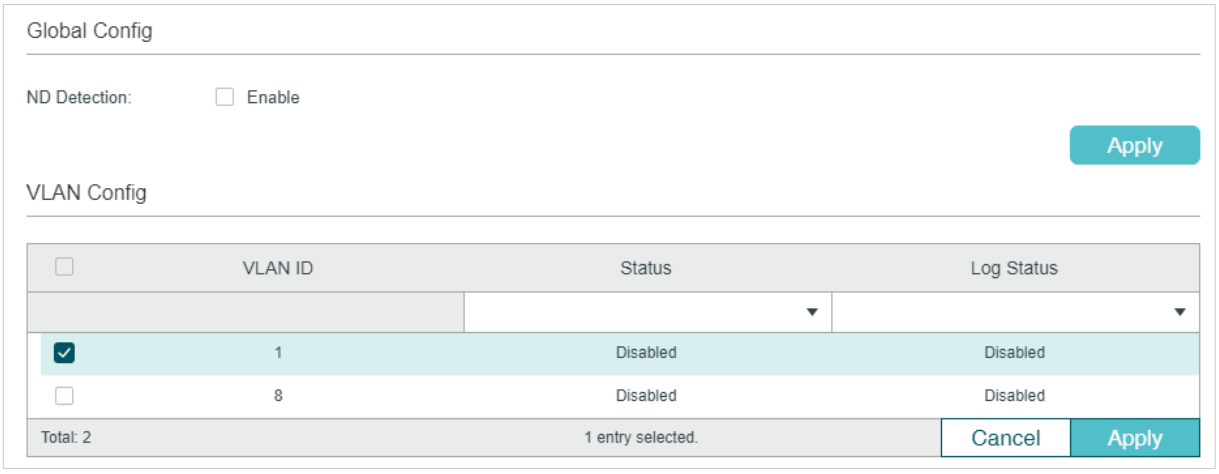
3.1.1 Adding IPv6-MAC Binding Entries

The ND Detection feature allows the switch to detect the ND packets based on the binding entries in the IPv6-MAC Binding Table and filter out the illegal ND packets. Before configuring ND Detection, complete IPv6-MAC Binding configuration. For details, refer to IPv6-MAC Binding Configuration.

3.1.2 Enabling ND Detection

Choose the menu **SECURITY > IPv6 IMPB > ND Detection > Global Config** to load the following page.

Figure 3-1 ND Detection Global Config



Follow these steps to enable ND Detection:

1) In the **Global Config** section, enable ND Detection and configure the related parameters. Click **Apply**.

ND Detection	Enable or disable ND Detection globally.

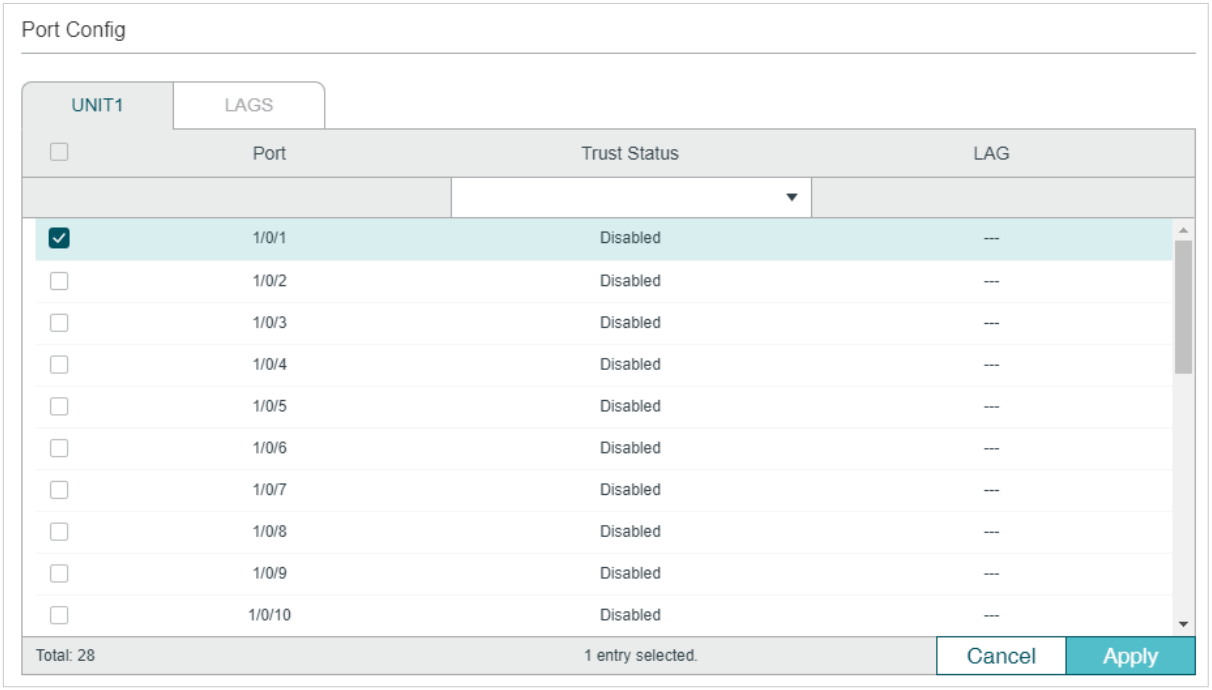
2) In the **VLAN Config** section, enable ND Detection on the selected VLANs. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable ND Detection on the VLAN.
Log Status	Enable or disable Log feature on the VLAN. With this feature enabled, the switch generates a log when an illegal ND packet is discarded.

3.1.3 Configuring ND Detection on Ports

Choose the menu **SECURITY > IPv6 IMPB > ND Detection >Port Config** to load the following page.

Figure 3-2 ND Detection on Port



Follow these steps to configure ND Detection on ports:

1) Select one or more ports and configure the parameters.

Port	Displays the port number.
Trust Status	Enable or disable this port to be a trusted port. On a trusted port, the ND packets are forwarded directly without checked. The specific ports, such as up-link ports and routing ports are suggested to be set as trusted.
LAG	Displays the LAG that the port is in.

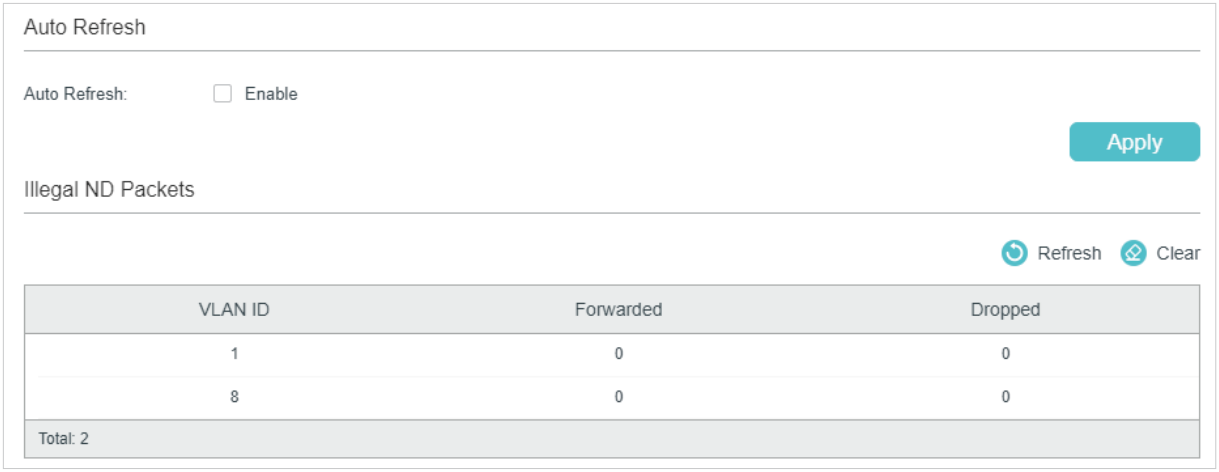
2) Click **Apply**.

3.1.4 Viewing ND Statistics

You can view the number of the illegal ND packets received on each port, which facilitates you to locate the network malfunction and take the related protection measures.

Choose the menu **SECURITY > IPv6 IMPB > ND Detection > ND Statistics** to load the following page.

Figure 3-3 View ND Statistics



In the **Auto Refresh** section, you can enable the auto refresh feature and specify the refresh interval, and thus the web page will be automatically refreshed.

In the **Illegal ND Packet** section, you can view the number of illegal ND packets in each VLAN.

VLAN ID	Displays the VLAN ID.
Forwarded	Displays the number of forwarded ND packets in this VLAN.
Dropped	Displays the number of dropped ND packets in this VLAN.

3.2 Using the CLI

3.2.1 Adding IPv6-MAC Binding Entries

The ND Detection feature allows the switch to detect the ND packets based on the binding entries in the IPv6-MAC Binding Table and filter out the illegal ND packets. Before configuring ND Detection, complete IPv6-MAC Binding configuration. For details, refer to IPv6-MAC Binding Configuration.

3.2.2 Enabling ND Detection

Follow these steps to enable ND Detection:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 nd detection** Globally enable the ND Detection feature.

Step 3	**ipv6 nd detection vlan** *vlan-range* Enable ND Detection on the specified VLAN. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 4	**ipv6 nd detection vlan** *vlan-range* **logging** (Optional) Enable the Log feature to make the switch generate a log when an ND packet is discarded. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 5	**show ipv6 nd detection** Verify the global ND Detection configuration.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable ND Detection globally and on VLAN 1:

Switch#configure

Switch(config)#ipv6 nd detection

Switch(config)#ipv6 nd detection vlan 1

Switch(config)#show ipv6 nd detection

Global Status: Enable

Switch(config)#show ipv6 nd detection vlan

VID	Enable status	Log Status
----	----------	----------
1	Enable	Disable

Switch(config)#end

Switch#copy running-config startup-config

3.2.3 Configuring ND Detection on Ports

Follow these steps to configure ND Detection on ports:

Step 1	**configure** Enter global configuration mode.

Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ipv6 nd detection trust** Configure the port as a trusted port, on which the ND packets will not be checked. The specific ports, such as up-linked ports and routing ports are suggested to be set as trusted ports.
Step 4	**show ipv6 nd detection interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Verify the global ND Detection configuration of the port.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure port 1/0/1 as trusted port:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 nd detection trust

Switch(config-if)#show ipv6 nd detection interface gigabitEthernet 1/0/1

Interface Trusted LAG

--------- ------- ---

Gi1/0/1 Enable N/A

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.4 Viewing ND Statistics

On privileged EXEC mode or any other configuration mode, you can use the following command to view ND statistics:

show ipv6 nd detection statistics View the ND statistics on each port, including the number of forwarded ND packets and the number of dropped ND packets.

4 IPv6 Source Guard Configuration

To complete IPv6 Source Guard configuration, follow these steps:

1) Add IP-MAC Binding entries.
2) Configure IPv6 Source Guard.

4.1 Using the GUI

4.1.1 Adding IPv6-MAC Binding Entries

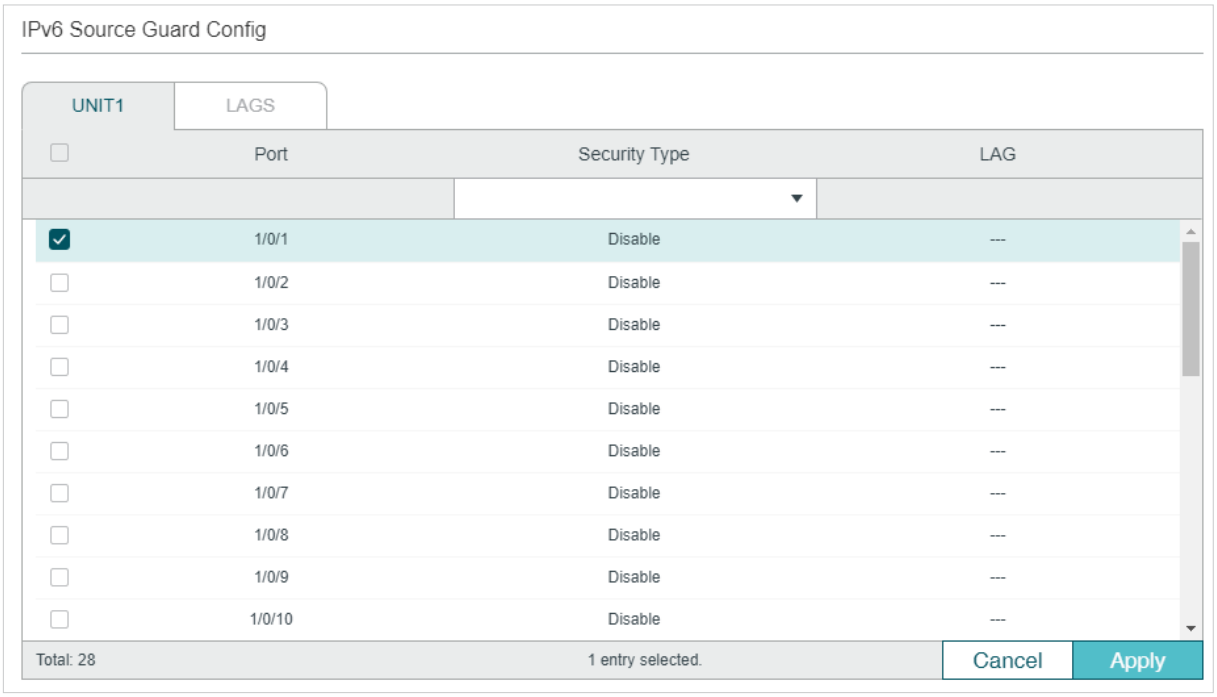
The ND Detection feature allows the switch to detect the ND packets based on the binding entries in the IPv6-MAC Binding Table and filter out the illegal ND packets. Before configuring ND Detection, complete IPv6-MAC Binding configuration. For details, refer to IPv6-MAC Binding Configuration.

4.1.2 Configuring IPv6 Source Guard

Before configuring IPv6 Source Guard, you need to configure the SDM template as EnterpriseV6.

Choose the menu **SECURITY > IPv6 IMPB > IPv6 Source Guard** to load the following page.

Figure 4-1 IPv6 Source Guard Config



Follow these steps to configure IPv6 Source Guard:

1) Select one or more ports and configure the protect type for ports.

Port	Displays the port number.
Security Type	Select Security Type on the port for IPv6 packets. The following options are provided: **Disable:** The IP Source Guard feature is disabled on the port. **SIPv6+MAC**: Only the packet with its source IPv6 address, source MAC address and port number matching the IPv6-MAC binding rules can be processed, otherwise the packet will be discarded. **SIPv6**: Only the packet with its source IPv6 address and port number matching the IPv6-MAC binding rules can be processed, otherwise the packet will be discarded.
LAG	Displays the LAG that the port is in.

2) Click **Apply**.

4.2 Using the CLI

4.2.1 Adding IPv6-MAC Binding Entries

The ND Detection feature allows the switch to detect the ND packets based on the binding entries in the IPv6-MAC Binding Table and filter out the illegal ND packets. Before configuring ND Detection, complete IPv6-MAC Binding configuration. For details, refer to IPv6-MAC Binding Configuration.

4.2.2 Configuring IPv6 Source Guard

Before configuring IPv6 Source Guard, you need to configure the SDM template as EnterpriseV6.

Follow these steps to configure IPv6 Source Guard:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ipv6 verify source {** sipv6+mac | sipv6 **}** Enable IPv6 Source Guard for IPv6 packets. sipv6+mac: Only the packet with its source IPv6 address, source MAC address and port number matching the IPv6-MAC binding rules can be processed, otherwise the packet will be discarded. sipv6: Only the packet with its source IPv6 address and port number matching the IPv6-MAC binding rules can be processed, otherwise the packet will be discarded.

Step 4	**show ipv6 verify source [interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}]** Verify the IP Source Guard configuration for IPv6 packets.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IPv6 Source Guard on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 verify source sipv6+mac

Switch(config-if)#show ipv6 verify source interface gigabitEthernet 1/0/1

Port Security-Type LAG

---- ------------ ----

Gi1/0/1 SIPv6+MAC N/A

Switch(config-if)#end

Switch#copy running-config startup-config

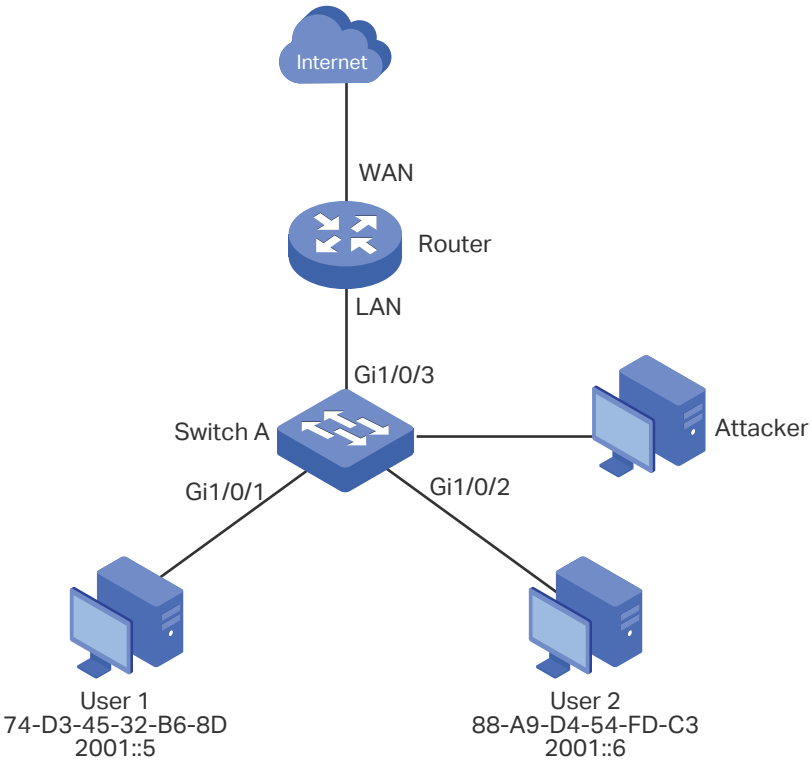
5 Configuration Examples

5.1 Example for ND Detection

5.1.1 Network Requirements

As shown below, User 1 and User 2 are legal IPv6 users in the LAN and connected to port 1/0/1 and port 1/0/2. Both of them are in the default VLAN 1. The router has been configured with security feature to prevent attacks from the WAN. Now the network administrator wants to configure Switch A to prevent ND attacks from the LAN.

Figure 5-1 Network Topology



5.1.2 Configuration Scheme

To meet the requirement, you can configure ND Detection to prevent the network from ND attacks in the LAN.

The overview of configurations on the switch is as follows:

1) Configure IPv6-MAC Binding. The binding entries for User 1 and User 2 should be manually bound.
2) Configure ND Detection globally.

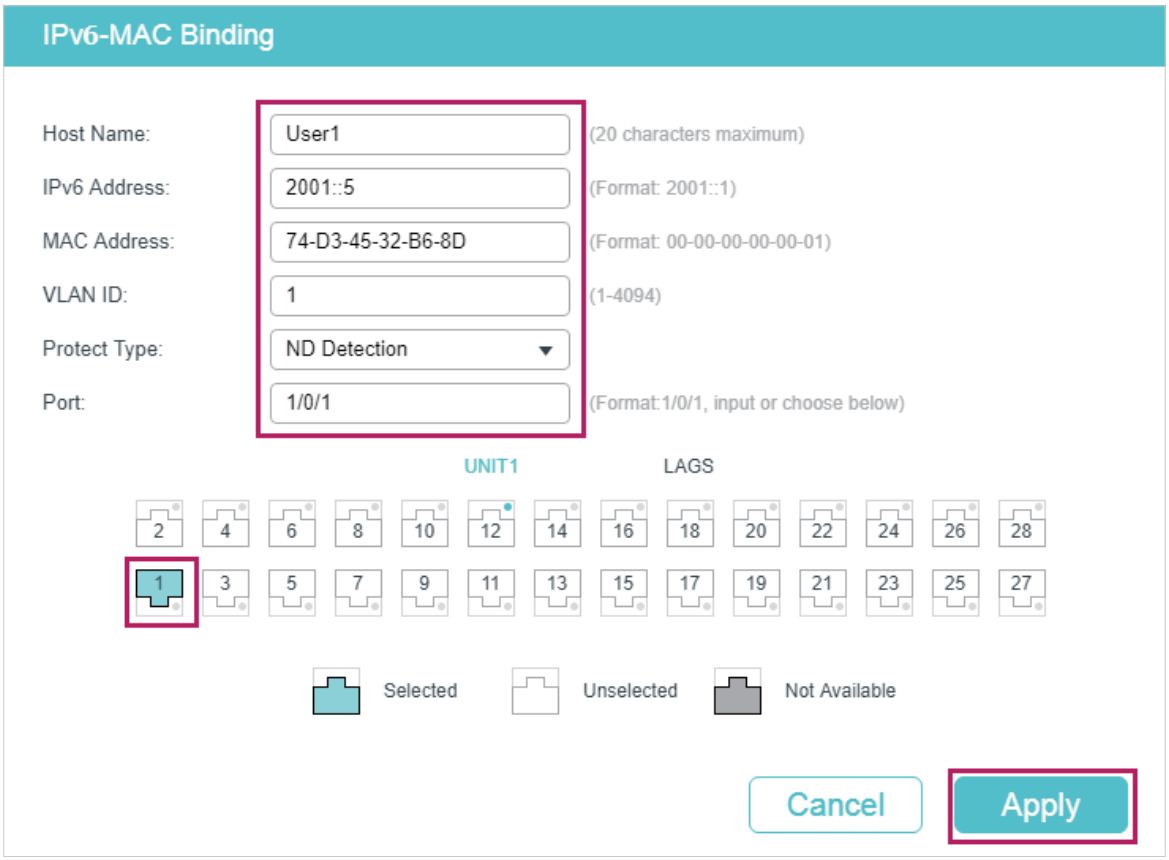
3) Configure ND Detection on ports. Since port 1/0/3 is connected to the gateway router, set port 1/0/3 as trusted port.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.1.3 Using the GUI

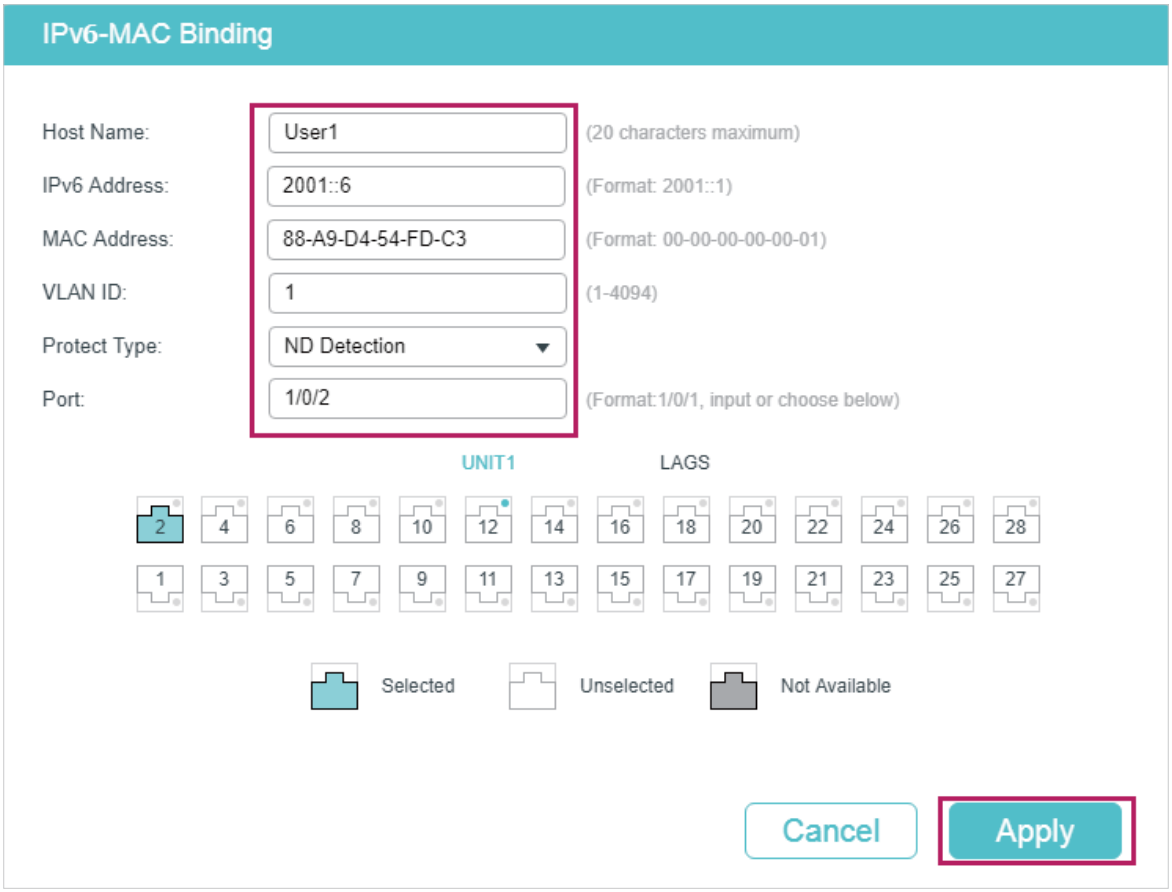
1) Choose the menu **SECURITY > IPv6 IMBP > IPv6-MAC Binding > Manual Binding** and click Add to load the following page. Enter the host name, IPv6 address, MAC address and VLAN ID of User 1, select the protect type as ND Detection, and select port 1/0/1 on the panel. Click **Apply**.

Figure 5-2 Binding Entry for User 1



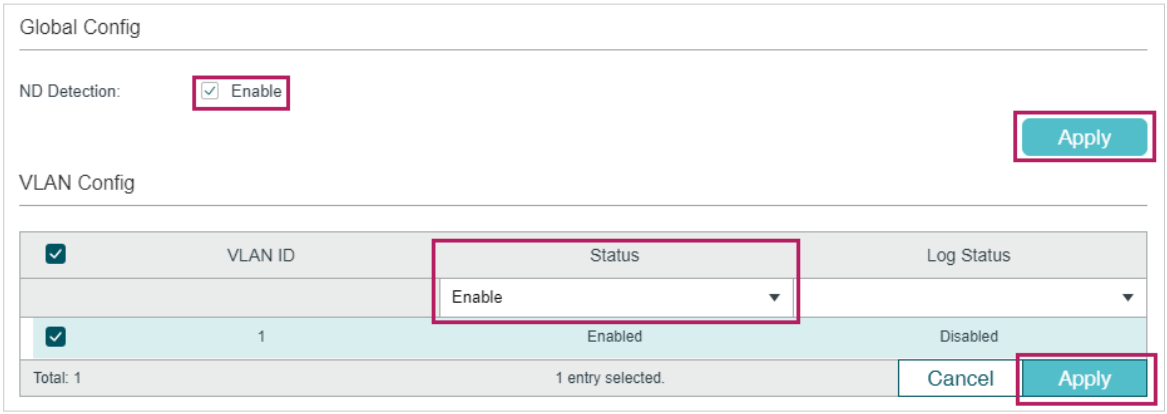
2) In the same way, add a binding entry for User 2. Enter the host name, IPv6 address, MAC address and VLAN ID of User 2, select the protect type as ND Detection, and select port 1/0/2 on the panel. Click **Apply**.

Figure 5-3 Binding Entry for User 2



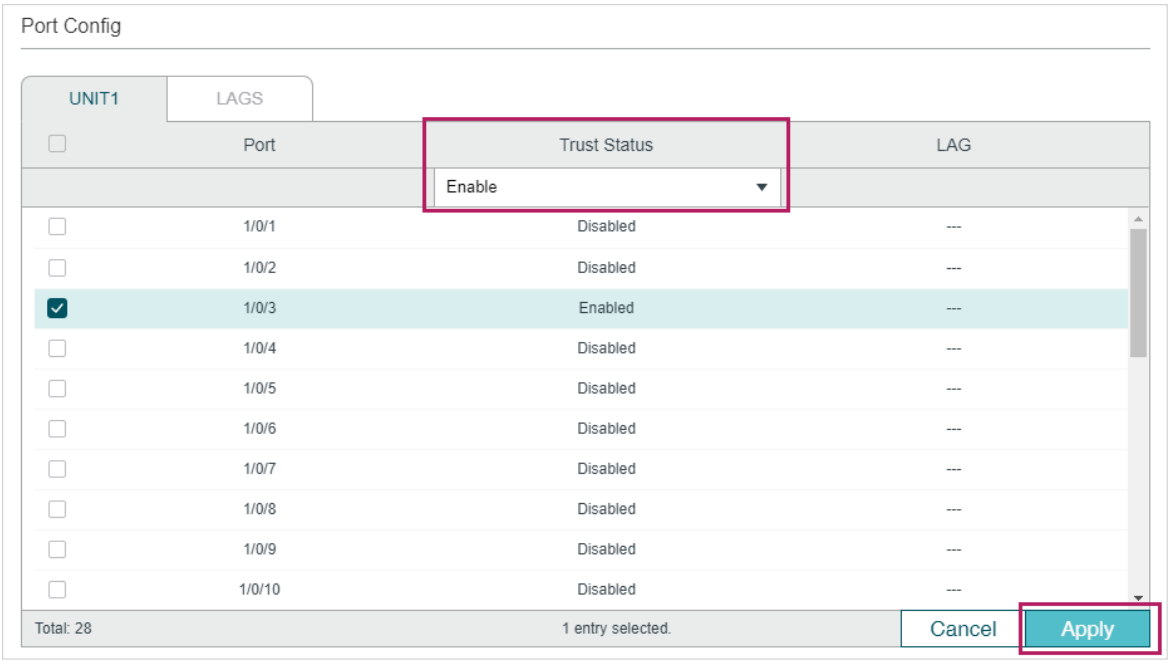
3) Choose the menu **SECURITY > IPv6 IMBP > ND Detection > Global Config** to load the following page. Enable ND Detection and click **Apply**. Select VLAN 1, change Status as Enabled and click **Apply**.

Figure 5-4 Enable ND Detection



4) Choose the menu **SECURITY > IPv6 IMBP > ND Detection > Port Config** to load the following page. By default, all ports are enabled with ND Detection. Since port 1/0/3 is connected to the gateway router, configure port 1/0/3 as trusted port. Click **Apply**.

Figure 5-5 Port Config



5) Click Save to save the settings.

5.1.4 Using the CLI

1) Manually bind the entries for User 1 and User 2.

   Switch_A#configure

   Switch_A(config)#ipv6 source binding User1 2001::5 74:d3:45:32:b6:8d vlan 1 interface gigabitEthernet 1/0/1 nd-detection

   Switch_A(config)#ip source binding User1 2001::6 88:a9:d4:54:fd:c3 vlan 1 interface gigabitEthernet 1/0/2 nd-detection

2) Enable ND Detection globally and on VLAN 1.

   Switch_A(config)#ipv6 nd detection vlan 1

3) Configure port 1/0/3 as trusted port.

   Switch_A(config)#interface gigabitEthernet 1/0/3

   Switch_A(config-if)#ipv6 nd detection trust

   Switch_A(config-if)#end

   Switch_A#copy running-config startup-config

Verify the Configuration

Verify the IPv6-MAC Binding entries:

Switch_A#show ipv6 source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	User1	2001::5	74:d3:45:32:b6:8d	1	Gi1/0/1	ND-D	Manual
1	User2	2001::6	88:a9:d4:54:fd:c3	1	Gi1/0/2	ND-D	Manual

Notice:

1.Here, 'ND-D' for 'ND-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Verify the global configuration of ND Detection:

Switch_A#show ipv6 nd detection

Global Status: Enable

Verify the ND Detection configuration on VLAN:

Switch_A#show ipv6 nd detection vlan

VID	Enable status	Log Status
----	----------	----------
1	Enable	Disable

Verify the ND Detection configuration on ports:

Switch_A#show ipv6 nd detection interface

Interface	Trusted	LAG
---------	----------	---
Gi1/0/1	Disable	N/A
Gi1/0/2	Disable	N/A
Gi1/0/3	Enable	N/A

...

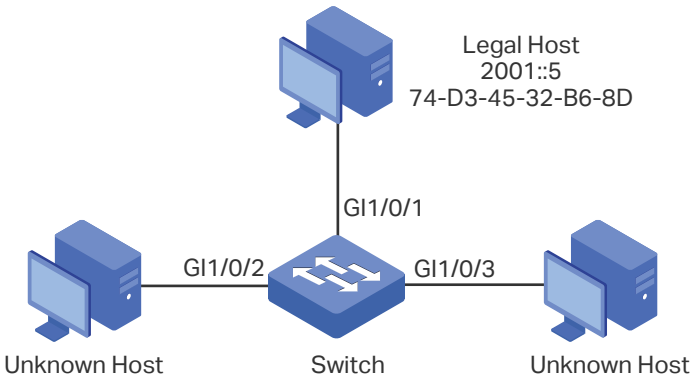
5.2 Example for IPv6 Source Guard

5.2.1 Network Requirements

As shown below, the legal IPv6 host connects to the switch via port 1/0/1 and belongs to the default VLAN 1. It is required that only the legal host can access the network via port

1/0/1, and other unknown hosts will be blocked when trying to access the network via ports 1/0/1-3.

Figure 5-6 Network Topology



5.2.2 Configuration Scheme

To implement this requirement, you can use IPv6-MAC Binding and IPv6 Source Guard to filter out the packets received from the unknown hosts. The overview of configuration on the switch is as follows:

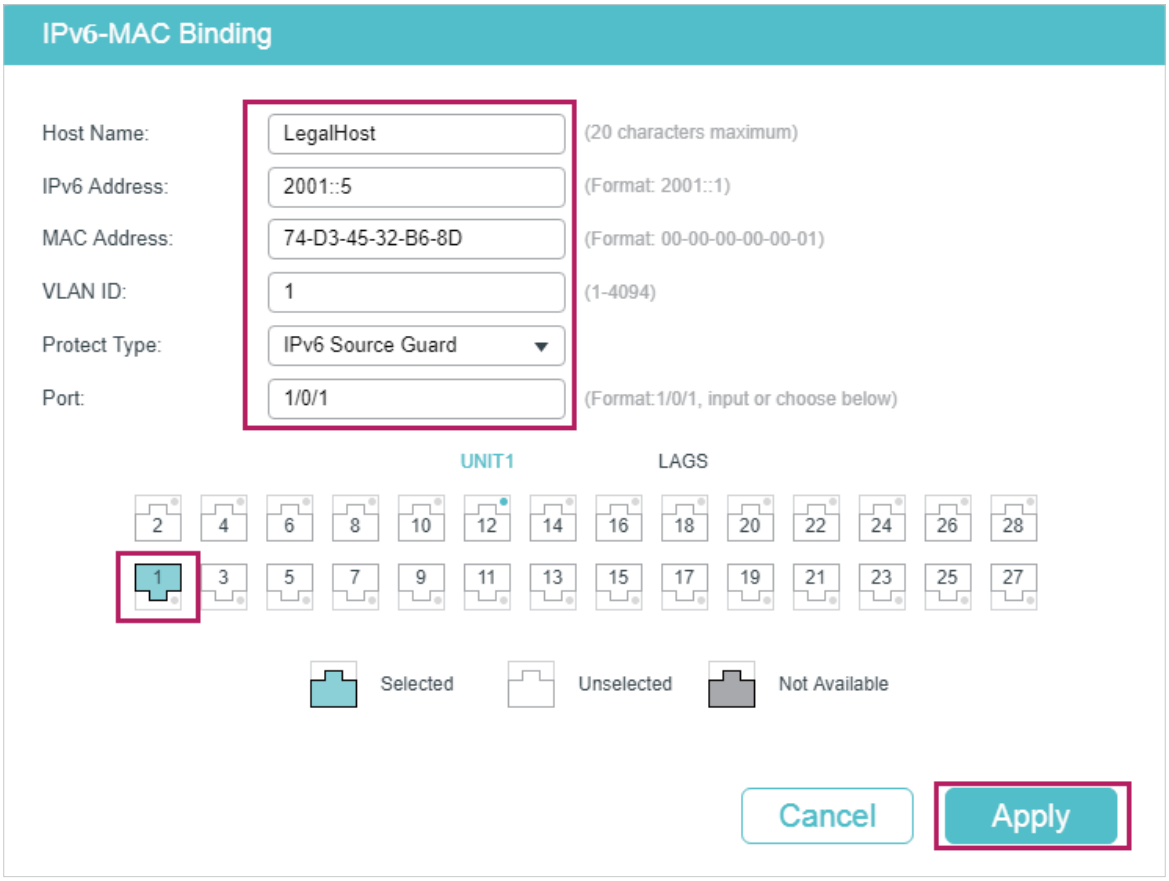
1) Bind the MAC address, IPv6 address, connected port number and VLAN ID of the legal host with IPv6-MAC Binding.
2) Enable IPv6 Source Guard on ports 1/0/1-3.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.2.3 Using the GUI

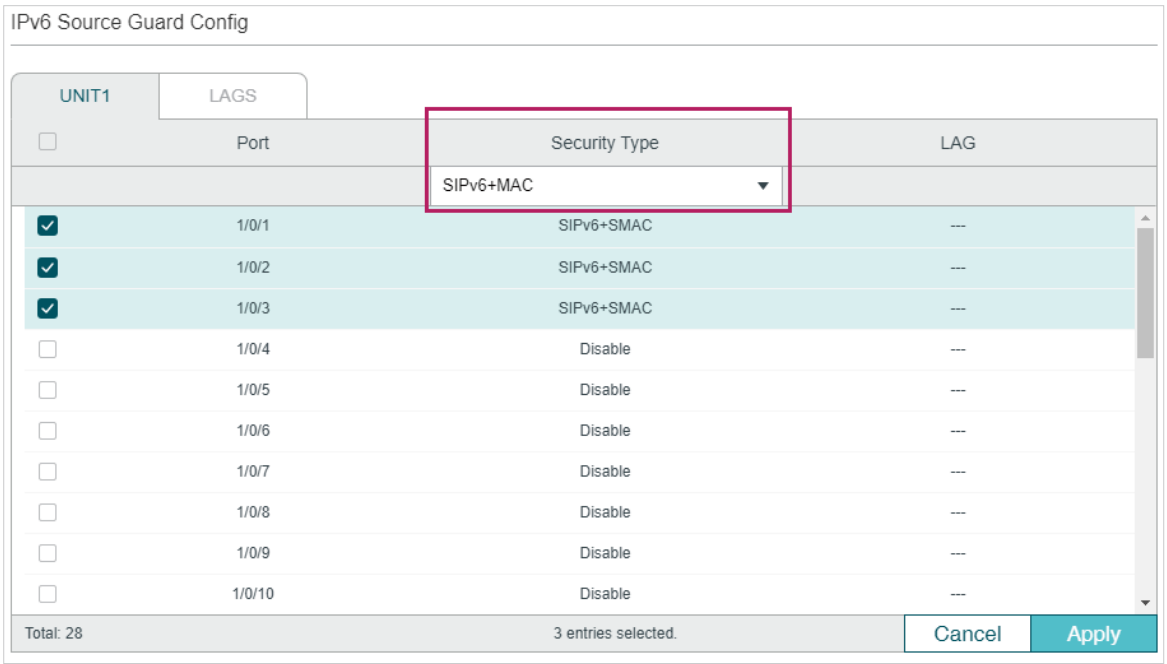
1) Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Manual Binding** and click Add to load the following page. Enter the host name, IPv6 address, MAC address and VLAN ID of the legal host, select the protect type as , and select port 1/0/1 on the panel. Click **Apply**.

Figure 5-7 Manual Binding



2) Choose the menu **SECURITY > IPv6 IMPB > IPv6 Source Guard** to load the following page. Select ports 1/0/1-3, configure the Security Type as SIPv6+MAC, and click **Apply**.

Figure 5-8 IPv6 Source Guard



3) Click Save to save the settings.

5.2.4 Using the CLI

1) Manually bind the IPv6 address, MAC address, VLAN ID and connected port number of the legal host, and apply this entry to the IPv6 Source Guard feature.

   Switch#configure

   Switch(config)#ipv6 source binding legal-host 2001::5 74:d3:45:32:b6:8d vlan 1 interface gigabitEthernet 1/0/1 ipv6-verify-source

2) Enable IPv6 Source Guard on ports 1/0/1-3.

   Switch(config)# ipv6 verify source

   Switch(config)# interface range gigabitEthernet 1/0/1-3

   Switch(config-if-range)#ipv6 verify source sipv6+mac

   Switch(config-if-range)#end

   Switch#copy running-config startup-config

Verify the Configuration

Verify the binding entry:

Switch#show ip source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	legal-host	2001::5	74:d3:45:32:b6:8d	1	Gi1/0/1	IP-V-S	Manual

Notice:

1.Here, 'ND-D' for 'ND-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Verify the configuration of IPv6 Source Guard:

Switch#show ipv6 verify source

Port	Security-Type	LAG
Gi1/0/1	SIPv6+MAC	N/A
Gi1/0/2	SIPv6+MAC	N/A
Gi1/0/3	SIPv6+MAC	N/A

...

6 Appendix: Default Parameters

Default settings of DHCP Snooping are listed in the following table:

Table 6-1 DHCPv6 Snooping

Parameter	Default Setting
Global Config	
DHCPv6 Snooping	Disabled
VLAN Config	
Status	Disabled
Port Config	
Maximum Entry	512

Default settings of ND Detection are listed in the following table:

Table 6-2 ND Detection

Parameter	Default Setting
Global Config	
ND Detection	Disabled
VLAN Config	
Status	Disabled
Log Status	Disabled
Port Config	
Trust Status	Disabled
ND Statistics	
Auto Refresh	Disabled
Refresh Interval	5 seconds

Default settings of IPv6 Source Guard are listed in the following table:

Table 6-3 ND Detection

Parameter	Default Setting
Port Config	
Security Type	Disabled

Part 30

Configuring DHCP Filter

CHAPTERS

1. DHCP Filter
2. DHCPv4 Filter Configuration
3. DHCPv6 Filter Configuration
4. Configuration Examples
5. Appendix: Default Parameters

1 DHCP Filter

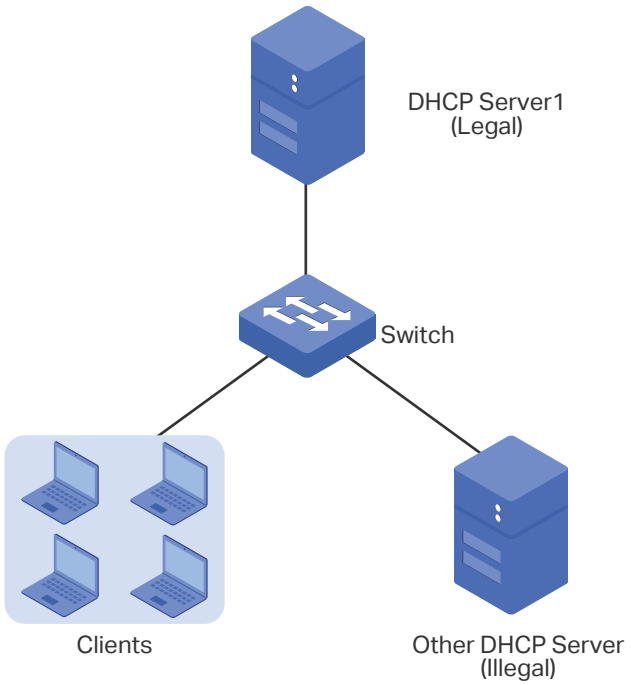
1.1 Overview

During the working process of DHCP, generally there is no authentication mechanism between the DHCP server and the clients. If there are several DHCP servers on the network, security problems and network interference will happen. DHCP Filter resolves this problem.

With DHCP Filter configured, the switch can check whether the received DHCP packets are legal and discard the illegal ones. In this way, DHCP Filter ensures that users get IP addresses only from the legal DHCP server and enhances the network security.

As the following figure shows, there are both legal and illegal DHCP servers on the network. You can configure DHCP Server1 as a legal DHCP server by providing the IP address and port number of DHCP Server1. When receiving the DHCP respond packets, the switch will forward the packets from the legal DHCP server.

Figure 1-1 Network Topology



Additionally, you can limit the forwarding rate of DHCP packets on each port.

1.2 Supported Features

The switch supports DHCPv4 Filter and DHCPv6 Filter.

DHCPv4 Filter

DHCPv4 Filter is used for DHCPv4 servers and IPv4 clients.

DHCPv6 Filter

DHCPv6 Filter is used for DHCPv6 servers and IPv6 clients.

2 DHCPv4 Filter Configuration

To complete DHCPv4 Filter configuration, follow these steps:

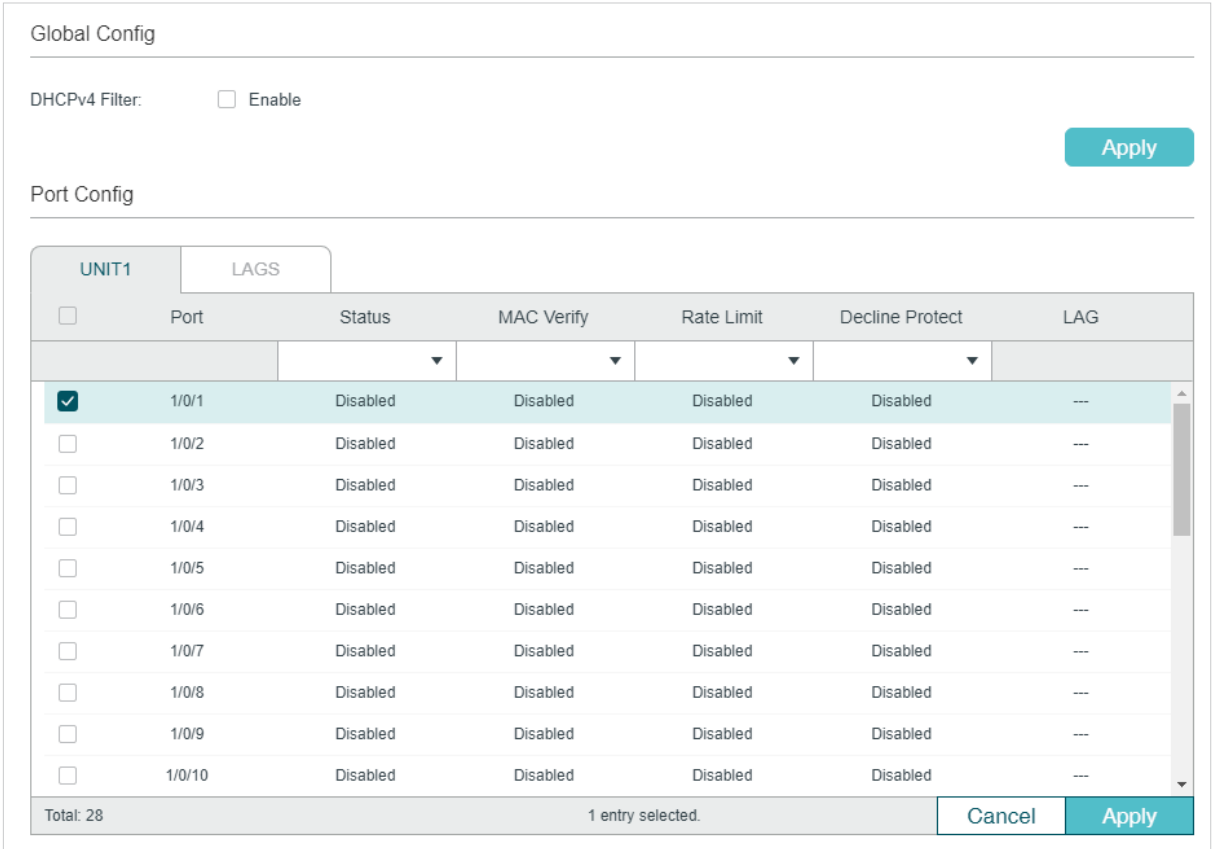
1) Configure the basic DHCPv4 Filter parameters.
2) Configure legal DHCPv4 servers.

2.1 Using the GUI

2.1.1 Configuring the Basic DHCPv4 Filter Parameters

Choose the menu **SECURITY > DHCP Filter > DHCPv4 Filter > Basic Config** to load the following page.

Figure 2-1 DHCPv4 Filter Basic Config



Follow these steps to complete the basic settings of DHCPv4 Filter:

1) In the **Global Config** section, enable DHCPv4 globally.
2) In the **Port Config** section, select one or more ports and configure the related parameters.

Port	Displays the port number.
Status	Enable or disable DHCPv4 Filter feature on the port.
MAC Verify	Enable or disable the MAC Verify feature. There are two fields in the DHCPv4 packet that contain the MAC address of the host. The MAC Verify feature compares the two fields of a DHCPv4 packet and discards the packet if the two fields are different. This prevents the IP address resource on the DHCPv4 server from being exhausted by forged MAC addresses.
Rate Limit	Select to enable the rate limit feature and specify the maximum number of DHCPv4 packets that can be forwarded on the port per second. The excessive DHCPv4 packets will be discarded.
Decline Protect	Select to enable the decline protect feature and specify the maximum number of Decline packets that can be forwarded on the port per second. The excessive Decline packets will be discarded.
LAG	Displays the LAG that the port is in.

3) Click **Apply**.

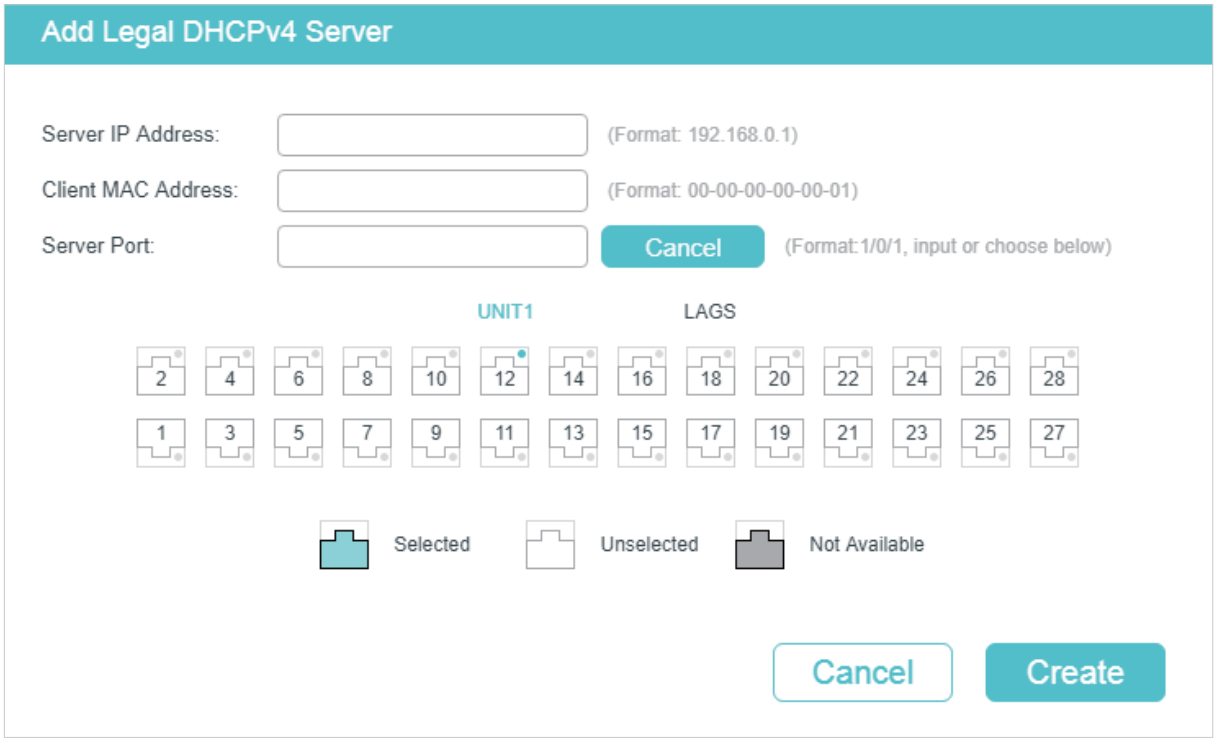
Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and not its own. The configurations of the port can take effect only after it leaves the LAG.

2.1.2 Configuring Legal DHCPv4 Servers

Choose the menu **SECURITY > DHCP Filter > DHCPv4 Filter > Legal DHCPv4 Servers** and click Add to load the following page.

Figure 2-2 Adding Legal DHCPv4 Server



Follow these steps to add a legal DHCPv4 server:

1) Configure the following parameters:

Server IP Address	Specify the IP address of the legal DHCPv4 server.
Client MAC Address	(Optional) Specify the MAC address of the DHCP Client. You can also keep this field empty, which represents for all DHCP clients.
Server Port	Select the port that the legal DHCPv4 server is connected.

2) Click **Create**.

2.2 Using the CLI

2.2.1 Configuring the Basic DHCPv4 Filter Parameters

Follow these steps to complete the basic settings of DHCPv4 Filter:

Step 1	**configure** Enter global configuration mode.

Step 2	**ip dhcp filter** Enable DHCPv4 Filter globally.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 4	**ip dhcp filter** Enable DHCPv4 Filter on the port.
Step 5	**ip dhcp filter mac-verify** Enable the MAC Verify feature. There are two fields in the DHCP packet that contain the MAC address of the host. The MAC Verify feature compares the two fields of a DHCP packet and discards the packet if the two fields are different. This prevents the IP address resource on the DHCP server from being exhausted by forged MAC addresses.
Step 6	**ip dhcp filter limit rate** *value* Enable the limit rate feature and specify the maximum number of DHCP messages that can be forwarded on the port per second. The excessive DHCP packets will be discarded. *value:* Specify the limit rate value. The following options are provided: 0, 5,10,15,20,25 and 30 (packets/second). The default value is 0, which indicates disabling limit rate.
Step 7	**ip dhcp filter decline rate** *value* Enable the decline protect feature and specify the maximum number of Decline packets can be forwarded per second on the port. The excessive Decline packets will be discarded. *value:* Specify the limit rate value of Decline packets. The following options are provided: 0, 5,10,15,20,25 and 30 (packets/second). The default value is 0, which indicates disabling this feature.
Step 8	**show ip dhcp filter** Verify the global DHCPv4 Filter configuration.
Step 9	**show ip dhcp filter interface** [**fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id*] Verify the DHCPv4 Filter configuration of the port.
Step 10	**end** Return to privileged EXEC mode.
Step 11	**copy running-config startup-config** Save the settings in the configuration file.

Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and not its own. The configurations of the port can take effect only after it leaves the LAG.

The following example shows how to enable DHCPv4 Filter globally and how to enable DHCPv4 Filter, enable the MAC verify feature, set the limit rate as 10 pps and set the decline rate as 20 pps on port 1/0/1:

Switch#configure

Switch(config)#ip dhcp filter

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip dhcp filter

Switch(config-if)#ip dhcp filter mac-verify

Switch(config-if)#ip dhcp filter limit rate 10

Switch(config-if)#ip dhcp filter decline rate 20

Switch(config-if)##show ip dhcp filter

Global Status: Enable

Switch(config-if)#show ip dhcp filter interface gigabitEthernet 1/0/1

Interface	state	MAC-Verify	Limit-Rate	Dec-rate	LAG
---	---	---	---	---	---
Gi1/0/1	Enable	Enable	10	20	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.2 Configuring Legal DHCPv4 Servers

Follow these steps configure legal DHCPv4 servers:

Step 1	**configure** Enter global configuration mode.

Step 2	**ip dhcp filter server permit-entry server-ip** *ipAddr* **client-mac** macAddr **interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}** Create an entry for the legal DHCPv4 server. *ipAddr*: Specify the IP address of the legal DHCPv4 server. macAddr : Specify the MAC address of the DHCP Client. The value "all" means all client mac addresses. *port-list* | *port-channel-id*: Specify the port that the legal DHCPv4 server is connected to.
Step 3	**show ip dhcp filter server permit-entry** Verify configured legal DHCPv4 server information.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an entry for the legal DHCPv4 server whose IP address is 192.168.0.100 and connected port number is 1/0/1 without client MAC address restricted:

Switch#configure

Switch(config)#ip dhcp filter server permit-entry server-ip 192.168.0.100 **client-mac** all **interface gigabitEthernet** 1/0/1

Switch(config)#show ip dhcp filter server permit-entry

Server IP Client MAC Interface

--- --- ---

192.168.0.100 all Gi1/0/1

Switch(config)#end

Switch#copy running-config startup-config

3 DHCPv6 Filter Configuration

To complete DHCPv6 Filter configuration, follow these steps:

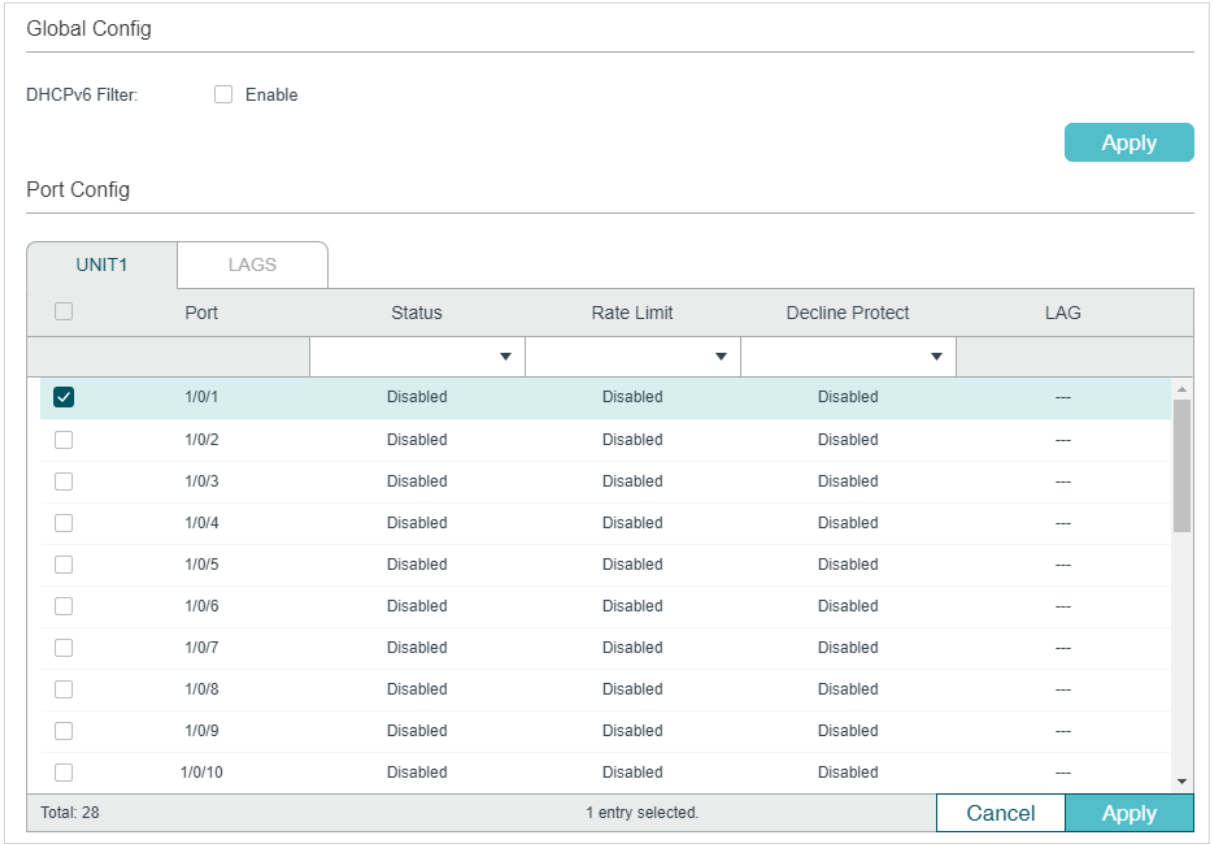
1) Configure the basic DHCPv6 Filter parameters.
2) Configure legal DHCPv6 servers.

3.1 Using the GUI

3.1.1 Configuring the Basic DHCPv6 Filter Parameters

Choose the menu **SECURITY > DHCP Filter > DHCPv6 Filter > Basic Config** to load the following page.

Figure 3-1 DHCPv6 Filter Basic Config



Follow these steps to complete the basic settings of DHCPv6 Filter:

1) In the **Global Config** section, enable DHCPv6 globally.
2) In the **Port Config** section, select one or more ports and configure the related parameters.

Port	Displays the port number.

Status	Enable or disable DHCPv6 Filter feature on the port.
Rate Limit	Select to enable the rate limit feature and specify the maximum number of DHCPv6 packets that can be forwarded on the port per second. The excessive DHCPv6 packets will be discarded.
Decline Protect	Select to enable the decline protect feature and specify the maximum number of DHCPv6 Decline packets that can be forwarded on the port per second. The excessive DHCPv6 Decline packets will be discarded.
LAG	Displays the LAG that the port is in.

3) Click **Apply**.

Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and not its own. The configurations of the port can take effect only after it leaves the LAG.

3.1.2 Configuring Legal DHCPv6 Servers

Choose the menu **SECURITY > DHCP Filter > DHCPv6 Filter > Legal DHCPv6 Servers** and click Add to load the following page.

Figure 3-2 Adding Legal DHCPv6 Server

Follow these steps to add a legal DHCPv6 server:

1) Configure the following parameters:

Server IPv6 Address	Specify the IP address of the legal DHCPv6 server.

Server Port	Select the port that the legal DHCPv6 server is connected.

2) Click **Create**.

3.2 Using the CLI

3.2.1 Configuring the Basic DHCPv6 Filter Parameters

Follow these steps to complete the basic settings of DHCPv6 Filter:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 dhcp filter** Enable DHCPv6 Filter globally.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 4	**ipv6 dhcp filter** Enable DHCPv6 Filter on the port.
Step 5	**ipv6 dhcp filter limit rate** *value* Enable the limit rate feature and specify the maximum number of DHCP messages that can be forwarded on the port per second. The excessive DHCP packets will be discarded. *value:* Specify the limit rate value. The following options are provided: 0, 5,10,15,20,25 and 30 (packets/second). The default value is 0, which indicates disabling limit rate.
Step 6	**ipv6 dhcp filter decline rate** *value* Enable the decline protect feature and specify the maximum number of Decline packets can be forwarded per second on the port. The excessive Decline packets will be discarded. *value:* Specify the limit rate value of Decline packets. The following options are provided: 0, 5,10,15,20,25 and 30 (packets/second). The default value is 0, which indicates disabling this feature.
Step 7	**show ipv6 dhcp filter** Verify the global DHCPv6 Filter configuration.
Step 8	**show ipv6 dhcp filter interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Verify the DHCPv6 Filter configuration of the port.

Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and not its own. The configurations of the port can take effect only after it leaves the LAG.

The following example shows how to enable DHCPv6 Filter globally and how to enable DHCPv6 Filter, set the limit rate as 10 pps and set the decline rate as 20 pps on port 1/0/1:

Switch#configure

Switch(config)#ipv6 dhcp filter

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 dhcp filter

Switch(config-if)#ipv6 dhcp filter limit rate 10

Switch(config-if)#ipv6 dhcp filter decline rate 20

Switch(config-if)##show ipv6 dhcp filter

Global Status: Enable

Switch(config-if)#show ip dhcp filter interface gigabitEthernet 1/0/1

Interface	state	Limit-Rate	Dec-rate	LAG
---	---	---	---	---
Gi1/0/1	Enable	10	20	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.2 Configuring Legal DHCPv6 Servers

Follow these steps configure legal DHCPv6 servers:

Step 1	**configure** Enter global configuration mode.

Step 2	**ipv6 dhcp filter server permit-entry server-ip** *ipAddr* **interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}** Create an entry for the legal DHCPv6 server. *ipAddr*: Specify the IPv6 address of the legal DHCPv6 server. *port-list* | *port-channel-id*: Specify the port that the legal DHCPv6 server is connected to.
Step 3	**show ip dhcp filter server permit-entry** Verify configured legal DHCPv6 server information.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an entry for the legal DHCPv6 server whose IPv6 address is 2001::54 and connected port number is 1/0/1:

Switch#configure

Switch(config)#ipv6 dhcp filter server permit-entry server-ip 2001::54 **interface gigabitEthernet** 1/0/1

Switch(config)#show ipv6 dhcp filter server permit-entry

Server IP Interface

---------- ---------

2001::54 Gi1/0/1

Switch(config)#end

Switch#copy running-config startup-config

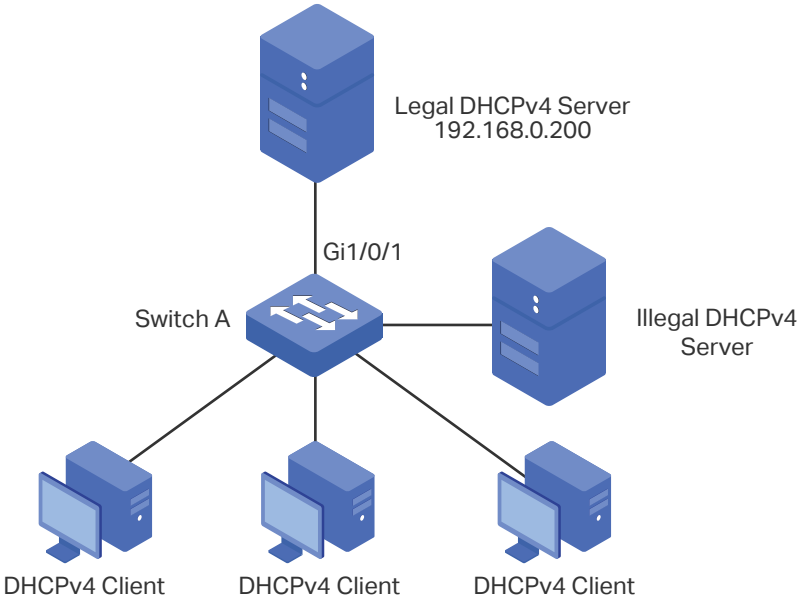
4 Configuration Examples

4.1 Example for DHCPv4 Filter

4.1.1 Network Requirements

As shown below, all the DHCPv4 clients get IP addresses from the legal DHCPv4 server, and any other DHCPv4 server in the LAN is regarded as illegal. Now it is required that only the legal DHCPv4 server is allowed to assign IP addresses to the clients.

Figure 4-1 Network Topology



4.1.2 Configuration Scheme

To meet the requirements, you can configure DHCPv4 Filter to filter the DHCPv4 packets from the illegal DHCPv4 server.

The overview of configuration is as follows:

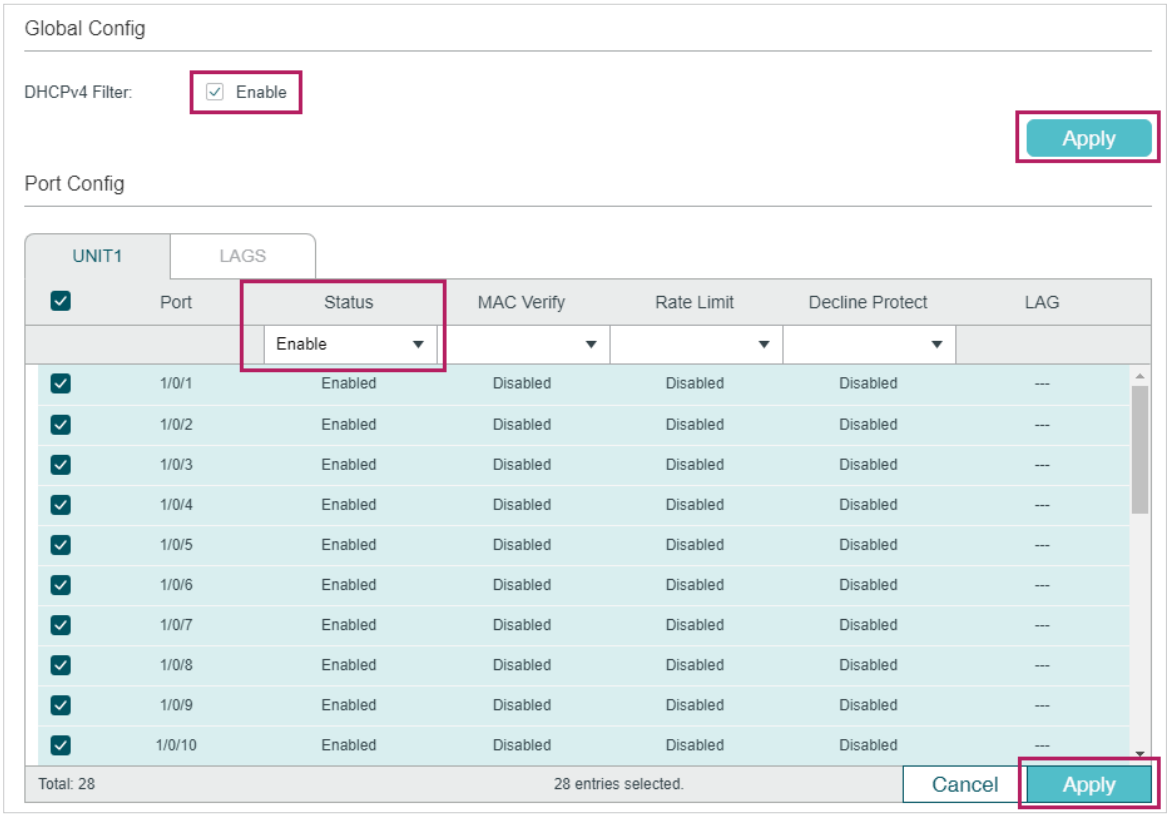
1) Enable DHCPv4 Filter globally and on all ports.
2) Create an entry for the legal DHCPv4 server.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

4.1.3 Using the GUI

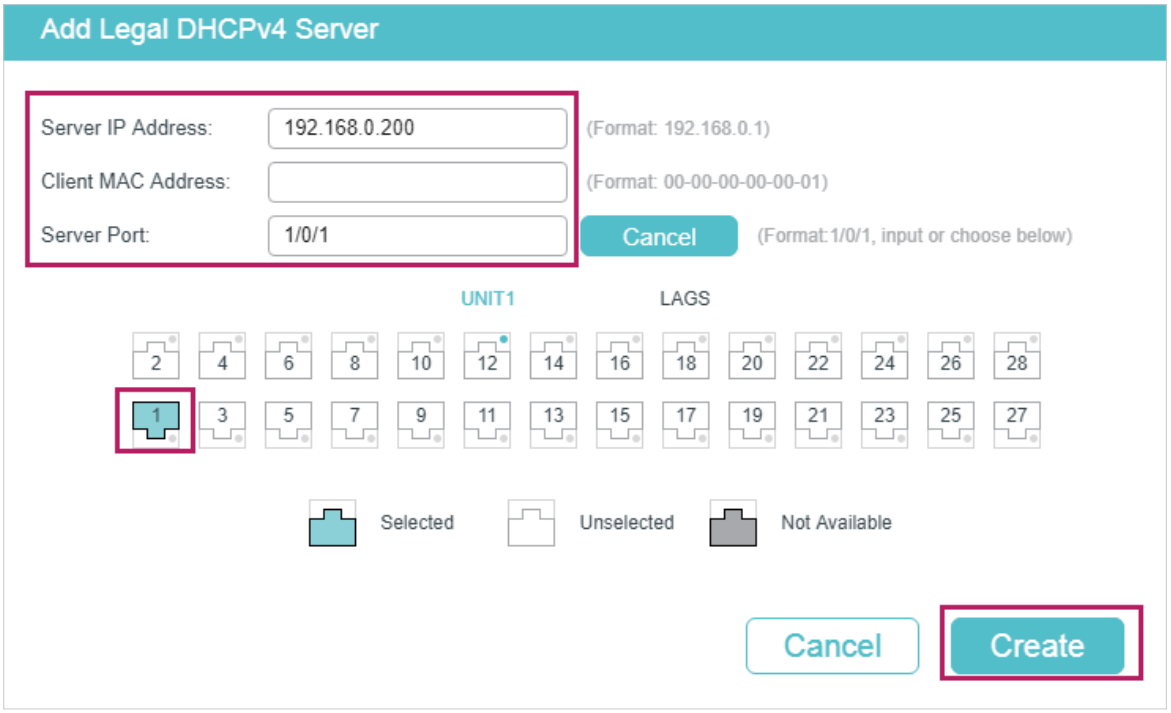
1) Choose the menu **SECURITY > DHCP Filter > DHCPv4 Filter > Basic Config** to load the following page. Enable DHCPv4 Filter globally and click **Apply**. Select all ports, change Status as Enable, and click **Apply**.

Figure 4-2 Basic Config



2) Choose the menu **SECURITY > DHCP Filter > DHCPv4 Filter > Legal DHCPv4 Servers** and click Add to load the following page. Specify the IP address and connected port number of the legal DHCPv4 server. Click **Create**.

Figure 4-3 Create Entry for Legal DHCPv4 Server



3) Click Save to save the settings.

4.1.4 Using the CLI

1) Enable DHCPv4 Filter globally and on all pots:

Switch_A#configure

Switch_A(config)#ip dhcp filter

Switch_A(config)#interface range gigabitEthernet 1/0/1-28

Switch_A(config-if-range)#ip dhcp filter

Switch_A(config-if-range)#exit

2) Create an entry for the legal DHCPv4 server:

Switch_A(config)#ip dhcp filter server permit-entry server-ip 192.168.0.200 client-mac all interface gigabitEthernet 1/0/1

Switch_A(config)#end

Switch_A#copy running-config startup-config

Verify the Configuration

Verify the global DHCPv4 Filter configuration:

Switch_A#show ip dhcp filter

Global Status: Enable

Verify the DHCPv4 Filter configuration on ports:

```
Switch_A#show ip dhcp filter interface
Interface   state     MAC-Verify  Limit-Rate      Dec-rate     LAG
---------   -------   ----------  ----------      --------     ---
Gi1/0/1     Enable    Disable     Disable         Disable      N/A
Gi1/0/2     Enable    Disable     Disable         Disable      N/A
Gi1/0/3     Enable    Disable     Disable         Disable      N/A
Gi1/0/4     Enable    Disable     Disable         Disable      N/A
...
```

Verify the legal DHCPv4 server configuration:

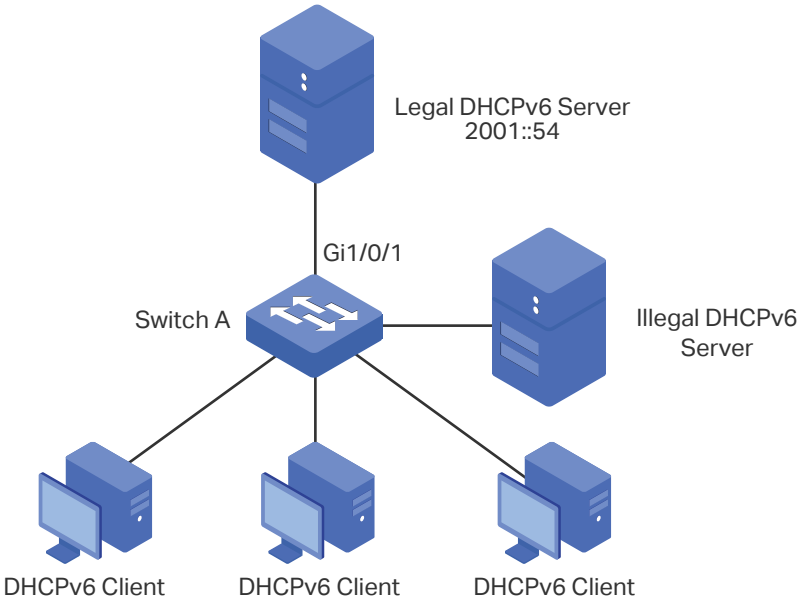
```
Switch_A#show ip dhcp filter server permit-entry
Server IP         Client MAC        Interface
---------------   ----------------  ---------
192.168.0.200     all               Gi1/0/1
```

4.2 Example for DHCPv6 Filter

4.2.1 Network Requirements

As shown below, all the DHCPv6 clients get IP addresses from the legal DHCPv6 server, and any other DHCPv6 server in the LAN is regarded as illegal. Now it is required that only the legal DHCPv6 server is allowed to assign IP addresses to the clients.

Figure 4-1 Network Topology



4.2.2 Configuration Scheme

To meet the requirements, you can configure DHCPv6 Filter to filter the DHCPv6 packets from the illegal DHCPv6 server.

The overview of configuration is as follows:

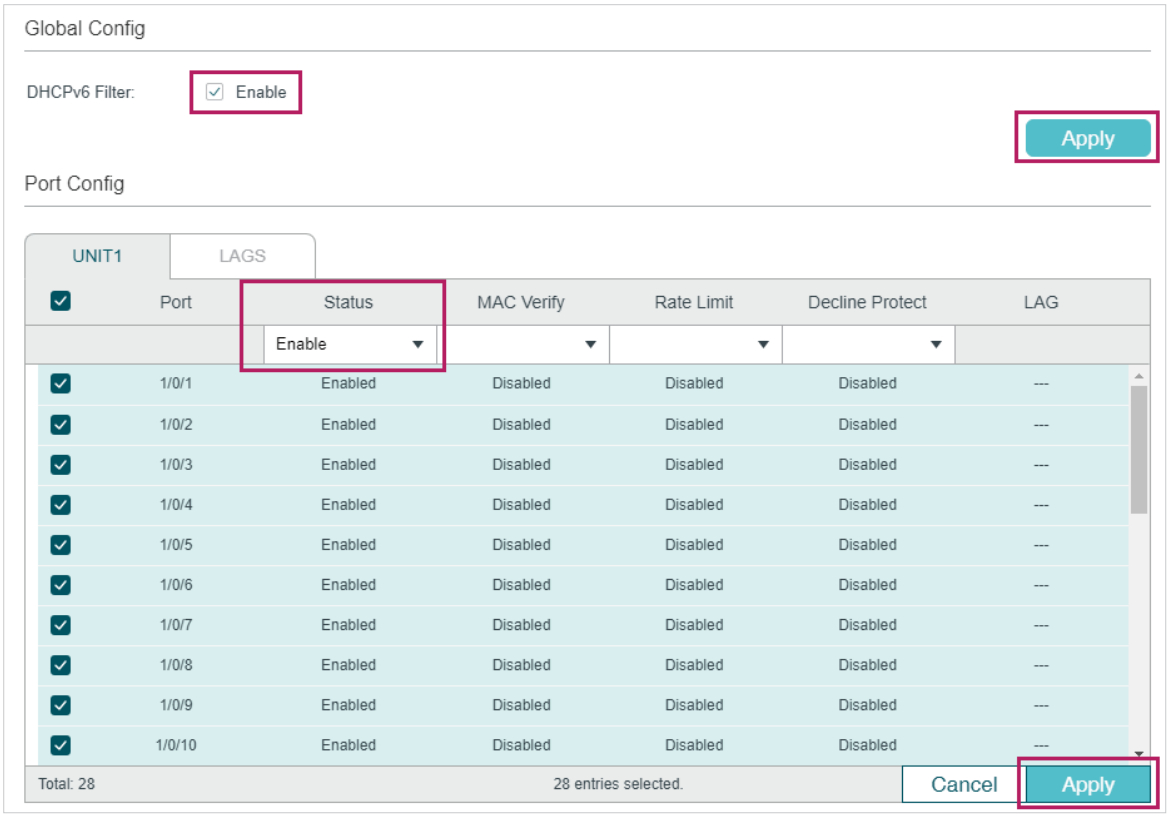
1) Enable DHCPv6 Filter globally and on all ports.
2) Create an entry for the legal DHCPv6 server.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

4.2.3 Using the GUI

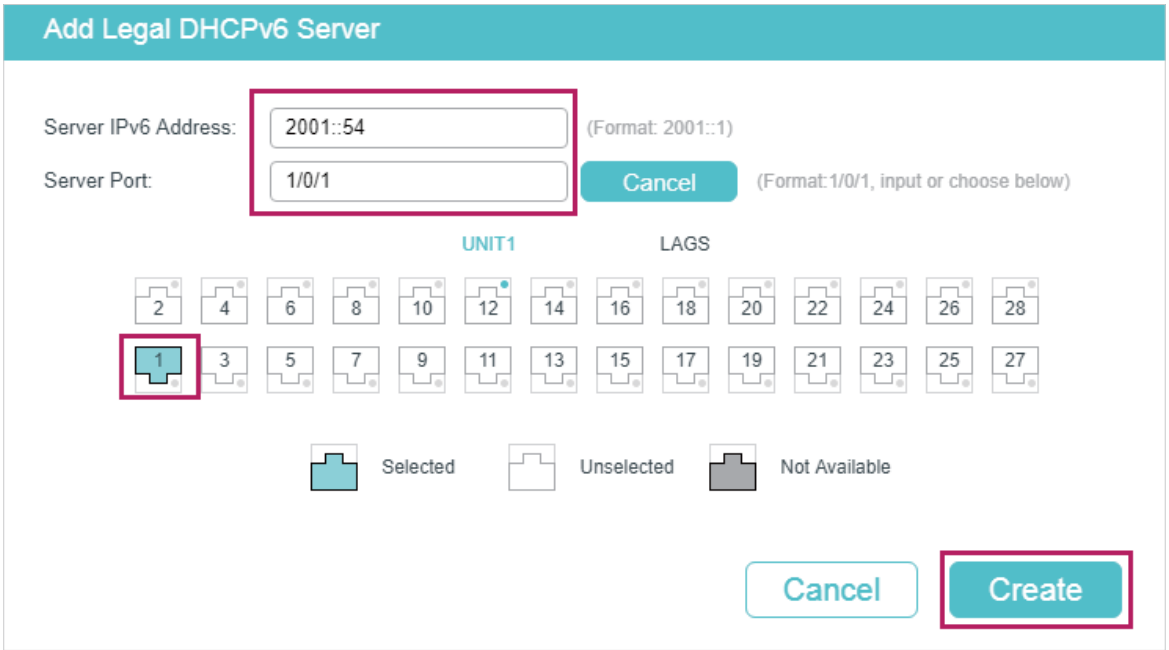
1) Choose the menu **SECURITY > DHCP Filter > DHCPv6 Filter > Basic Config** to load the following page. Enable DHCPv6 Filter globally and click **Apply**. Select all ports, change Status as Enable, and click **Apply**.

Figure 4-2 Basic Config



2) Choose the menu **SECURITY > DHCP Filter > DHCPv6 Filter > Legal DHCPv6 Servers** and click Add to load the following page. Specify the IP address and connected port number of the legal DHCPv6 server. Click **Create**.

Figure 4-3 Create Entry for Legal DHCPv6 Server



3) Click Save to save the settings.

4.2.4 Using the CLI

1) Enable DHCPv6 Filter globally and on all pots:

   Switch_A#configure

   Switch_A(config)#ipv6 dhcp filter

   Switch_A(config)#interface range gigabitEthernet 1/0/1-28

   Switch_A(config-if-range)#ipv6 dhcp filter

   Switch_A(config-if-range)#exit

2) Create an entry for the legal DHCPv6 server:

   Switch_A(config)#ipv6 dhcp filter server permit-entry server-ip 2001::54 interface gigabitEthernet 1/0/1

   Switch_A(config)#end

   Switch_A#copy running-config startup-config

Verify the Configuration

Verify the global DHCPv6 Filter configuration:

Switch_A#show ipv6 dhcp filter

Global Status: Enable

Verify the DHCPv6 Filter configuration on ports:

Switch_A#show ipv6 dhcp filter interface

Interface	state	Limit-Rate	Dec-rate	LAG
---	---	---	---	---
Gi1/0/1	Enable	Disable	Disable	N/A
Gi1/0/2	Enable	Disable	Disable	N/A
Gi1/0/3	Enable	Disable	Disable	N/A
Gi1/0/4	Enable	Disable	Disable	N/A

...

Verify the legal DHCPv6 server configuration:

Switch_A#show ipv6 dhcp filter server permit-entry

```
Server IP          Interface
----------------   ----------
2001::54           Gi1/0/1
```

5 Appendix: Default Parameters

Default settings of DHCPv4 Filter are listed in the following table:

Table 5-1 DHCPv4 Filter

Parameter	Default Setting
Global Config	
DHCPv4 Filter	Disabled
Port Config	
Status	Disabled
MAC Verify	Disabled
Rate Limit	Disabled
Decline Protect	Disabled

Table 5-2 DHCPv6 Filter

Parameter	Default Setting
Global Config	
DHCPv6 Filter	Disabled
Port Config	
Status	Disabled
Rate Limit	Disabled
Decline Protect	Disabled

Part 31

Configuring DoS Defend

CHAPTERS

1. Overview
2. DoS Defend Configuration
3. Appendix: Default Parameters

1 Overview

The DoS (Denial of Service) defend feature provides protection against DoS attacks. DoS attacks occupy the network bandwidth maliciously by sending numerous service requests to the hosts. It results in an abnormal service or breakdown of the network.

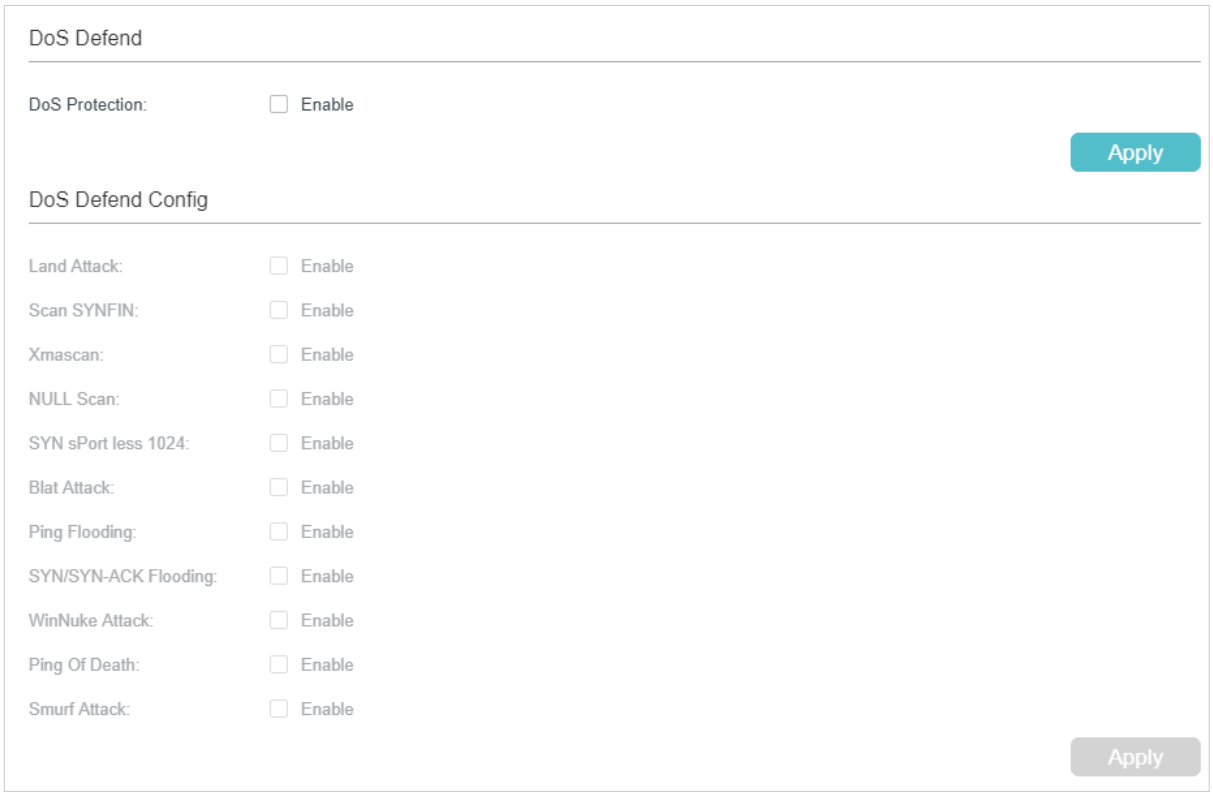
With DoS Defend feature, the switch can analyze the specific fields of the IP packets, distinguish the malicious DoS attack packets and discard them directly. Also, DoS Defend feature can limit the transmission rate of legal packets. When the number of legal packets exceeds the threshold value and may incur a breakdown of the network, the switch will discard the packets.

2 DoS Defend Configuration

2.1 Using the GUI

Choose the menu **SECURITY > DoS Defend** to load the following page.

Figure 2-1 DoS Defend



Follow these steps to configure DoS Defend:

1) In the **DoS Defend** section, enable DoS Protection and click **Apply**.
2) In the **DoS Defend Config** section, select one or more defend types according to your needs and click **Apply**. The following table introduces each type of DoS attack.

Land Attack	The attacker sends a specific fake SYN (synchronous) packet to the destination host. Because both of the source IP address and the destination IP address of the SYN packet are set to be the IP address of the host, the host will be trapped in an endless circle of building the initial connection.
Scan SYNFIN	The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal.
Xmascan	The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1.

NULL Scan	The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all control fields set to 0 are considered illegal.
SYN sPort less 1024	The attacker sends the illegal packet with its TCP SYN field set to 1 and source port smaller than 1024.
Blat Attack	The attacker sends the illegal packet with the same source port and destination port on Layer 4 and with its URG field set to 1. Similar to the Land Attack, the system performance of the attacked host is reduced because the Host circularly attempts to build a connection with the attacker.
Ping Flooding	The attacker floods the destination system with Ping packets, creating a broadcast storm that makes it impossible for the system to respond to legal communication.
SYN/SYN-ACK Flooding	The attacker uses a fake IP address to send TCP request packets to the server. Upon receiving the request packets, the server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied.
WinNuke Attack	Because the Operation System with bugs cannot correctly process the URG (Urgent Pointer) of TCP packets, the attacker sends this type of packets to the TCP port139 (NetBIOS) of the host with the Operation System bugs, which will cause the host with a blue screen.
Ping of Death	Ping of Death attack means that the attacker sends abnormal ping packets larger than 65535 bytes to cause system crash on the target computer. Note: Ping of Death is only available on certain devices.
Smurf Attack	Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. Note: Smurf Attack is only available on certain devices.

3) Click **Apply**.

2.2 Using the CLI

Follow these steps to configure DoS Defend:

Step 1	**configure** Enter global configuration mode.

Step 2	**ip dos-prevent** Globally enable the DoS defend feature.
Step 3	**ip dos-prevent type {** land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf **}** Configure one or more defend types according to your needs. The types of DoS attack are introduced as follows. land: The attacker sends a specific fake SYN (synchronous) packet to the destination host. Because both the source IP address and the destination IP address of the SYN packet are set to be the IP address of the host, the host will be trapped in an endless circle of building the initial connection. scan-synfin: The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, a packet of this type is illegal. xma-scan: The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1. null-scan: The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all the control fields set to 0 are considered as the illegal packets. port-less-1024: The attacker sends the illegal packet with its TCP SYN field set to 1 and source port smaller than 1024. blat: The attacker sends the illegal packet with the same source port and destination port on Layer 4 and with its URG field set to 1. Similar to the Land Attack, the system performance of the attacked host is reduced because the Host circularly attempts to build a connection with the attacker. ping-flood: The attacker floods the destination system with Ping packets, creating a broadcast storm that makes it impossible for system to respond to legal communication. syn-flood: The attacker uses a fake IP address to send TCP request packets to the server. Upon receiving the request packets, the server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied. win-nuke: An Operation System with bugs cannot process the URG (Urgent Pointer) of TCP packets. If the attacker sends TCP packets to port139 (NetBIOS) of the host with Operation System bugs, it will cause blue screen. ping-of-death: Ping of Death attack means that the attacker sends abnormal ping packets larger than 65535 bytes to cause system crash on the target computer. Note: Ping of Death is only available on certain devices. smurf: Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. Note: Smurf is only available on certain devices.

Step 4	**show ip dos-prevent** Verify the DoS Defend configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable the DoS Defend type named land:

Switch#configure

Switch(config)#ip dos-prevent

Switch(config)#ip dos-prevent type land

Switch(config)#show ip dos-prevent

DoS Prevention State: Enabled

Type	Status
----	------
Land Attack	Enabled
Scan SYNFIN	Disabled
Xmascan	Disabled
NULL Scan	Disabled
SYN sPort less 1024	Disabled
Blat Attack	Disabled
Ping Flooding	Disabled
SYN/SYN-ACK Flooding	Disabled
WinNuke Attack	Disabled
Smurf Attack	Disabled
Ping Of Death	Disabled

Switch(config)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

Default settings of Network Security are listed in the following tables.

Table 3-1 DoS Defend

Parameter	Default Setting
DoS Defend	Disabled

Part 32

Monitoring the System

CHAPTERS

1. Overview
2. Monitoring the CPU
3. Monitoring the Memory

1 Overview

With System Monitor function, you can:

- Monitor the CPU utilization of the switch.
- Monitor the memory utilization of the switch.

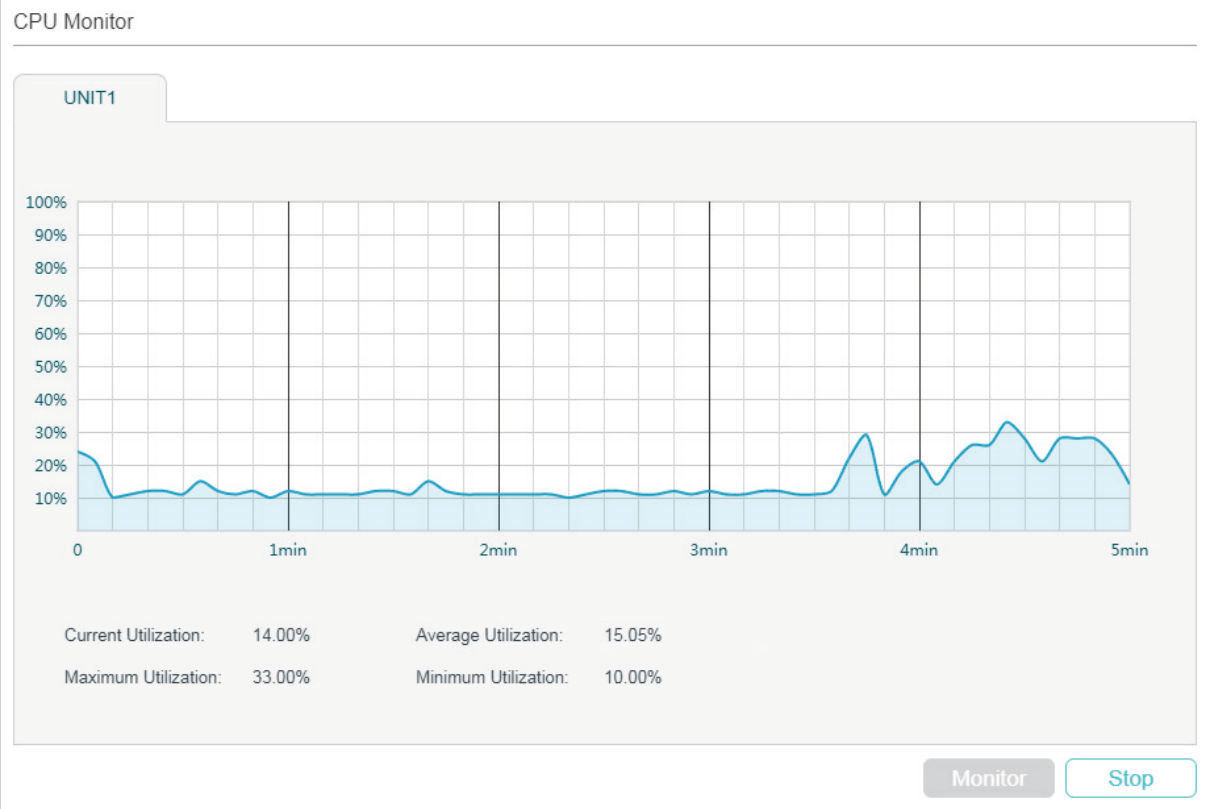
The CPU utilization should be always under 80%, and excessive use may result in switch malfunctions. For example, the switch fails to respond to management requests (ICMP ping, SNMP timeouts, slow Telnet or SSH sessions). You can monitor the system to verify a CPU utilization problem.

2 Monitoring the CPU

2.1 Using the GUI

Choose the menu **MAINTENANCE > System Monitor > CPU Monitor** to load the following page.

Figure 2-1 Monitoring the CPU



Click **Monitor** to enable the switch to monitor and display its CPU utilization rate every five seconds.

2.2 Using the CLI

On privileged EXEC mode or any other configuration mode, you can use the following command to view the CPU utilization:

show cpu-utilization

View the memory utilization of the switch in the last 5 seconds, 1minute and 5minutes.

The following example shows how to monitor the CPU:

Switch#show cpu-utilization

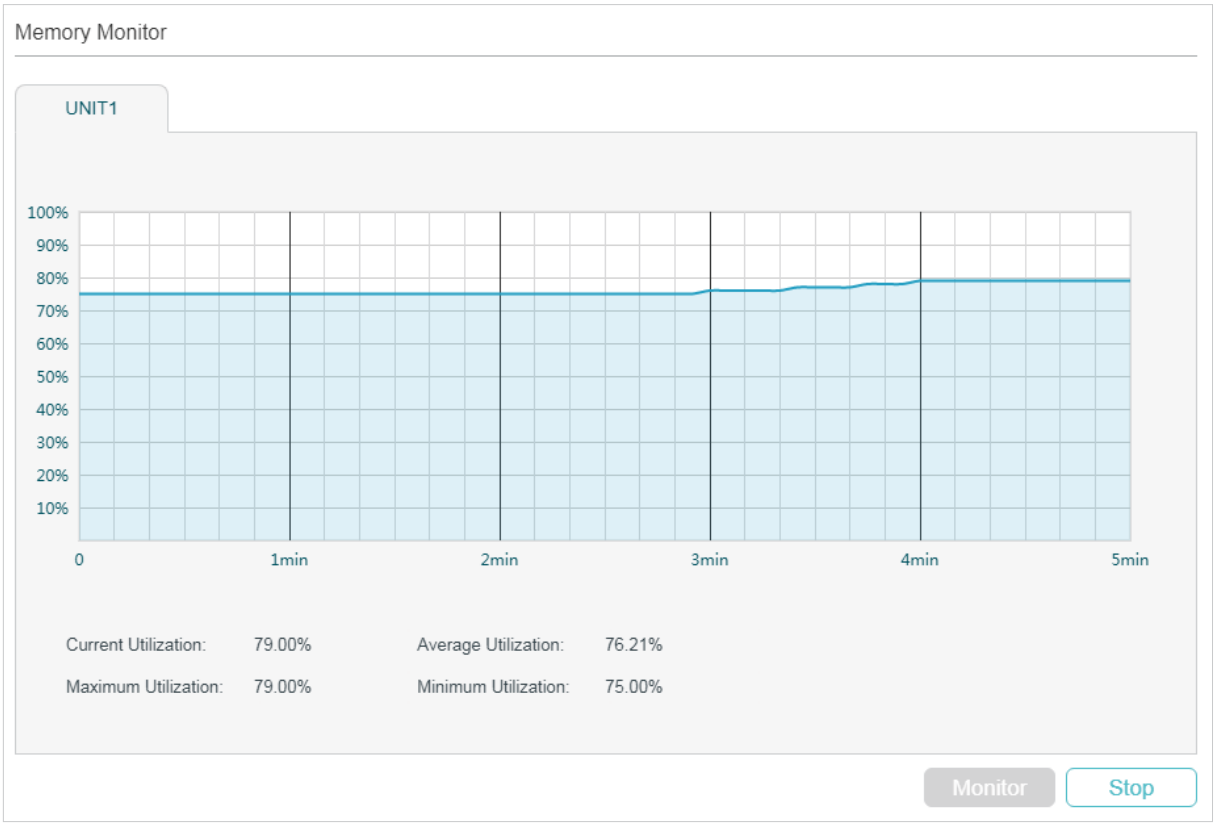
```
Unit   |                CPU Utilization
No.    |  Five-Seconds  One-Minute  Five-Minutes
------+-----------------------------------------------
1      |  13%           13%         13%
```

3 Monitoring the Memory

3.1 Using the GUI

Choose the menu **MAINTENANCE > System Monitor > Memory Monitor** to load the following page.

Figure 3-1 Monitoing the Memory



Click **Monitor** to enable the switch to monitor and display its memory utilization rate every five seconds.

3.2 Using the CLI

On privileged EXEC mode or any other configuration mode, you can use the following command to view the memory utilization:

show memory-utilization

View the current memory utilization of the switch.

The following example shows how to monitor the memory:

Switch#show memory-utilization

```
Unit   |   Current Memory Utilization
------+--------------------------
1      |   74%
```

Part 33

Monitoring Traffic

CHAPTERS

1. Traffic Monitor
2. Appendix: Default Parameters

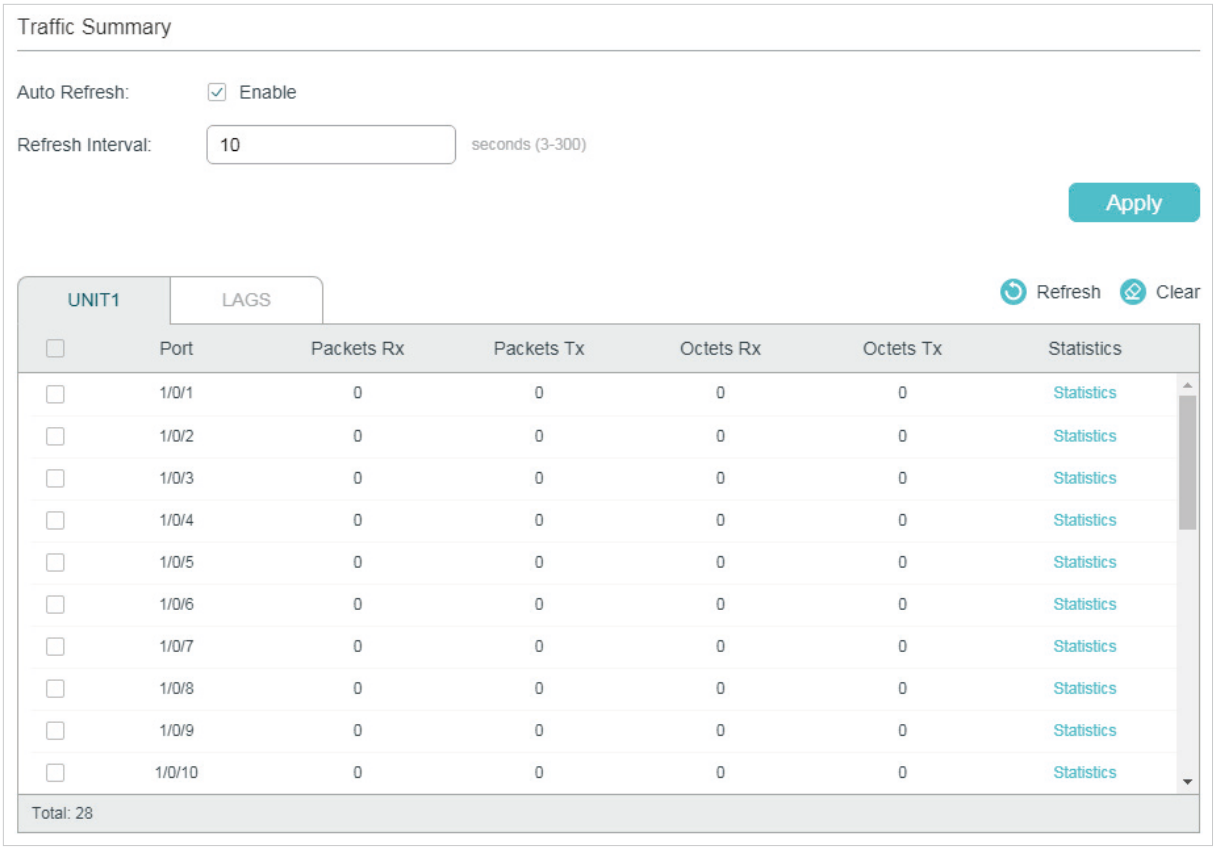
1 Traffic Monitor

With Traffic Monitor function, you can monitor each port's traffic information, including the traffic summary and traffic statistics in detail.

1.1 Using the GUI

Choose the menu **MAINTENANCE > Traffic Monitor** to load the following page.

Figure 1-1 Traffic Summary



Follow these steps to view the traffic summary of each port:

1) To get the real-time traffic summary, enable **Auto Refresh**, or click **Refresh**.

Auto Refresh:	With this option enabled, the switch will automatically refresh the traffic summary.
Refresh Interval:	Specify the time interval for the switch to refresh the traffic summary.

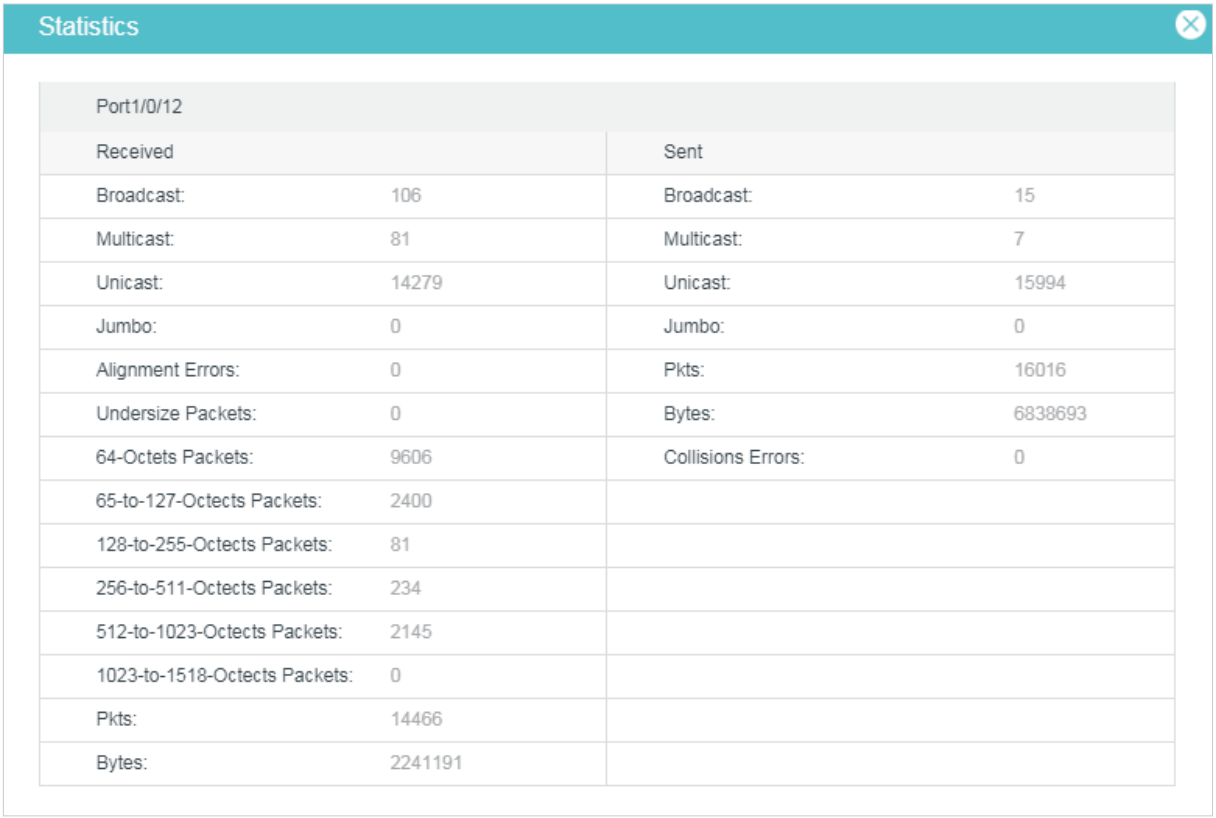
2) In the **Traffic Summary** section, click **UNIT1** to show the information of the physical ports, and click **LAGS** to show the information of the LAGs.

Packets Rx:	Displays the number of packets received on the port. Error packets are not counted.

Packets Tx:	Displays the number of packets transmitted on the port. Error packets are not counted.
Octets Rx:	Displays the number of octets received on the port. Error octets are counted.
Octets Tx:	Displays the number of octets transmitted on the port. Error octets are counted .

To view a port's traffic statistics in detail, click **Statistics** on the right side of the entry.

Figure 1-2 Traffic Statistics



Received:	Displays the detailed information of received packets. Broadcast: Displays the number of valid broadcast packets received on the port. Error frames are not counted. Multicast: Displays the number of valid multicast packets received on the port. Error frames are not counted. Unicast: Displays the number of valid unicast packets received on the port. Error frames are not counted. Jumbo: Displays the number of valid jumbo packets received on the port. Error frames are not counted. Alignment Errors: Displays the number of the received packets that have a Frame Check Sequence (FCS) with a non-integral octet (Alignment Error). The size of the packet is between 64 bytes and 1518 bytes. Undersize Packets: Displays the number of the received packets (excluding error packets) that are less than 64 bytes long. 64-Octets Packets: Displays the number of the received packets (including error packets) that are 64 bytes long. 65-to-127-Octects Packets: Displays the number of the received packets (including error packets) that are between 65 and 127 bytes long. 128-to-255-Octects Packets: Displays the number of the received packets (including error packets) that are between 128 and 255 bytes long. 256-to-511-Octects Packets: Displays the number of the received packets (including error packets) that are between 256 and 511 bytes long. 512-to-1023-Octects Packets: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long. 1023-to-1518-Octects Packets: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long. Pkts: Displays the number of packets received on the port. Error packets are not counted. Bytes: Displays the number of bytes received on the port. Error packets are not counted.

Sent:	Displays the detailed information of sent packets. Broadcast: Displays the number of valid broadcast packets transmitted on the port. Error frames are not counted. Multicast: Displays the number of valid multicast packets transmitted on the port. Error frames are not counted. Unicast: Displays the number of valid unicast packets transmitted on the port. Error frames are not counted. Pkts: Displays the number of packets transmitted on the port. Error packets are not counted. Bytes: Displays the number of bytes transmitted on the port. Error packets are not counted. Collisions: Displays the number of collisions experienced by a half-duplex port during packet transmissions.

1.2 Using the CLI

On privileged EXEC mode or any other configuration mode, you can use the following command to view the traffic information of each port or LAG:

show interface counters [fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **]**

port: The port number.

port-channel-id : The group number of the LAG.

If you enter no port number or group number, the information of all ports and LAGs will be displayed.

The displaying information includes:

Tx Collisions: Displays the number of collisions experienced by a port during packet transmissions.

Tx Ucast / Tx Mcast / Tx Bcast / Tx Jumbo: Displays the number of valid unicast / multicast / broadcast / jumbo packets transmitted on the port. Error frames are not counted.

Tx Pkts: Displays the number of packets transmitted on the port. Error packets are not counted.

Tx Bytes: Displays the number of bytes transmitted on the port. Error packets are not counted.

Rx Ucast / Rx Mcast / Rx Bcast / Rx Jumbo: Displays the number of valid unicast / multicast / broadcast / jumbo packets received on the port. Error frames are not counted.

Rx Alignment: Displays the number of the received packets that have a Frame Check Sequence (FCS) with a non-integral octet (Alignment Error). The size of the packet is between 64 bytes and 1518 bytes.

Rx UnderSize: Displays the number of the received packets (excluding error packets) that are less than 64 bytes long.

Rx 64Pkts: Displays the number of the received packets (including error packets) that are 64 bytes long.

Rx 65-127Pkts: Displays the number of the received packets (including error packets) that are between 65 and 127 bytes long.

Rx 128-255Pkts: Displays the number of the received packets (including error packets) that are between 128 and 255 bytes long.

Rx 256-511Pkts: Displays the number of the received packets (including error packets) that are between 256 and 511 bytes long.

Rx 512-1023Pkts: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long.

Rx 1024-1518Pkts: Displays the number of the received packets (including error packets) that are between 1024 and 1518 bytes long.

Rx Pkts: Displays the number of packets received on the port. Error packets are not counted.

Rx Bytes: Displays the number of bytes received on the port. Error packets are not counted.

2 Appendix: Default Parameters

Table 2-1 Traffic Statistics Monitoring

Parameter	Default Setting
Traffic Summary	
Auto Refresh	Disabled
Refresh Rate	10 seconds

Part 34

Mirroring Traffic

CHAPTERS

1. Mirroring
2. Configuration Examples
3. Appendix: Default Parameters

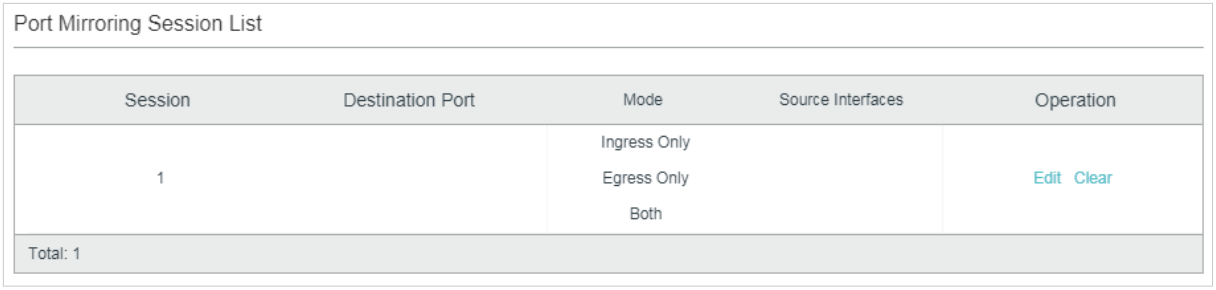
1 Mirroring

You can analyze network traffic and troubleshoot network problems using Mirroring. Mirroring allows the switch to send a copy of the traffic that passes through specified sources (ports, LAGs or the CPU) to a destination port. It does not affect the switching of network traffic on source ports, LAGs or the CPU.

1.1 Using the GUI

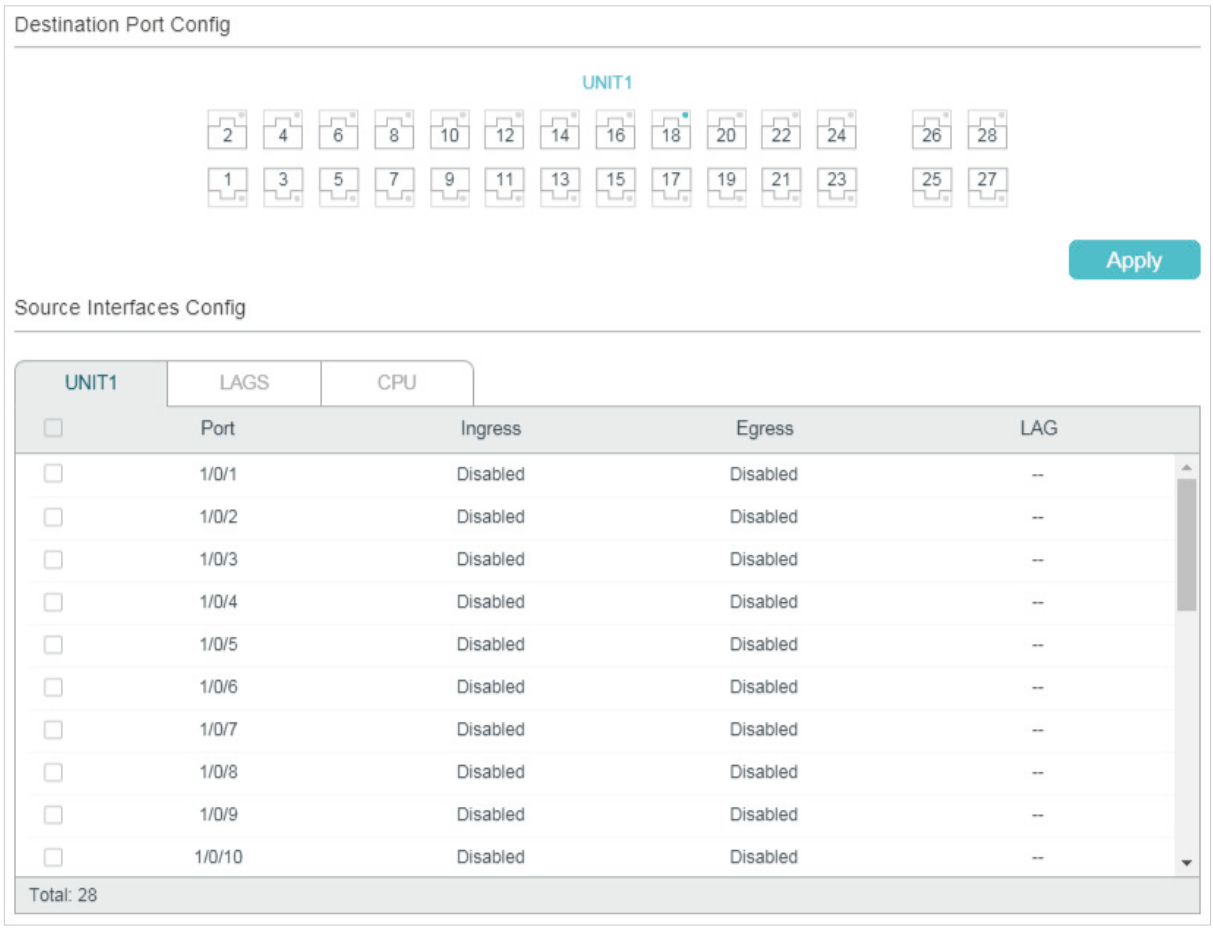
Choose the menu **MAINTENANCE > Mirroring** to load the following page.

Figure 1-1 Port Mirroring Session List



The above page displays a mirroring session, and no more session can be created. Click **Edit** to configure this mirroring session on the following page.

Figure 1-2 Configure the Mirroring Session



Follow these steps to configure the mirroring session:

1) In the **Destination Port Config** section, specify a destination port for the mirroring session, and click **Apply**.

2) In the **Source Interfaces Config** section, specify the source interfaces and click **Apply**. Traffic passing through the source interfaces will be mirrored to the destination port. There are three source interface types: port, LAG, and CPU. Choose one or more types according to your need.

UNIT1	Select the desired ports as the source interfaces. The switch will send a copy of traffic passing through the port to the destination port.
LAGS	Select the desired LAGs as the source interfaces. The switch will send a copy of traffic passing through the LAG members to the destination port.
CPU	When selected, the switch will send a copy of traffic passing through the CPU to the destination port.
Ingress	With this option enabled, the packets received by the corresponding interface (port, LAG or CPU) will be copied to the destination port. By default, it is disabled.
Egress	With this option enabled, the packets sent by the corresponding interface (port, LAG or CPU) will be copied to the destination port. By default, it is disabled.

Note:

- The member ports of an LAG cannot be set as a destination port or source port.
- A port cannot be set as the destination port and source port at the same time.

1.2 Using the CLI

Follow these steps to configure Mirroring.

Step 1	**configure** Enter global configuration mode.
Step 2	**monitor session** *session_num* **destination interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port***}** Enable the port mirror function and set the destination port. *session_num:* The monitor session number. It can only be specified as 1. *port*: The destination port number. You can specify only one destination port for the mirror session.
Step 3	**monitor session** *session_num* **source { cpu** *cpu_numbr* **| interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}}** *mode* Configure ports or LAGs as the monitored interfaces. *session_num*: The monitor session number. It can only be specified as 1. *cpu_number:* The CPU number. It can only be specified as 1. *port-list:* List of source ports. It is multi-optional. *mode*: The monitor mode. There are three options: **rx**, **tx** and **both**: **rx**: The incoming packets of the source port will be copied to the destination port. **tx**: The outgoing packets of the source port will be copied to the destination port. **both**: Both of the incoming and outgoing packets on source port can be copied to the destination port. *Note:* You can configure one or more source interface types (ports, LAGs and the CPU) according to your needs.
Step 4	**show monitor session** Verify the Port Mirror configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to copy the received and transmitted packets on port 1/0/1,2,3 and the CPU to port 1/0/10.

Switch#configure

Switch(config)#monitor session 1 **destination interface gigabitEthernet** 1/0/10

Switch(config)#monitor session 1 **source interface gigabitEthernet** 1/0/1-3 both

Switch(config)#monitor session 1 **source cpu** 1 both

Switch(config)#show monitor session

Monitor Session: 1

Destination Port: Gi1/0/10

Source Ports(Ingress): Gi1/0/1-3

Source Ports(Egress): Gi1/0/1-3

Source CPU(Ingress): cpu1

Source CPU(Egress): cpu1

Switch(config-if)#end

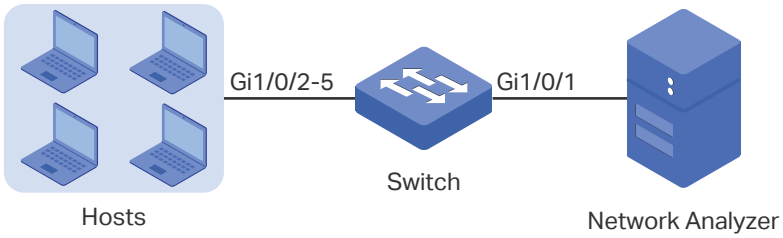
Switch#copy running-config startup-config

2 Configuration Examples

2.1 Network Requirements

As shown below, several hosts and a network analyzer are directly connected to the switch. For network security and troubleshooting, the network manager needs to use the network analyzer to monitor the data packets from the end hosts.

Figure 2-1 Network Topology



2.2 Configuration Scheme

To implement this requirement, you can use Mirroring feature to copy the packets from ports 1/0/2-5 to port 1/0/1. The overview of configuration is as follows:

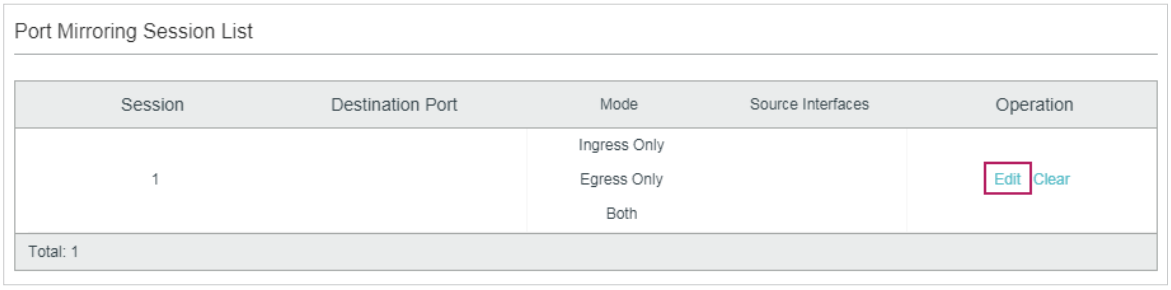
1) Specify ports 1/0/2-5 as the source ports, allowing the switch to copy the packets from the hosts.
2) Specify port 1/0/1 as the destination port so that the network analyzer can receive mirrored packets from the hosts.

Demonstrated with T1600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

2.3 Using the GUI

1) Choose the menu **MAINTENANCE > Mirroring** to load the following page. It displays the information of the mirroring session.

Figure 2-2 Mirror Session List

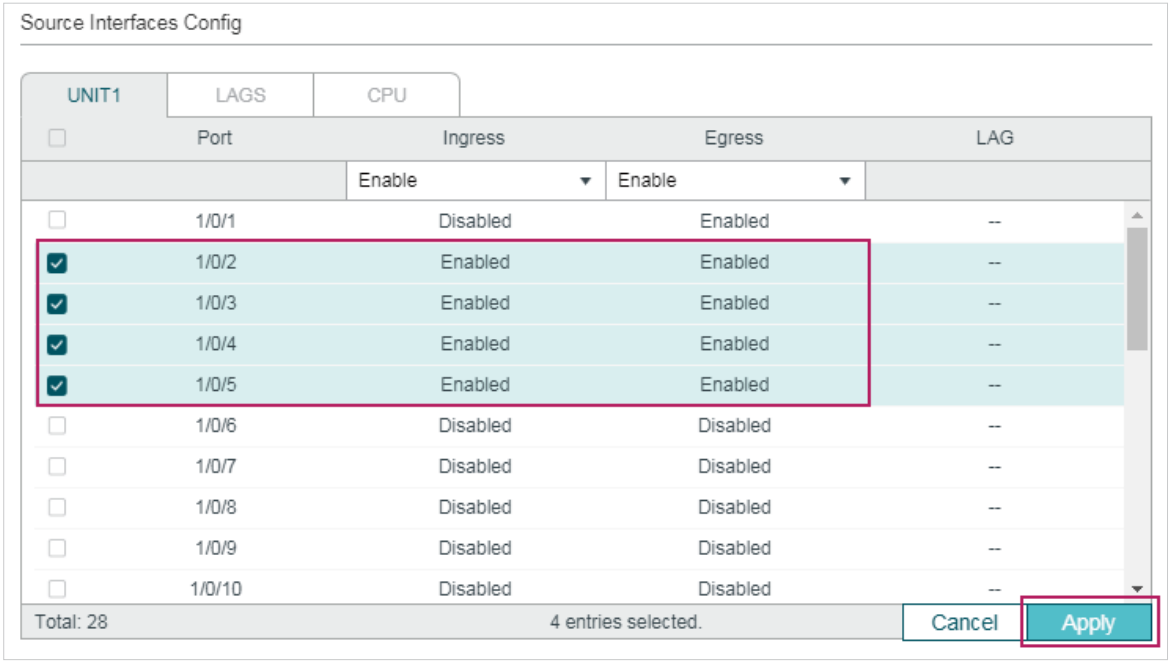


2) Click **Edit** on the above page to load the following page. In the **Destination Port Config** section, select port 1/0/1 as the destination port and click **Apply**.

Figure 2-3 Destination Port Configuration

3) In the **Source Interfaces Config** section, select ports 1/0/2-5 as the source ports, and enable **Ingress** and **Egress** to allow the received and sent packets to be copied to the destination port. Then click **Apply.**

Figure 2-4 Source Port Configuration



4) Click Save to save the settings.

2.4 Using the CLI

Switch#configure

Switch(config)#monitor session 1 destination interface gigabitEthernet 1/0/1

Switch(config)#monitor session 1 source interface gigabitEthernet 1/0/2-5 both

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configuration

Switch#show monitor session 1

Monitor Session:	1
Destination Port:	Gi1/0/1
Source Ports(Ingress):	Gi1/0/2-5
Source Ports(Egress):	Gi1/0/2-5

3 Appendix: Default Parameters

Default settings of Switching are listed in th following tables.

Table 3-1 Configurations for Ports

Parameter	Default Setting
Ingress	Disabled
Egress	Disabled

Part 35

Configuring sFlow

(Only for Certain Devices)

CHAPTERS

1. Overview
2. sFlow Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

Note:

sFlow is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If sFlow is available, there is **MAINTENANCE > sFlow** in the menu structure.

sFlow (Sampled Flow) is a technology for monitoring high-speed switched and routed networks. It provide complete visibility into network activity. With sFlow, you can analyze traffic statistics and monitor the network usage, thus implement effective management and control of network resources.

The sFlow monitoring system consists of an sFlow Agent and an sFlow Collector.

sFlow Agent

The sFlow Agent is embedded in a switch or router or in a standalone probe. It uses sampling technology to capture traffic statistics from the device it is monitoring, and packages the sampled data into sFlow datagrams. sFlow datagrams are used to immediately forward the sampled data to an sFlow Collector for analysis.

The switch provides a packet-based sFlow, which samples one packet out of a specified number of packets.

sFlow Collector

The sFlow Collector is installed in a host. It analyzes sFlow datagrams to produce a rich, real-time, network-wide view of traffic flows.

2 sFlow Configuration

To complete the configuration, follow these steps:

1) Configure the sFlow Agent.
2) Configure the sFlow Collector.
3) Configure the sFlow Sampler.

Configuration Guidelines

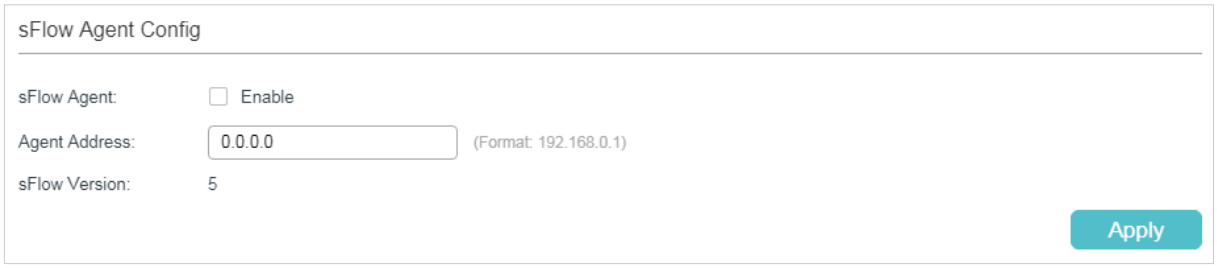
To get analytic results, you should choose a proper collector. For details on sFlow collectors, refer to https://sflow.org.

2.1 Using the GUI

2.1.1 Configuring the sFlow Agent

Choose the menu **MAINTENANCE > sFlow > sFlow Agent** to load the following page.

Figure 2-1 Configuring the sFlow Agent



Follow these steps to configure the sFlow Agent:

1) Enable the sFlow function, specify the sFlow Agent IP address.

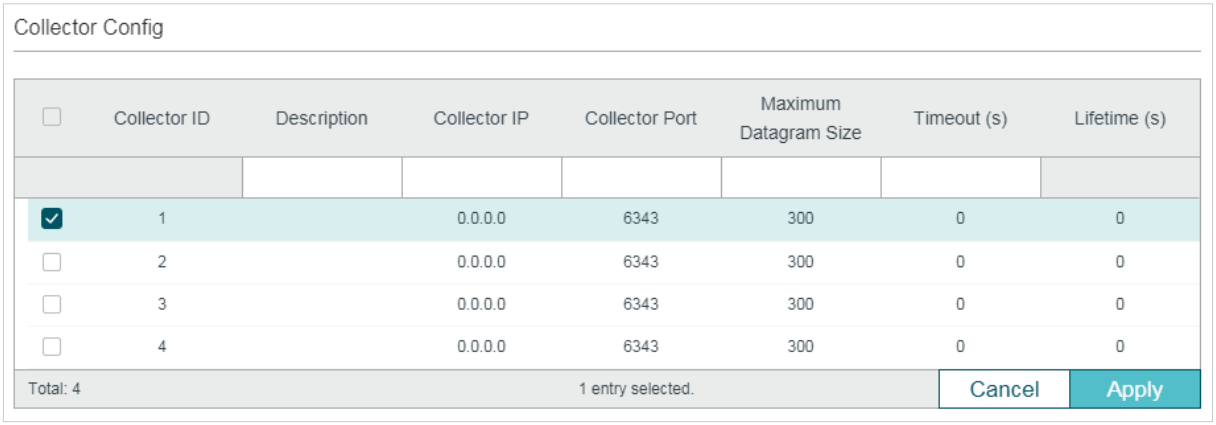
sFlow Agent	Enable or disable sFlow Agent. When enabled, the switch acts as an sFlow Agent.
Agent Address	Enter the IP address of the sFlow Agent. Normally it is the management IP address of the switch.
sFlow Version	The sFlow version is v5.

2) Click **Apply**.

2.1.2 Configuring the sFlow Collector

Choose the menu **MAINTENANCE > sFlow > sFlow Collector** to load the following page.

Figure 2-2 Configuring the sFlow Collector



Follow these steps to configure the sFlow Collector:

1) Select a Collector and configure the relevant parameters.

Collector ID	Displays the Collector ID. The switch supports 4 collectors at most.
Description	Give the collector a description for identification with 16 characters at most.
Collector IP	Enter the IP address of the host that runs the sFlow Collector.
Collector Port	Specify the UDP port number for the sFlow collector. The default is port 6343.
Maximum Datagram Size	Specify the maximum number of data bytes that can be sent in a single sample datagram. Valid values are from 300 to 1400 bytes and the default is 300 bytes.
Timeout (s)	Specify the aging time after which the sFlow Collector will become invalid. Valid values are from 0 to 2000000 seconds; the default is 0, which means the collector is always valid.
Lifetime (s)	Displays the remaining time of the collector. Lifetime counts down from Timeout.

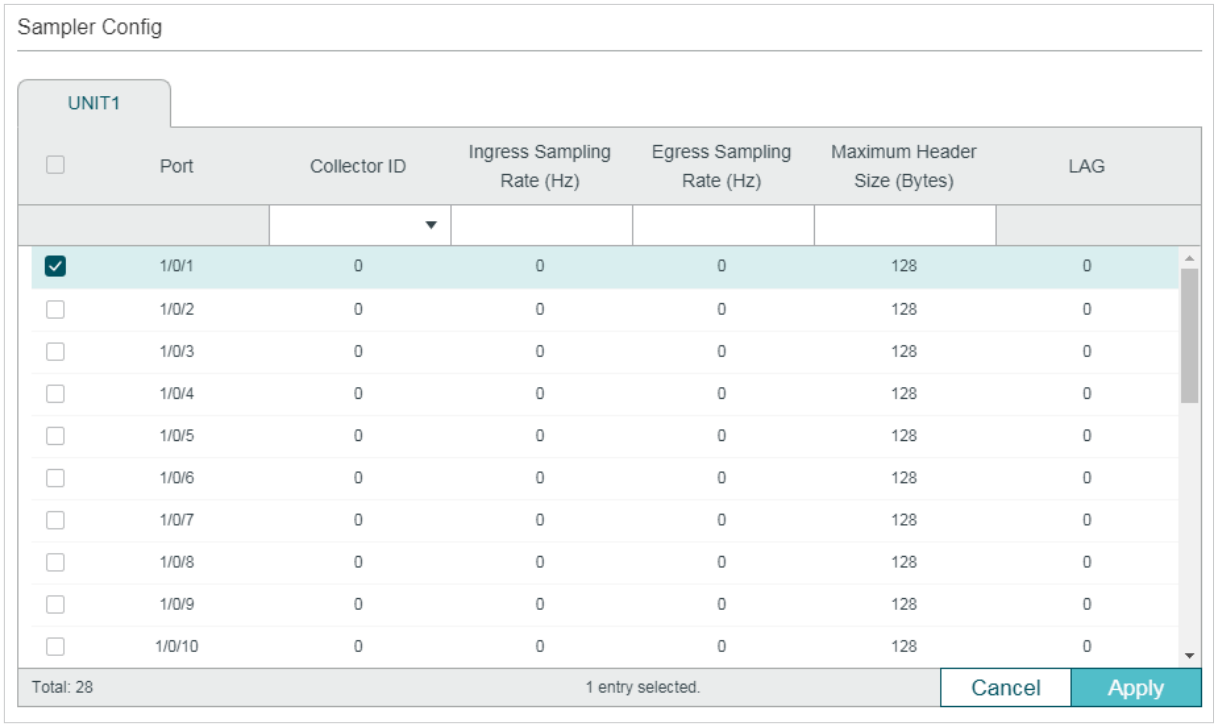
2) Click **Apply**.

2.1.3 Configuring the sFlow Sampler

An sFlow Sampler is a data source that collects flow samples. Usually the ports act as sFlow Samplers.

Choose the menu **MAINTENANCE > sFlow> sFlow Sampler** to load the following page.

Figure 2-3 Configuring the sFlow Sampler



Follow these steps to configure the sFlow Sampler:

1) Set one or more ports to be Samplers and configure the relevant parameters . One port can be bound to only one collector.

Collector ID	Choose a collector to be bound with the port.
Ingress Sampling Rate (Hz)	Specify the ingress sampling frequency; the sampler takes one packet out of the specified number of packets. Valid values are from 1024 to 65535. The default is 0 which means no packets will be sampled.
Egress Sampling Rate (Hz)	Specify the egress sampling frequency; the sampler takes one packet out of the specified number of packets. Valid values are from 1024 to 65535. The default is 0 which means no packets will be sampled.
Maximum Header Size (Bytes)	Specify the maximum number of bytes that should be copied from a sampled packet. Valid values are from 18 to 256 bytes and the default is 128 bytes.
LAG	Displays the LAG the port belongs to.

2) Click **Apply**.

2.2 Using the CLI

Follow these steps to configure the sFlow:

Step 1	**configure** Enter global configuration mode.
Step 2	**sflow address** { *ipv4-addr* } Configure the IP address of sFlow Agent. *ipv4-addr:* Enter the management IP address of the switch to monitor traffic on the switch ports.
Step 3	**sflow enable** Enable the sFlow function.
Step 4	**sflow collector collector-ID** *value* { [**descript** *descript*]	[**ip** *ip*]	[**port** *port*]	[**maxData** *maxData*]	[**timeout** *timeout*] } Configure parameters of the sFlow collector. *value*: Enter the ID of the sFlow collector. The values are from 1 to 4. *descript*: Give a collector description for identification with 16 characters at most. *ip*: Enter the IP address of the host that runs the sFlow collector. *port*: Enter the UDP port number for the sFlow collector. The default is port 6343. *maxData*: Specify the maximum number of data bytes that can be sent in a single sample datagram. The values are from 300 to 1400 bytes; the default is 300 bytes. *timeout*: Specify the aging time after which the sFlow collector will become invalid. The values are from 0 to 2000000 seconds; the default is 0, which means the collector is always valid.
Step 5	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **]** Configure the sampler on the specified ports. *port/port-list:* The number or the list of the Ethernet ports that you want to monitor.
Step 6	**sflow sampler** { [**collector-ID** *value*]	[**ingRate** *ingress-rate*] [**egRate** *egress-rate*]	[**maxHeader** *maxHeader*] } Configure parameters of the sFlow sampler. *value*: Enter the ID of the sFlow collector which the sFlow sampler will send sFlow datagrams to. The values are from 0 to 4. 0 means sampling feature is disabled on the port. *ingress-rate*: Specify the ingress sampling frequency. The samplers takes one packet out of the specified number of packets. Valid values are from 1024 to 65535. The default is 0 which means no packets will be sampled. *egress-rate*: Specify the egress sampling frequency. The samplers takes one packet out of the specified number of packets. Valid values are from 1024 to 65535. The default is 0 which means no packets will be sampled. *maxHeader*: Specify the maximum number of bytes that should be copied from a sampled packet. Valid values are from 18 to 256 bytes and the default is 128 bytes.

Step 7	**show sflow** { [global] | [collector] | [sampler] } Verify the sFlow configurations. global: View the global configuration of sFlow. collector: View the global configuration of the sFlow collector. sampler: View the global configuration of the sFlow sampler.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch whose IP address is 192.168.0.1 to send sFlow packets to the host whose IP address is 192.168.0.100. Set the sFlow agent IP address as 192.168.0.1, the sFlow collector IP address 1 as 192.168.0.100; configure Gigabit Ethernet port 1 as the sFlow sampler, the Collector-ID as 1, and the ingress rate as 1024:

Switch#configure

Switch(config)#sflow address 192.168.0.1

Switch(config)#sflow enable

Switch(config)#sflow collector collector-ID 1 **ip** 192.168.0.100

Switch(config)# sflow collector collector-ID 1 **port** 6343

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#sflow sampler collector-ID 1

Switch(config-if)#sflow sampler ingRate 1024

Switch(config-if)#show sflow global

sFlow Status: Enable

Agent Address: 192.168.0.1

sFlow Version: v5

Switch(config-if)#show sflow collector

Collector	Col-IP	Col-Port	MaxData	Timeout	Lifetime	Description
1	192.168.0.100	6343	300	0	0	

...

Switch(config-if)#show sflow sampler

Port	Collector	IngRate	EgRate	MaxHeader	LAG
Gi1/0/1	1	1024	0	128	N/A
Gi1/0/2	0	0	0	128	N/A
Gi1/0/3	0	0	0	128	N/A

...

Switch(config-if)#end

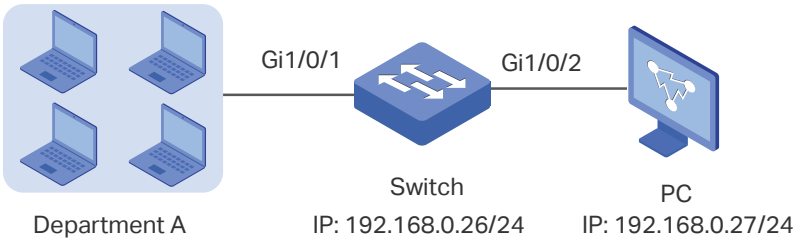
Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

The company network manager needs to monitor and analyze the network usage in department A.

Figure 3-1 Network Topology



3.2 Configuration Scheme

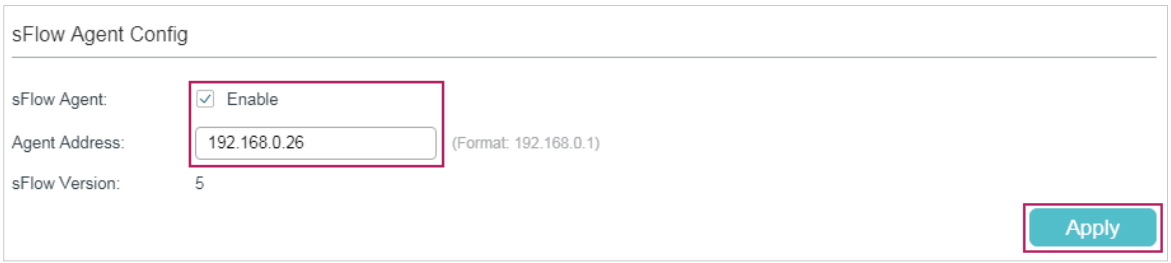
The network manager can configure sFlow to monitor and analyze the network. Set the switch as the sFlow Agent that collects traffic data on port 1/0/1, and configure an sFlow Collector on the PC to process sFlow packets and display results.

Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and Using the CLI.

3.3 Using the GUI

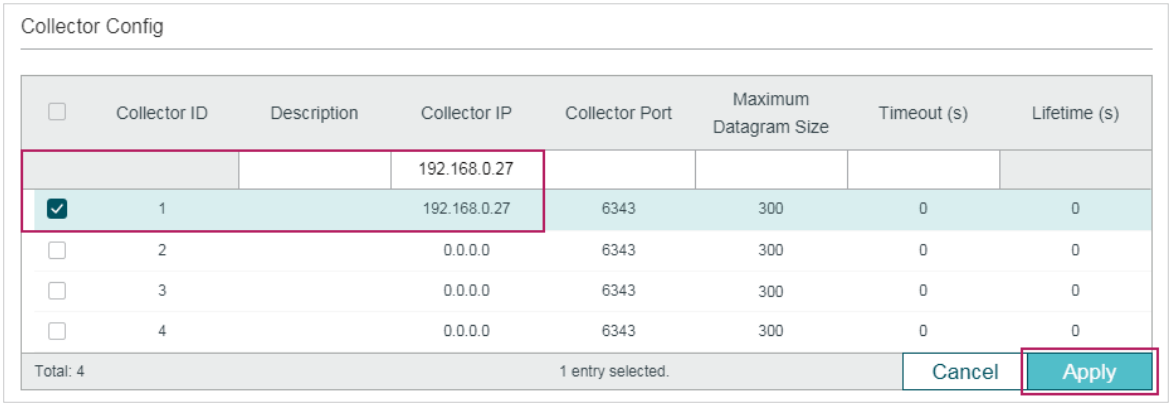
1) Choose the menu **MAINTENANCE > sFlow > sFlow Agent** to load the following page. Enable sFlow Agent, set the switch IP address 192.168.0.26 as the Agent address, and click **Apply**.

Figure 3-2 Configuring sFlow Agent



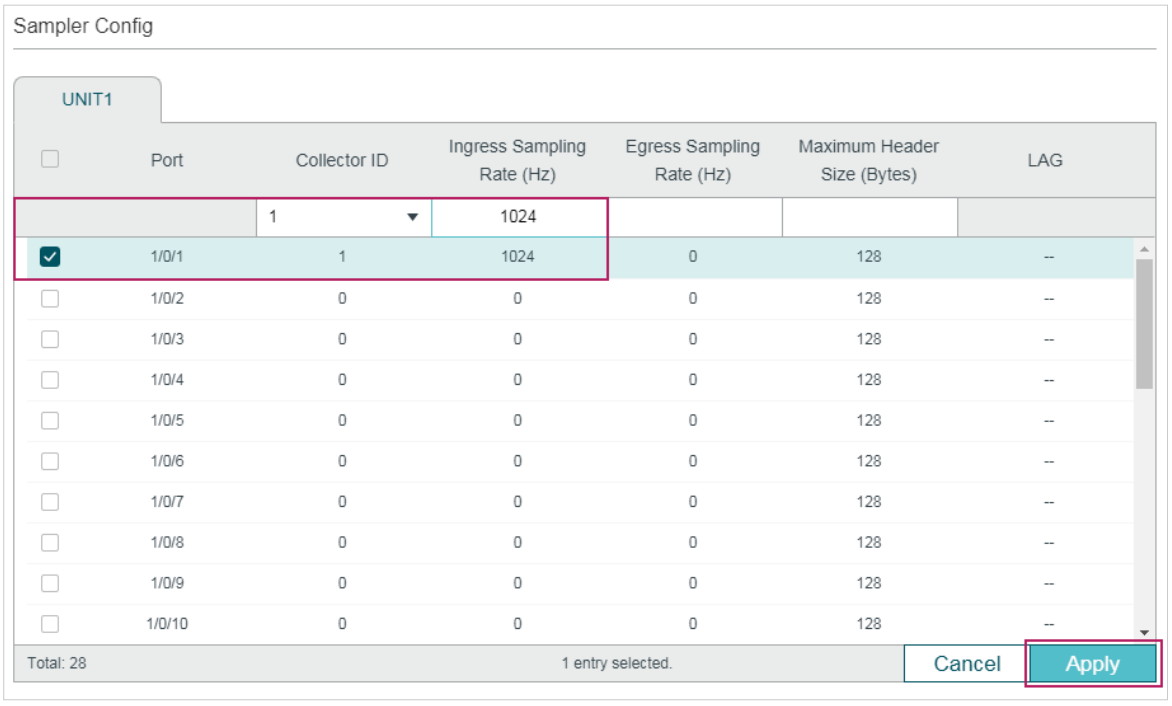
2) Choose the menu **MAINTENANCE > sFlow > sFlow Collector** to load the following page. Select Collector 1, enter the PC's IP address 192.168.0.27 as the Collector IP address, and click **Apply**.

Figure 3-3 Configuring sFlow Collector



3) Choose the menu **MAINTENANCE > sFlow > sFlow Sampler** to load the following page. Select Collector 1 for port 1/0/1, set the ingress rate as 1024, then click **Apply**.

Figure 3-4 Configuring sFlow Sampler



4) Click Save to save the settings.

3.4 Using the CLI

1) Configure the sFlow Agent.

Switch#configure

Switch(config)#sflow address 192.168.0.26

Switch(config)#sflow enable

2) Configure the sFlow collector.

Switch(config)#sflow collector collector-ID 1 ip 192.168.0.27

Switch(config)# sflow collector collector-ID 1 port 6343

3) Configure the sFlow sampler.

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#sflow sampler collector-ID 1

Switch(config-if)#sflow sampler ingRate 1024

Switch(config-if)#end

Switch#copy running-config startup-config

Verify the Configurations

Verify the configuration of global sFlow:

Switch#show sflow global

sFlow Status: Enable

Agent Address: 192.168.0.26

sFlow Version: v5

Verify the configuration of sFlow collector:

Switch#show sflow collector

Collector	Col-IP	Col-Port	MaxData	Timeout	Lifetime	Description
1	192.168.0.27	6343	300	0	0	
2	0.0.0.0	6343	300	0	0	
3	0.0.0.0	6343	300	0	0	
4	0.0.0.0	6343	300	0	0	

Verify the configuration of sFlow sampler:

Switch#show sflow sampler

Port	Collector	IngRate	EgRate	MaxHeader	LAG
Gi1/0/1	1	1024	0	128	N/A
Gi1/0/2	0	0	0	128	N/A

...

4 Appendix: Default Parameters

Default settings of maintenance are listed in the following tables.

Table 4-1 Default Settings of sFlow

Parameter	Default Setting
sFlow Agent	
sFlow Agent	Disabled
Agent Address	0.0.0.0
sFlow Version	5
sFlow Collector	
Collector IP	0.0.0.0
Collector Port	6343
Maximum Datagram Size	300 bytes
Timeout (s)	0
sFlow Sampler	
Collector ID	0, indicates sampling feature is disabled on the port.
Ingress Sampling Rate (Hz)	0
Egress Sampling Rate (Hz)	0
Maximum Header Size (Bytes)	128

Part 36

Configuring OAM

(Only for Certain Devices)

CHAPTERS

1. Ethernet OAM
2. Ethernet OAM Configurations
3. Viewing OAM Statistics
4. Configuration Example
5. Appendix: Default Parameters

1 Ethernet OAM

1.1 Overview

Note:

Ethernet OAM is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If Ethernet OAM is available, there is **MAINTENANCE > Ethernet OAM** in the menu structure.

Ethernet OAM (Operation, Administration, and Maintenance) is a Layer 2 protocol for monitoring and troubleshooting Ethernet networks. It can monitor link performance, monitor faults and generate alarms so that a network administrator can manage the network effectively. TP-Link switches support EFM OAM which is defined in IEEE 802.3ah.

The following basic concepts of OAM will be introduced: OAM entity, OAMPDUs (OAM Protocol Data Units), and OAM connection.

OAM Entity

A port that is enabled with OAM on the switch is called an OAM entity.

OAMPDUs

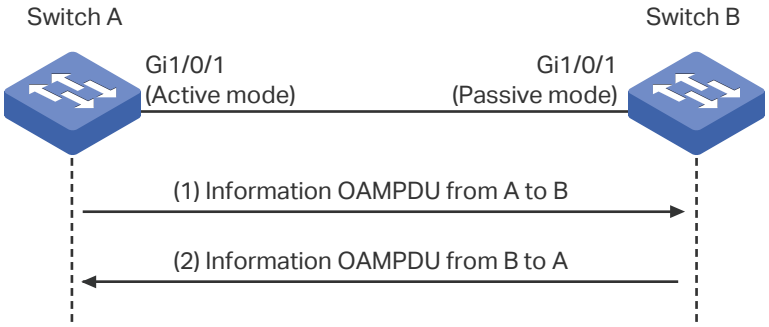
Through OAMPDUs exchanged between OAM entities, failure conditions on the network are reported to network administrators. The OAMPDUs are defined as follows:

- **Information OAMPDU**: The Information OAMPDU is used to send state information, such as local information, remote information, and user-defined information, to the remote OAM entity for maintaining OAM connection.
- **Event Notification OAMPDU**: The Event Notification OAMPDU is used for the Link Monitoring feature. The local OAM entity can use the Event Notification OAMPDU to notify the remote OAM entity that a fault has occurred to the link.
- **Loopback Control OAMPDU**: Loopback Control OAMPDU is used for the Remote Loopback feature. The local OAM entity can control OAM remote loopback state of the remote OAM entity through the Loopback Control OAMPDU.

OAM Connection

OAM connection is established between OAM entities before OAM works. An OAM entity can operate in two modes: active and passive. Only the active OAM entity can initiate an OAM connection; the passive OAM entity waits and responds to OAM connection establishment requests. So at least one of the two entities should be in active mode.

Figure 1-1 OAM Connection Establishment



As the above figure shows, the OAM entity on Switch A is in active mode, and that on Switch B is in passive mode. Switch A initiates an OAM connection by sending an Information OAMPDU. Switch B compares the OAM information in the received OAMPDU with its own and sends back an Information OAMPDU to Switch A. If the OAM information of the two entities matches, an OAM connection will be established. After that, the two OAM entities will exchange Information OAMPDUs periodically to keep the OAM connection valid.

1.2 Supported Features

The switch supports the following OAM features: Link Monitoring, Remote Failure Indication (RFI), and Remote Loopback.

Link Monitoring

Link Monitoring is for monitoring link performance under various circumstances. When problems are detected on the link, the OAM entity will send its remote peer the Event Notification OAMPDUs to report link events.

The link events are described as follows:

Table 1-1 OAM Link Events

OAM Link Events	Definition
Error Symbol Period	An Error Symbol Period event occurs if the number of error symbols exceeds the defined threshold within a specific period of time.
Error Frame	An Error Frame event occurs if the number of error frames exceeds the defined threshold within a specific period of time.
Error Frame Period	An Error Frame Period event occurs if the number of error frames in a specific number of received frames exceeds the defined threshold.
Error Frame Seconds	An Error Frame Seconds event occurs if the number of error frame seconds exceeds the threshold within a specific period of time. A second is defined as an error frame second if error frames occur within that second.

Remote Failure Indication (RFI)

With Remote Failure Indication, an OAM entity can send the failure conditions of the link, such as disruption in traffic because of the device failure, to its peer through Information OAMPDUs. This allows the network administrator to stay informed of the link faults and take action quickly. The switch supports two kinds of failure conditions:

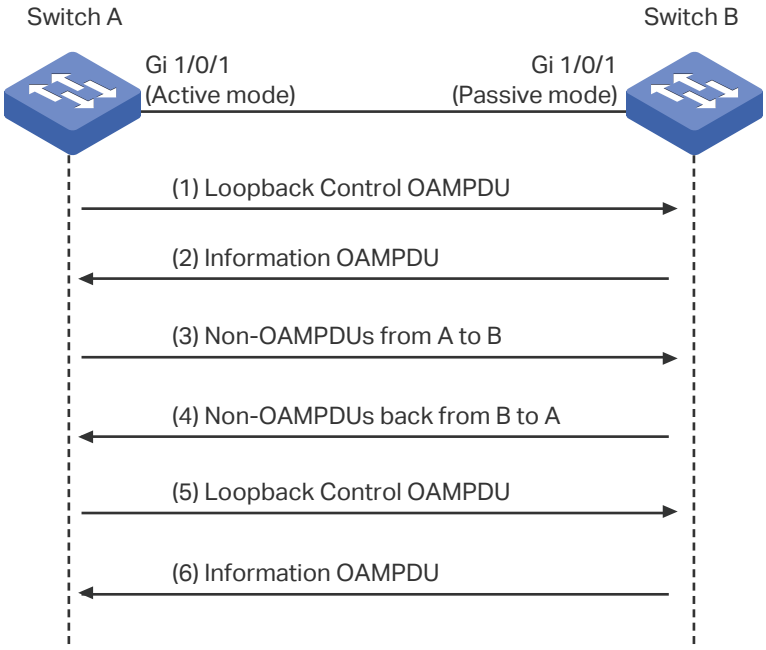
Dying Gasp: An unrecoverable fault, such as power failure, occurs.

Critical Event: Unspecified critical event occurs.

Remote Loopback

With Remote Loopback, administrators can test link performance including the delay, jitter, and frame loss rate during installation or troubleshooting.

Figure 1-2 Remote Loopback



As the above figure shows, the OAM connection has been established between the two entities. The OAM entity on Switch A is in active mode, and that on Switch B is in passive mode.

The working mechanism of Remote Loopback is as follows:

1) Switch A sends a Loopback Control OAMPDU to put the peer into remote loopback mode. Note that at least one of the two entities should be configured in active mode because only the entity in active mode can generate Loopback Control OAMPDU.
2) After receiving the Loopback Control OAMPDU, Switch B turns into remote loopback mode and sends an Information OAMPDU to inform its state updating.
3) Switch A sends Non-OAMPDU packets to Switch B for link testing.
4) Switch B receives the testing packets and sends back these packets along the original path. Through these returned packets, administrators can test the link performance.

5) When Remote Loopback is finished, Switch A sends a Loopback Control OAMPDU to disable the remote loopback mode on Switch B.
6) Switch B receives the Loopback Control OAMPDU and exits remote loopback mode. Besides, Switch B sends an Information OAMPDU to inform its state updating.

TP-Link switches can act as Switch A and initiate Remote Loopback request.

2 Ethernet OAM Configurations

To complete OAM configurations, follow these steps:

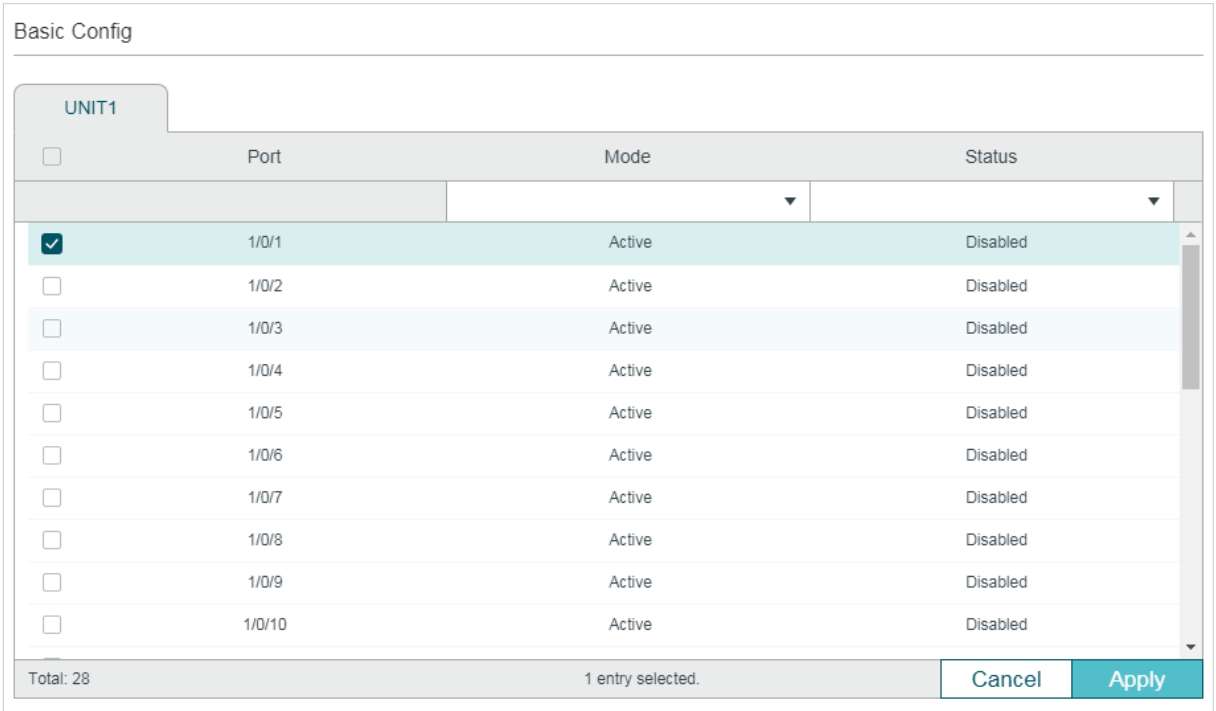
1) Enable OAM and configure OAM mode on the port.
2) Configure the following OAM features according to your needs:
   - Link Monitoring
   - Remote Failure Indication (RFI)
   - Remote Loopback
3) View the OAM status on the port.

2.1 Using the GUI

2.1.1 Enabling OAM and Configuring OAM Mode

Choose the menu **MAINTENANCE > Ethernet OAM > Basic Config > Basic Config** to load the following page.

Figure 2-1 Basic Configuration



Follow these steps to complete the basic OAM configuration:

1) Select one or more ports, configure the OAM mode and enable OAM.

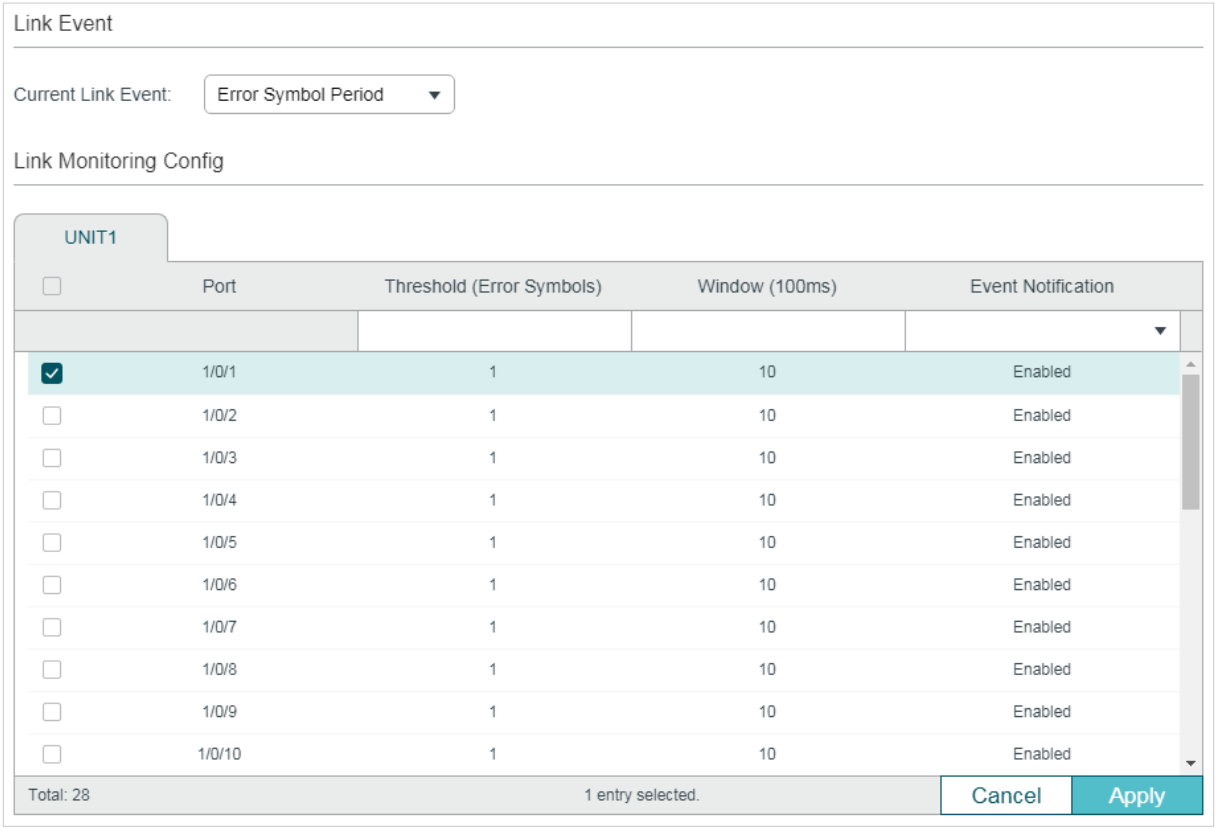
Mode	Select OAM mode for the port. **Active:** The port in this mode can initiate OAM connection. It is the default setting. **Passive:** The port in this mode cannot initiate OAM connection or send loopback control OAMPDUs. *Note:* OAM connection cannot be established between two ports in passive mode. Make sure that at least one side is in active mode.
Status	Enable or disable OAM on the port. By default, it is disabled.

2) Click **Apply**.

2.1.2 Configuring Link Monitoring

Choose the menu **MAINTENANCE > Ethernet OAM > Link Monitoring > Link Monitoring** to load the following page.

Figure 2-2 Configure Link Monitoring



Follow these steps to configure Link Monitoring:

1) In the **Link Event** section, select a Link Event type to configure.

Current Link Event	Select Link Event type. The following options are provided: **Error Symbol Period**: An Error Symbol Period event occurs if the number of error symbols exceeds the defined threshold within a specific period of time. **Error Frame**: An Error Frame event occurs if the number of error frames exceeds the defined threshold within a specific period of time. **Error Frame Period**: An Error Frame Period event occurs if the number of error frames in a specific number of received frames exceeds the defined threshold. **Error Frame Seconds**: An Error Frame Seconds event occurs if the number of error frame seconds exceeds the threshold within a specific period of time. A second is defined as an error frame second if error frames occur within that second.

2) In the **Link Monitoring Config** section, select one or more ports, and configure the threshold and period for the selected link event.

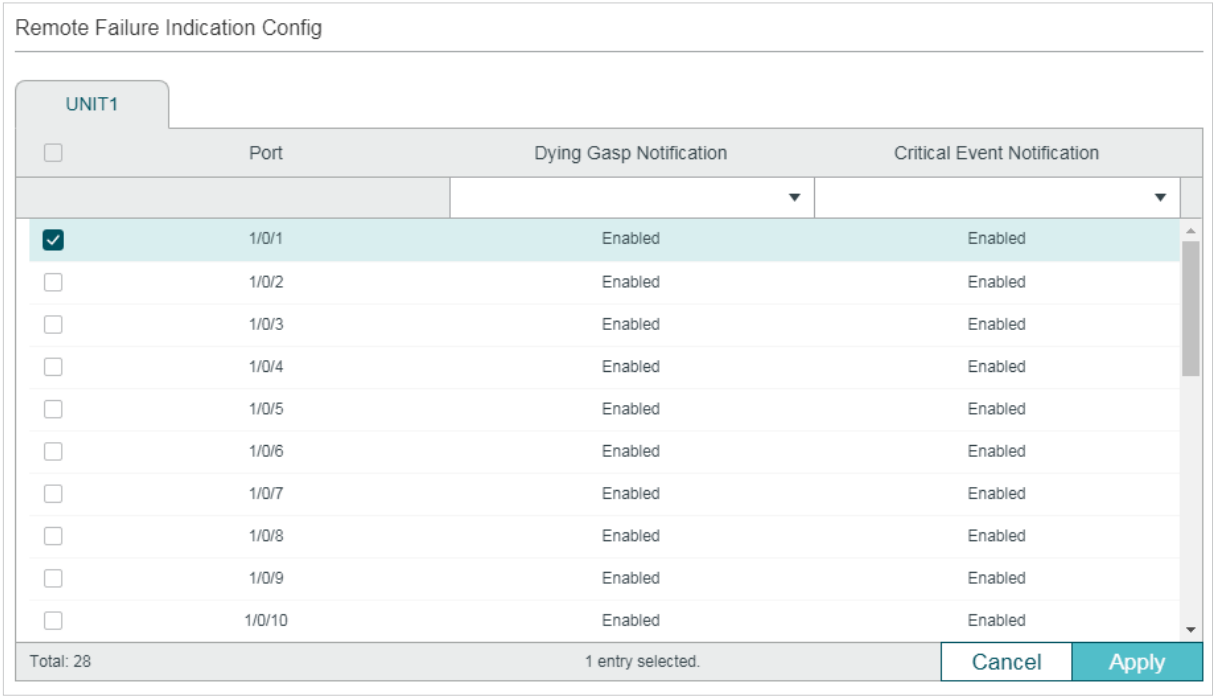
Threshold	Specify the threshold for the selected link event. **Threshold (Error Symbols)**: If you select **Error Symbol Period** as the link event type, specify the threshold of received error symbols within a specific period of time. Valid error frame values are from 1 to 4294967295, and the default value is 1. **Threshold (Error Frames)**: If you select **Error Frame** or **Error Frame Period** as the link event type, specify the threshold of error frames within a specific period of time or in specific number of received frames. Valid error frame values are from 1 to 4294967295, and the default value is 1. **Threshold (Error Seconds)**: If you select **Error Frame Seconds** as the link event type, specify the threshold of error frame seconds. Valid values are from 1 to 900, and the default value is 1.
Window	Specify the period for the selected link event. **Window (100ms)**: If you select **Error Symbol Period**, **Error Frame** or **Error Frame Seconds** as the link event type, specify the time period in units of 100ms (for example, 2 refers to 200ms), in which if the received errors exceed the threshold, a link event will be generated. For **Error Symbol Period** and **Error Frame**, valid values are from 10*100 to 600*100 ms. For **Error Frame Seconds**, valid values are from 100*100 to 9000*100 ms. **Window (Frames)**: If you select **Error Frame Period** as the link event type, specify the number of frames, in which if the frame errors exceed the threshold, a link event will be generated. Valid values are from 148810 to 89286000 frames, and the default value is 1488100 frames.
Event Notification	Enable or disable notifications to report the link event. By default, all types of link event can be reported.

3) Click **Apply**.

2.1.3 Configuring RFI

Choose the menu **MAINTENANCE > Ethernet OAM > Remote Failure Indication** to load the following page.

Figure 2-3 Configure RFI



Follow these steps to configure Remote Failure Indication:

1) Select one or more ports and configure the Dying Gasp Notification and Critical Event Notification features.

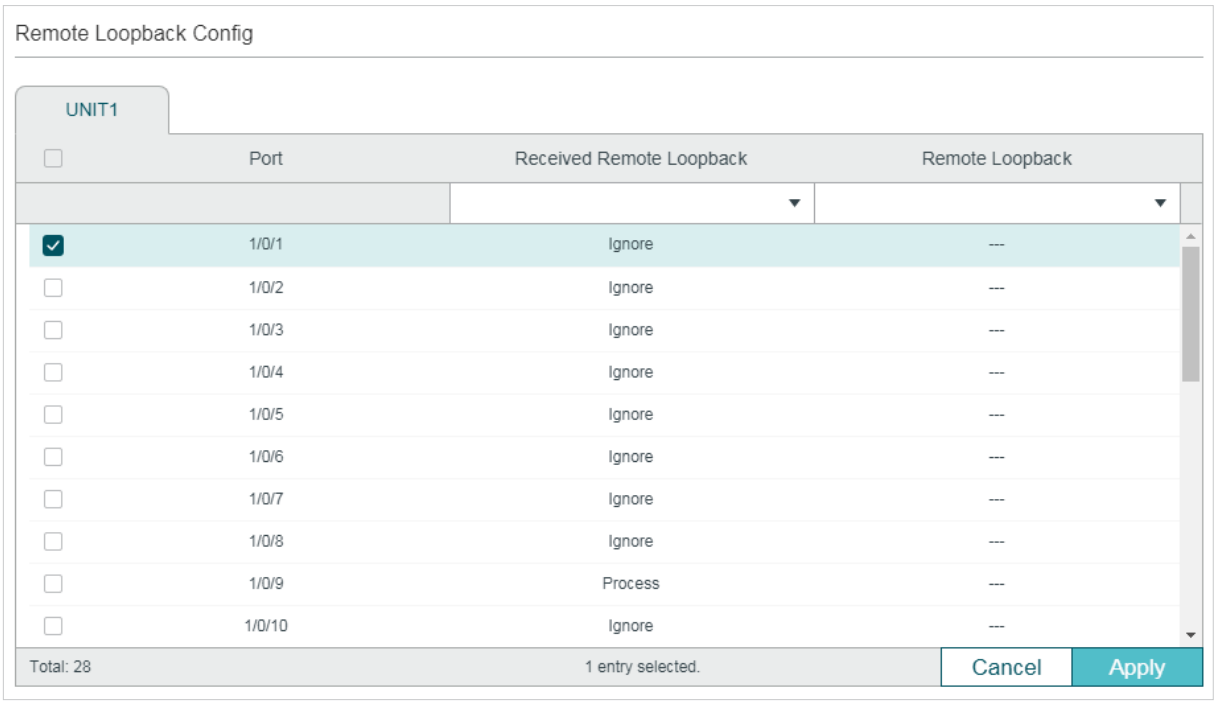
Dying Gasp Notification	With Dying Gasp Notification enabled, if the switch detects an unrecoverable fault on the network, it will report this condition locally and send Information OAMPDU to notify the peer.
Critical Event Notification	With Critical Event Notification enabled, if the switch detects an unspecified critical event occurs, it will report this condition locally and send Information OAMPDU to notify the peer.

2) Click **Apply**.

2.1.4 Configuring Remote Loopback

Choose the menu **MAINTENANCE > Ethernet OAM > Remote Loopbak** to load the following page.

Figure 2-4 Configure Remote Loopback



Follow these steps to configure Remote Loopback:

1) Select one or more ports and configure the relevant options.

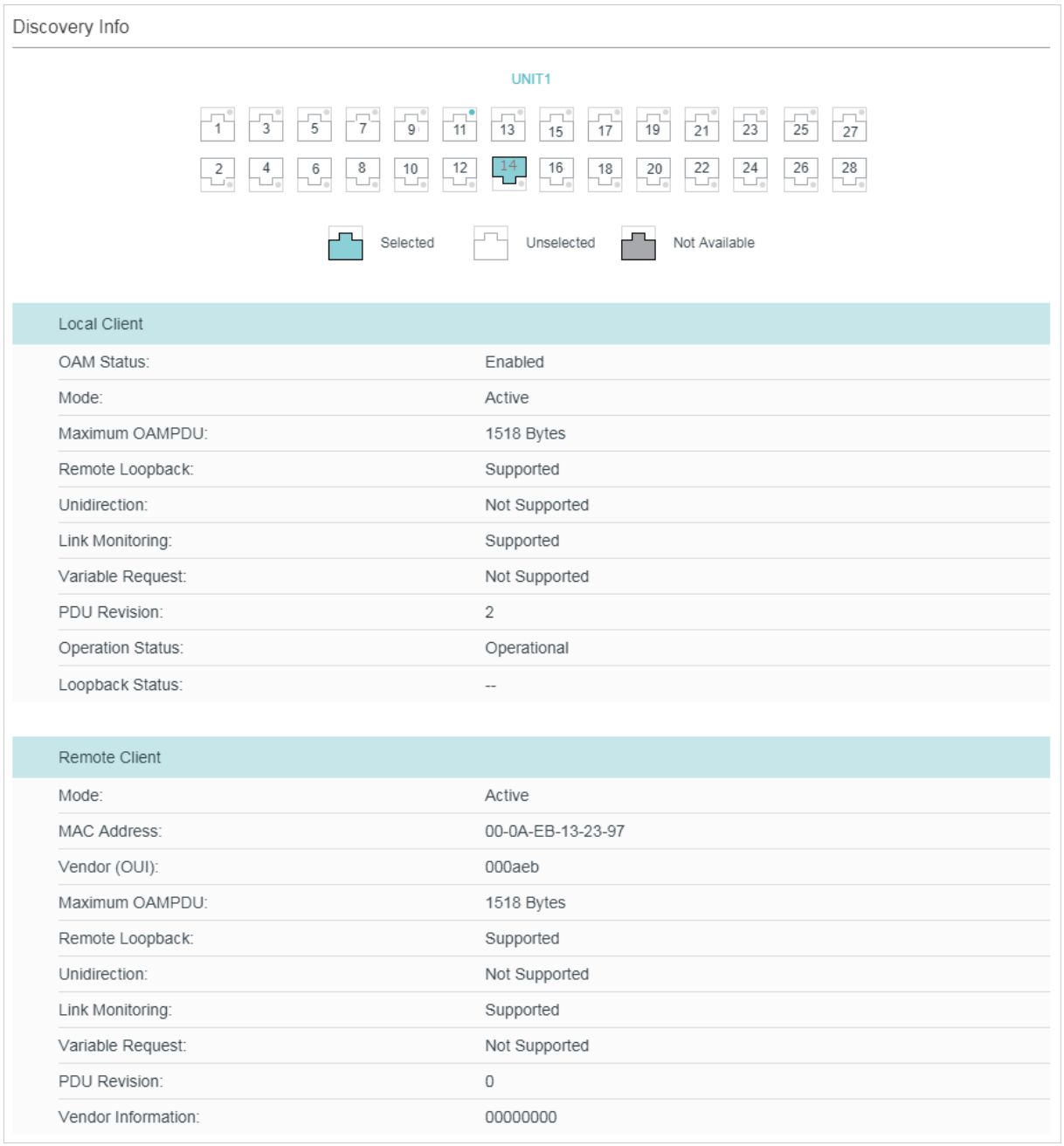
Received Remote Loopback	Choose to ignore or to process the received remote loopback requests.
Remote Loopback	Start or stop the remote loopback process. The port to be configured should be in active mode and has established OAM connection with the peer. **Start**: Request the remote peer to start the OAM remote loopback mode. **Stop**: Request the remote peer to stop the OAM remote loopback mode.

2) Click **Apply**.

2.1.5 Viewing OAM Status

Choose the menu **MAINTENANCE > Ethernet OAM > Basic Config > Discovery Info** to load the following page.

Figure 2-5 View OAM Status



Select a port to view whether the OAM connection is established with the peer. Additionally, you can view the OAM information of the local and the remote entities.

The OAM information of the local entity is as follows:

OAM Status	Displays whether OAM is enabled.
Mode	Displays the OAM mode of the local entity.

Maximum OAMPDU	Displays the maximum size of OAMPDU.
Remote Loopback	Displays whether the local entity supports Remote Loopback.
Unidirection	Displays whether the local entity supports Unidirection.
Link Monitoring	Displays whether the local entity supports Link Monitoring.
Variable Request	Displays whether the local entity supports Variable Request.
PDU Revision	Displays the PDU Revision of the local entity.
Operation Status	Displays the status of OAM connection: **Disable**: OAM is disabled on the port. **LinkFault**: The link between the local entity and the remote entity is down. **PassiveWait**: The port is in passive mode and is waiting to see if the peer device is OAM capable. **ActiveSendLocal**: The port is in active mode and is sending local information. **SendLocalAndRemote**: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer. **SendLocalAndRemoteOK**: The local device agrees the OAM peer entity. **PeeringLocallyRejected**: The local OAM entity rejects the remote peer OAM entity. **PeeringRemotelyRejected**: The remote OAM entity rejects the local device. **NonOperHalfDuplex**: Ethernet OAM is enabled but the port is in half-duplex operation. You should configure the port as a full-duplex port. **Operational**: OAM connection is established with the peer and OAM works normally.
Loopback Status	Displays the loopback status. **No Loopback**: Neither the local entity nor the remote entity is in the loopback mode. **Local Loopback**: The local entity is in the loopback mode. **Remote Loopback**: The remote entity is in the loopback mode.

The OAM information of the remote entity is as follows:

Mode	Displays the OAM mode of the remote entity.
MAC Address	Displays the MAC address of the remote entity.
Vendor (OUI)	Displays the Vendor's OUI of the remote entity.

Maximum OAMPDU	Displays the maximum size of OAMPDU.
Remote Loopback	Displays whether the remote entity supports Remote Loopback.
Unidirection	Displays whether the remote entity supports Unidirection.
Link Monitoring	Displays whether the remote entity supports Link Monitoring.
Variable Request	Displays whether the remote entity supports Variable Request.
PDU Revision	Displays the PDU Revision of the remote entity.
Vendor Information	Displays the vendor information of the remote entity.

2.2 Using the CLI

2.2.1 Enabling OAM and Configuring OAM Mode

Follow these steps to enable OAM and configure OAM mode on the port:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam** Enable OAM on the port.
Step 4	**ethernet-oam mode** { passive | active } Configure the OAM mode of the port. passive: Specify the OAM mode as passive. The port in this mode cannot initiate OAM connection or send Loopback Control OAMPDU. active: Specify the OAM mode as active. The port in this mode can initiate OAM connection. It is the default setting. *Note*: OAM connection cannot be established between two ports in passive mode. Make sure that at least one side is in active mode.
Step 5	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| ten-gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.

Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable OAM and configure the OAM mode as passive on port 1/0/1.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ethernet-oam

Switch(config-if)#ethernet-oam mode passive

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

OAM : Enabled

Mode : Passive

...

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.2 Configuring Link Monitoring

With Link Monitoring, the following link events can be reported: Error Symbol Period, Error Frame, Error Frame Period, Error Frame Seconds.

■ Configuring Error Symbol Period Event

An Error Symbol Period event occurs if the number of symbol errors exceeds the defined threshold within a specific period of time.

Follow these steps to configure the Error Symbol Period event:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode.

Step 3	**ethernet-oam link-monitor symbol-period** [**threshold** *threshold*] [**window** *window*] [**notify** {disable | enable}] Configure the relevant parameters of Error Symbol Period event. *threshold*: Specify the threshold of received symbol errors within a specific period of time. Valid values are from 1 to 4294967295, and the default value is 1. *window*: Specify the time period in units of 100ms (for example, 2 refers to 200ms), in which if the received errors exceed the threshold, a link event will be generated. Valid values are from 10*100 to 600*100 ms, and the default value is 10*100 ms. disable | enable: Enable or disable notifications to report the link event. By default, it is enabled.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| interface ten-gigabitEthernet** { *port* **|** *port-list* }**]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Error Frame event notification and configure the threshold as 1 and the window as 1000 ms (10*100 ms) on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ethernet-oam link-monitor symbol-period threshold 1 **window** 10 **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Symbol Period Error

Notify State	: Enabled
Window	: 1000 milliseconds
Threshold	: 1 Error Symbol

...

Switch(config-if)#end

Switch#copy running-config startup-config

Configuring Error Frame Event

An Error Frame event occurs if the number of frame errors exceeds the defined threshold within a specific period of time.

Follow these steps to configure the Error Frame event:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam link-monitor frame [threshold** *threshold* **] [window** *window* **] [notify** {disable | enable}] Configure the relevant parameters of Error Frame event. *threshold*: Specify the threshold of received frame errors within a specific period of time. Valid values are from 1 to 4294967295, and the default value is 1. *window*: Specify the time period in units of 100ms (for example, 2 refers to 200ms), in which if the number of received errors exceeds the threshold, a link event will be generated. Valid values are from 10*100 to 600*100 ms, and the default value is 10*100 ms. disable | enable: Enable or disable notifications to report the link event. By default, it is enabled.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| ten-gigabitEthernet** { *port* **|** *port-list* }**]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Error Frame notification and configure the threshold as 1 and the window as 2000 ms (20*100 ms) on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ethernet-oam link-monitor frame threshold 1 **window** 20 **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Frame Error

Notify State : Enabled

Window : 2000 milliseconds

Threshold : 1 Error Frame

...

Switch(config-if)#end

Switch#copy running-config startup-config

■ Configuring Error Frame Period Event

An Error Frame Period event occurs if the number of frame errors in specific number of received frames exceeds the defined threshold.

Follow these steps to configure the Error Frame Period event:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam link-monitor frame-period** [**threshold** *threshold*] [**window** *window*] [**notify** {disable | enable}] Configure the relevant parameters of Error Frame Period. *threshold*: Specify the threshold of received symbol errors in specific number of received frames. Valid values are from 1 to 4294967295, and the default value is 1. *window*: Specify the number of frames, in which if the frame errors exceed the threshold, a link event will be generated. Valid values are from 148810 to 89286000, and the default value is 1488100. disable | enable: Enable or disable the port to report the failure condition.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| ten-gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.

Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Error Frame Period notification and configure the threshold as 1 and the window as 1488100 on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ethernet-oam link-monitor frame-period threshold 1 **window** 1488100 **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Frame Period Error

Notify State : Enabled

Window : 1488100 Frames

Threshold : 1 Error Frame

...

Switch(config-if)#end

Switch#copy running-config startup-config

■ Configuring Error Frame Seconds Event

An Error Frame Seconds event occurs if the number of error frame seconds exceeds the threshold within a specific period of time. A second is called an error frame second if error frames occur in the second.

Follow these steps to configure Error Frame Seconds event:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode.

Step 3	**ethernet-oam link-monitor frame-seconds** [**threshold** *threshold*] [**window** *window*] [**notify** {disable | enable}] Configure the relevant parameters of Error Frame Period. *threshold*: Specify the threshold of received error frame seconds within a specific period of time. Valid values are from 1 to 900, and the default value is 1. *window*: Specify the period time in 100ms, in which if the received errors exceed the threshold, a link event will be generated. Valid values are from 100*100 to 9000*100 ms, and the default value is 600*100 ms. disable | enable : Enable or disable the port to report the failure condition.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| ten-gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Error Frame Seconds notification and configure the threshold as 1 and the window as 80000 ms (800*100 ms)on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ethernet-oam link-monitor frame-seconds threshold 1 **window** 800 **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Frame Seconds Error

Notify State : Enabled

Window : 80000 milliseconds

Threshold : 1 Error Seconds

...

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Configuring Remote Failure Indication

Follow these steps to configure Remote Failure Indication:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam remote-failure {** dying-gasp | critical-event **} notify {** disable | enable **}** Configure the Dying Gasp Notification and Critical Event Notification features on the port. dying-gasp: Enable Dying Gasp Notification, and if the switch detects an unrecoverable fault on the network, such as power failure, occurs, it will send Information OAMPDU to notify the peer. critical-event: Enable Critical Event Notification, and if the switch detects an unspecified critical event occurs, it will send Information OAMPDU to notify the peer. disable | enable: Enable or disable notification to report the link events.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| ten-gigabitEthernet** { *port* **|** *port-list* }**]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Dying Gasp and Critical Event on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ethernet-oam remote-failure dying-gasp **notify** enable

Switch(config-if)#ethernet-oam remote-failure critical-event **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Dying Gasp : Enabled

Critical Event : Enabled

...

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Configuring Remote Loopback

Follow these steps to configure Remote Loopback:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam remote-loopback received-remote-loopback {** process | ignore **}** Configure the port to ignore or to process the received remote loopback request.
Step 4	**ethernet-oam remote-loopback {** start | stop **}** Request the remote peer to start or stop the OAM remote loopback mode. The port to be configured here should be in active mode that has established OAM connection with the peer.
Step 5	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| ten-gigabitEthernet** { *port* **|** *port-list* }**]** Verify the OAM configuration.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to start the OAM remote loopback mode of the peer on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)# ethernet-oam remote-loopback start

2.2.5 Verifying OAM Connection

On privileged EXEC mode or any other configuration mode, you can use the following command to view whether the OAM connection is established with the peer. Additionally, you can view the OAM information of the local entity and the remote entity.

show ethernet-oam status [interface fastEthernet { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| ten-gigabitEthernet** { *port* **|** *port-list* }**]**

View the OAM status and the relevant information of the specified port, including the local entity and the remote entity.

The displayed OAM information of the local entity is as follows:

OAM: Displays whether OAM is enabled.

Mode: Displays OAM mode of the local entity.

Max OAMPDU: Displays the maximum size of OAMPDU.

Remote Loopback: Displays whether the local entity supports Remote Loopback.

Unidirection: Displays whether the local entity supports Unidireciton.

Link Monitoring: Displays whether the local entity supports Link Monitoring.

Variable Request: Displays whether the local entity supports Variable Request.

PDU Revision: Displays the PDU Revision of the local entity.

Operation Status: Displays the status of OAM connection, including:

Disable: OAM is disabled on the port.

LinkFault: The link between the local entity and the remote entity is down.

PassiveWait: The port is in passive mode and is waiting to see if the peer device is OAM capable.

ActiveSendLocal: The port is in active mode and is sending local information.

SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer.

SendLocalAndRemoteOK: The local device agrees the OAM peer entity.

PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity.

PeeringRemotelyRejected: The remote OAM entity rejects the local device.

NonOperHalfDuplex: Ethernet OAM is enabled but the port is in half-duplex operation. You should configure the port as a full-duplex port.

Operational: OAM connection is established with the peer and OAM works normally.

Loopback Status: Displays the loopback status, including:

No Loopback: Neither the local client nor the remote client is in the loopback mode.

Local Loopback: The local client is in the loopback mode.

Remote Loopback: The remote client is in the loopback mode.

The displayed OAM information of the remote entity is as follows:

Mode: Displays OAM mode of the local entity.

MAC Address: Displays the MAC address of the remote entity.

Vendor (OUI): Displays the Vendor's OUI of the remote entity.

Max OAMPDU: Displays the maximum size of OAMPDU.

Remote Loopback: Displays whether the remote entity supports Remote Loopback.

Unidirection: Displays whether the remote entity supports Unidireciton.

Link Monitoring: Displays whether the remote entity supports Link Monitoring.

Variable Request: Displays whether the remote entity supports Variable Request.

PDU Revision: Displays the PDU Revision of the remote entity.

Vendor Information: Displays the vendor information of the remote entity.

The following example shows how to view the OAM status of port 1/0/1:

Switch(config)#show ethernet-oam status interface gigabitEthernet 1/0/1

Gi1/0/1

Local Client

OAM : Enabled

Mode : Active

Max OAMPDU : 1518 Bytes

Remote Loopback : Supported

Unidirection : Not Supported

Link Monitoring : Supported

Variable Request : Not Supported

PDU Revision : 1

Operation Status : Operational

Loopback Status : No Loopback

Remote Client

Mode : Passive

MAC Address : 18-A6-F7-DB-63-81

Vendor(OUI) : 000aeb

Max OAMPDU : 1518 Bytes

Remote Loopback : Supported

Unidirection : Not Supported

Link Monitoring : Supported

Variable Request : Not Supported

PDU Revision : 1

Loopback Status : No Loopback

Vendor Information : 00000000

3 Viewing OAM Statistics

You can view the following OAM statistics:

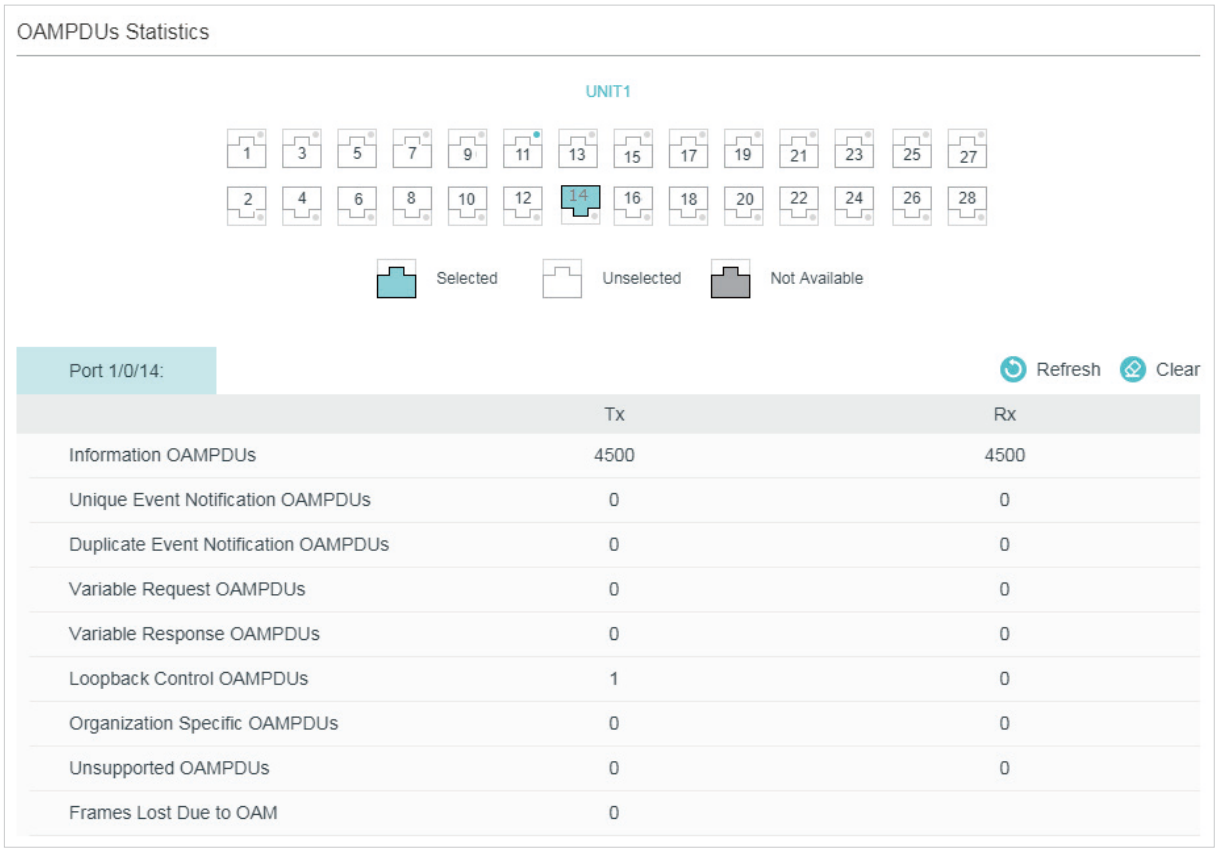
- OAMPDUs
- Event Logs

3.1 Using the GUI

3.1.1 Viewing OAMPDUs

Choose the menu **MAINTENANCE > Ethernet OAM > Statistics > OAMPDUs Statistics** to load the following page.

Figure 3-1 OAMPDUs Statistics



Select a port and view the number of different OAMPDUs transmitted and received on it:

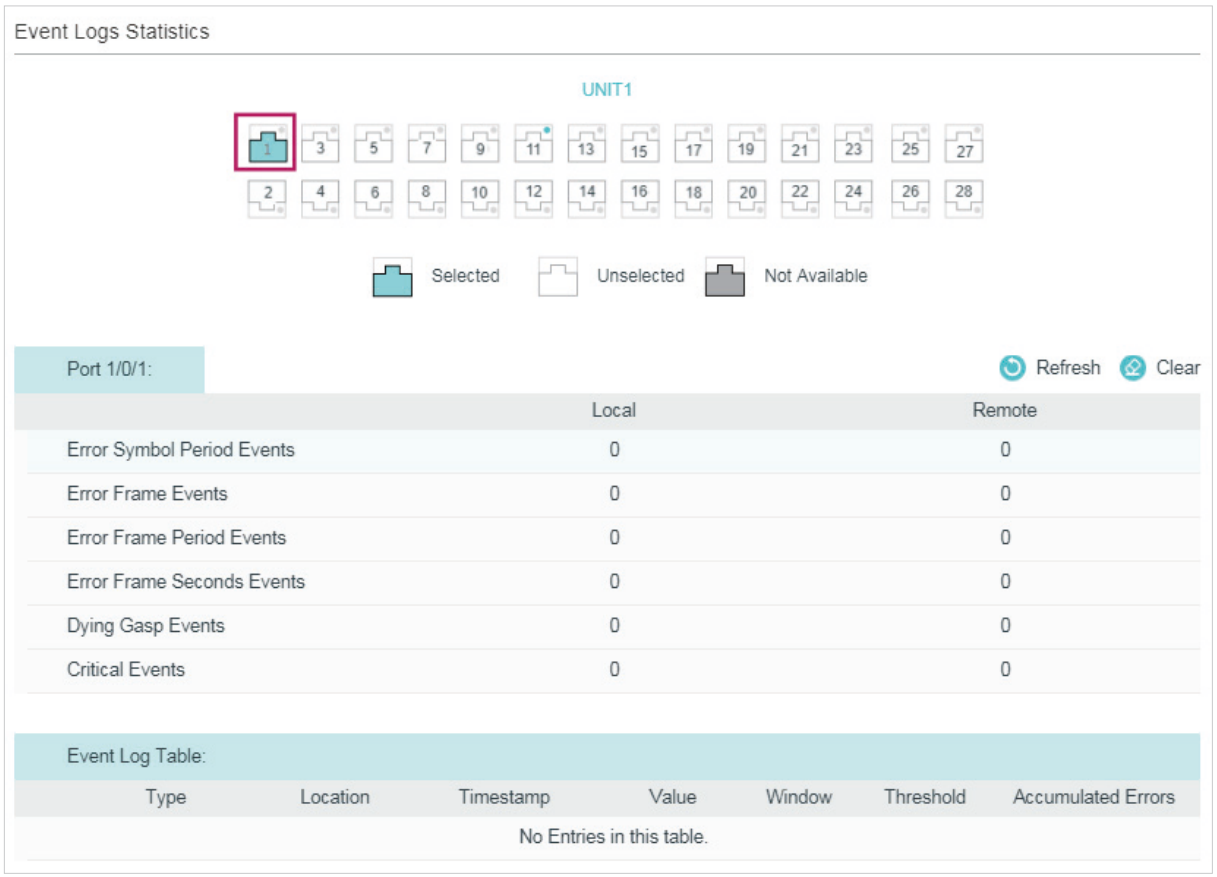
Tx	Displays the number of OAMPDUs that have been transmitted on the port.
Rx	Displays the number of OAMPDUs that have been received on the port.

Information OAMPDUs	Displays the number of Information OAMPDUs that have been transmitted or received on the port.
Unique Event Notification OAMPDUs	Displays the number of Unique Event Notification OAMPDUs that have been transmitted or received on the port.
Duplicate Event Notification OAMPDUs	Displays the number of Duplicate Event Notification OAMPDUs that have been transmitted or received on the port.
Variable Request OAMPDUs	Displays the number of Variable Request OAMPDUs that have been transmitted or received on the port.
Variable Response OAMPDUs	Displays the number of Variable Response OAMPDUs that have been transmitted or received on the port.
Loopback Control OAMPDUs	Displays the number of Loopback Control OAMPDUs that have been transmitted or received on the port.
Organization Specific OAMPDUs	Displays the number of Organization Specific OAMPDUs that have been transmitted or received on the port.
Unsupported OAMPDUs	Displays the number of Unsupported OAMPDUs that have been transmitted or received on the port.
Frames Lost Due To OAM	Displays the number of frames that are not transmitted successfully on the OAM sublayer but not due to an internal OAM error.

3.1.2 Viewing Event Logs

Choose the menu **MAINTENANCE > Ethernet OAM > Statistics > Event Logs Statistics** to load the following page.

Figure 3-2 Event Logs Statistics



Select a port and view the local and remote event logs on it.

Local	Displays the number of link events that have occurred on the local link.
Remote	Displays the number of link events that have occurred on the remote link.
Error Symbol Period Events	Displays the number of error symbol period link events that have occurred on the local link or remote link.
Error Frame Events	Displays the number of error frame link events that have occurred on the local link or remote link.
Error Frame Period Events	Displays the number of error frame period link events that have occurred on the local link or remote link.
Error Frame Seconds Events	Displays the number of error frame seconds link events that have occurred on the local link or remote link.
Dying Gasp Events	Displays the number of Dying Gasp link events that have occurred on the local link or remote link.

Critical Events	Displays the number of Critical Event link events that have occurred on the local link or remote link.

Additionally, you can view the detailed information of the event logs in the **Event Log Table** section.

Type	Displays the types of the link event.
Location	Displays the location where the link event occurred.
Timestamp	Displays the time reference when the link event occurred.
Value	Displays the number of symbol errors or frame errors in the period.
Window	Displays the period of the link event.
Threshold	Displays the threshold of the errors.
Accumulated Errors	Displays the number of errors that have been detected since the OAM feature was last reset.

3.2 Using the CLI

3.2.1 Viewing OAMPDUs

On privileged EXEC mode or any other configuration mode, you can use the following command to view the number of OAMPDUs received and sent on the specified port.

show ethernet-oam statistics [interface fastEthernet { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| ten-gigabitEthernet** { *port* **|** *port-list* }**]**

View the number of different OAMPDUs transmitted and received on the specified port, including Information OAMPDU, Unique Event Notification OAMPDU, Duplicate Event Notification OAMPDU, Loopback Control OAMPDU, Variable Request OAMPDU, Variable Response OAMPDU, Organization Specific OAMPDUs, Unsupported OAMPDU, and Frames Lost Due To OAM (frames that are not transmitted successfully on the OAM sublayer but not due to an internal OAM error).

The following example shows how to view the transmitted and received OAMDPUs on port 1/0/1.

Switch#show ethernet-oam statistics interface gigabitEthernet 1/0/1

Gi1/0/1

Information OAMPDU TX : 28

Information OAMPDU RX : 28

Unique Event Notification OAMPDU TX : 0

Unique Event Notification OAMPDU RX : 0

Duplicate Event Notification OAMPDU TX : 0

Duplicate Event Notification OAMPDU RX : 0

Loopback Control OAMPDU TX : 1

Loopback Control OAMPDU RX : 0

Variable Request OAMPDU TX : 0

Variable Request OAMPDU RX : 0

Variable Response OAMPDU TX : 0

Variable Response OAMPDU RX : 0

Organization Specific OAMPDUs TX : 0

Organization Specific OAMPDUs RX : 0

Unsupported OAMPDU TX : 0

Unsupported OAMPDU RX : 0

Frames Lost Due To OAM : 0

3.2.2 Viewing Event Logs

On privileged EXEC mode or any other configuration mode, you can use the following command to view the local and remote event logs on the specified port.

show ethernet-oam event-log [interface fastEthernet { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **| ten-gigabitEthernet** { *port* **|** *port-list* }**]**

View the local and remote event logs on the specified port.

An event list will be displayed, including the following information:

Type: Displays the type of the link event.

Location: Displays the location where the link event occurred (local or remote).

Timestamp: Displays the time reference when the link event occurred.

And the number of local and remote event logs will be displayed, including the following events:

Error Symbol Event: Displays the number of error symbol period link events that have occurred on the local link or remote link.

Error Frame Event: Displays the number of error frame link events that have occurred on the local link or remote link.

Error Frame Period Event: Displays the number of error frame period link events that have occurred on the local link or remote link.

Error Frame Seconds Event: Displays the number of error frame seconds link events that have occurred on the local link or remote link.

Dying Gasp: Displays the number of Dying Gasp link events that have occurred on the local link or remote link.

Critical Event: Displays the number of Critical Event link events that have occurred on the local link or remote link.

The following example shows how to view the event logs on port 1/0/1.

Switch#show ethernet-oam event-log interface gigabitEthernet 1/0/1

Gi1/0/1

Event Listing

Type Location Time Stamp

--- --- ---

Critical Event Remote 2016-01-01 08:08:00

Local Event Statistics

Error Symbol Event : 0

Error Frame Event : 0

Error Frame Period Event : 0

Error Frame Seconds Event : 0

Dying Gasp : 0

Critical Event : 0

Remote Event Statistics

Error Symbol Event : 0

Error Frame Event : 0

Error Frame Period Event : 0

Error Frame Seconds Event : 0

Dying Gasp : 0

Critical Event : 1

4 Configuration Example

4.1 Network Requirements

A network administrator wants to manage and troubleshoot the network more effectively, requiring that the link failure and frame errors on the link between Switch A and Switch B can be monitored and reported via the Ethernet OAM feature.

Figure 4-1 Network Topology

4.1.1 Configuration Scheme

To meet the requirement, configure OAM on port 1/0/1 of each switch. Two features can be configured: Link Monitoring and Remote Failure Indication. With Link Monitoring, the frame errors on the link can be monitored and reported; with Remote Failure Indication, the link failure can be monitored and reported.

The overview of configuration is as follows:

1) Enable OAM and configure the OAM mode for port 1/0/1 on each switch. Here we configure OAM mode of the port on Switch A as active, and that on switch B as passive.
2) Configure Link Monitoring for port 1/0/1 on each switch.
3) Configure Remote Failure Indication for port 1/0/1 on each switch.

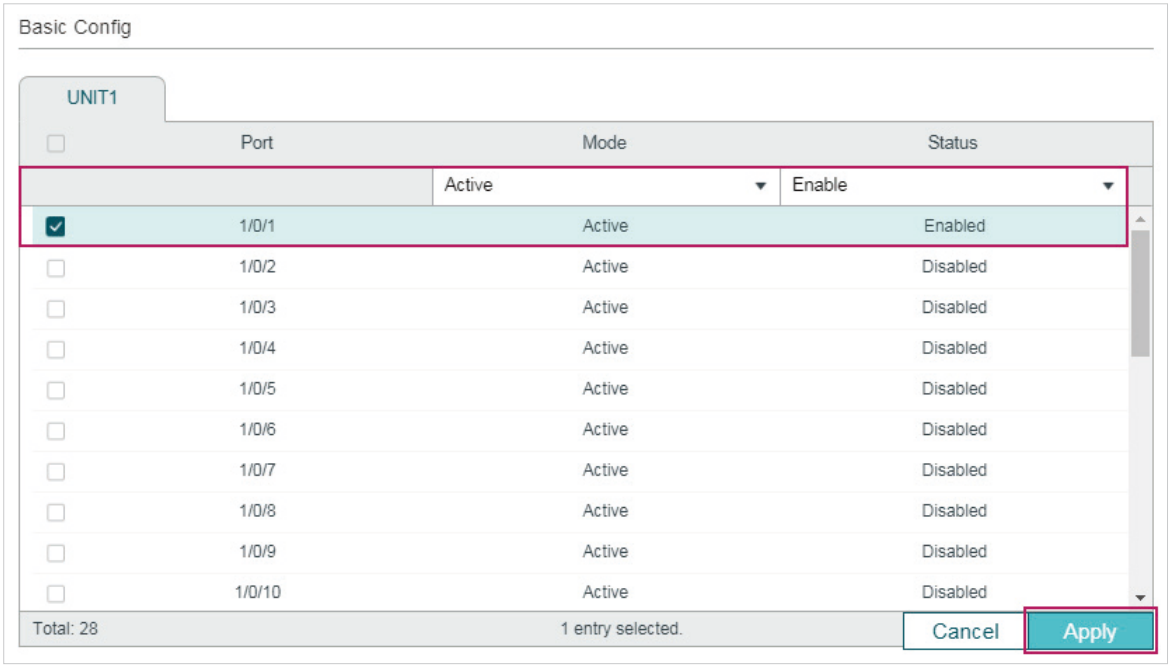
Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

4.1.2 Using the GUI

The configurations for Switch A and Switch B are similar. We take Switch A as an example.

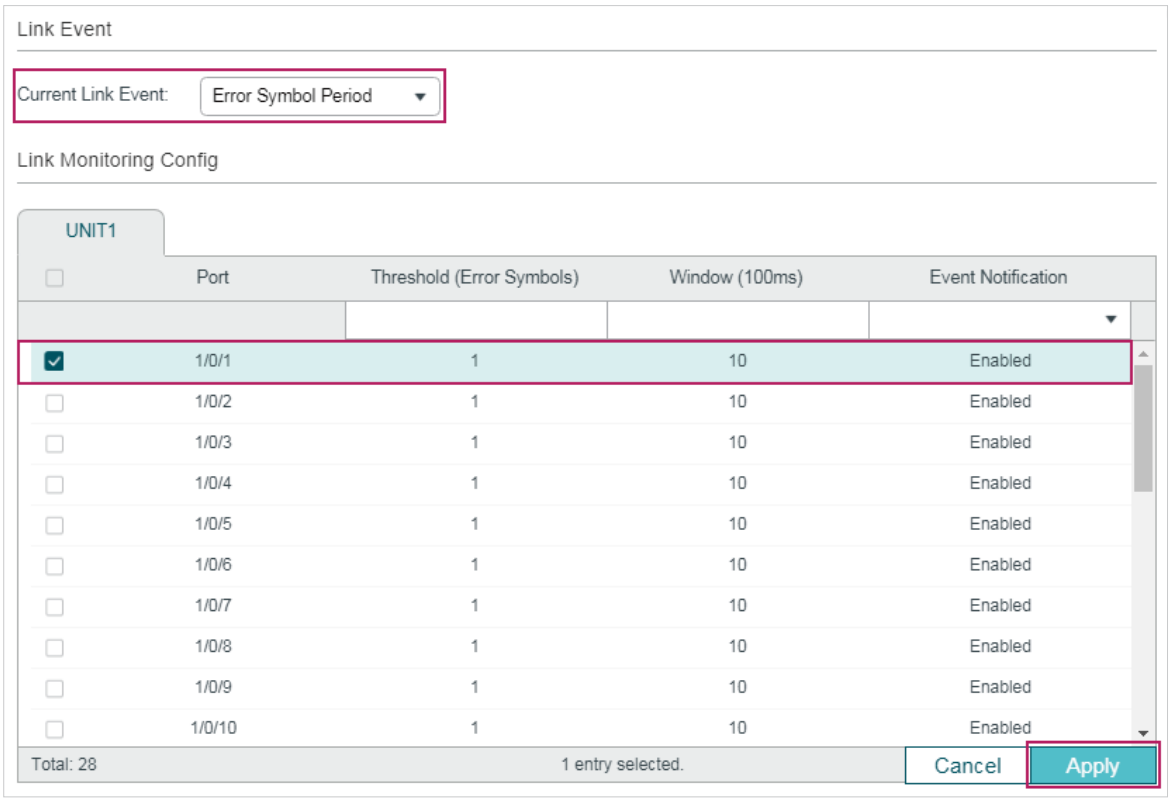
1) Choose the menu **MAINTENANCE > Ethernet OAM > Basic Config > Basic Config** to load the following page. Select port 1/0/1, and configure the mode as Active and the state as Enable. Click **Apply**.

Figure 4-2 Basic Configuration



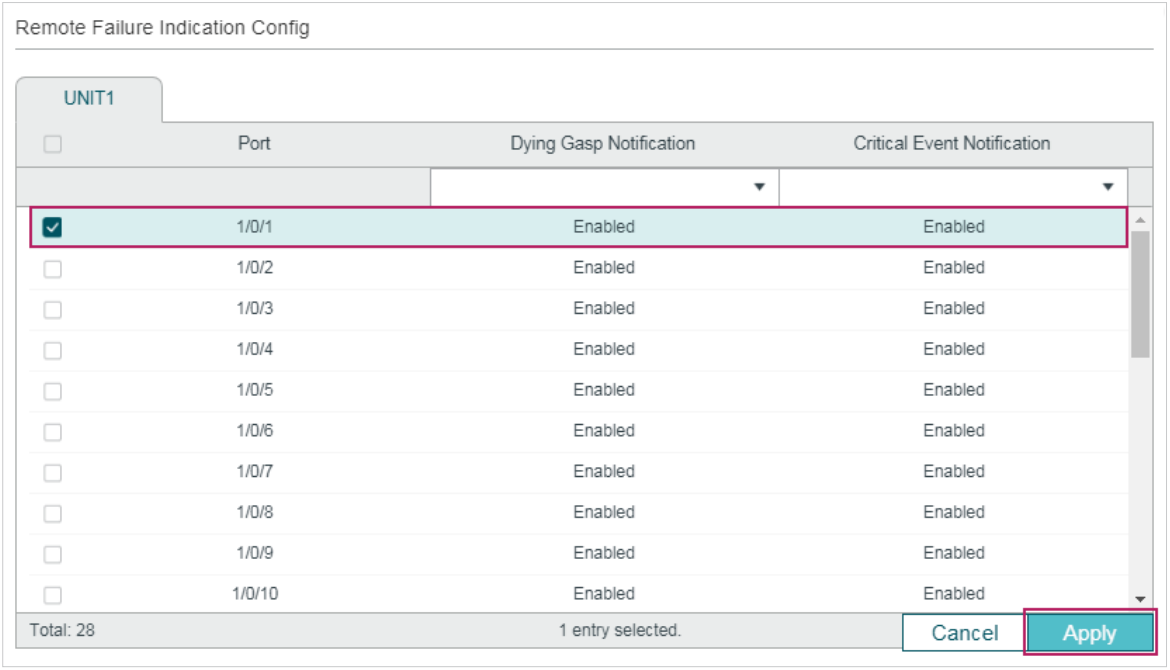
2) Choose the menu **MAINTENANCE > Ethernet OAM > Link Monitoring** to load the following page. Select each Link Event type and configure the relevant parameters on port 1/0/1. Make sure that Event Notification is enabled and specify the threshold and window according to your needs. Here we keep the default parameters. Click **Apply**.

Figure 4-3 Link Monitoring Configuration



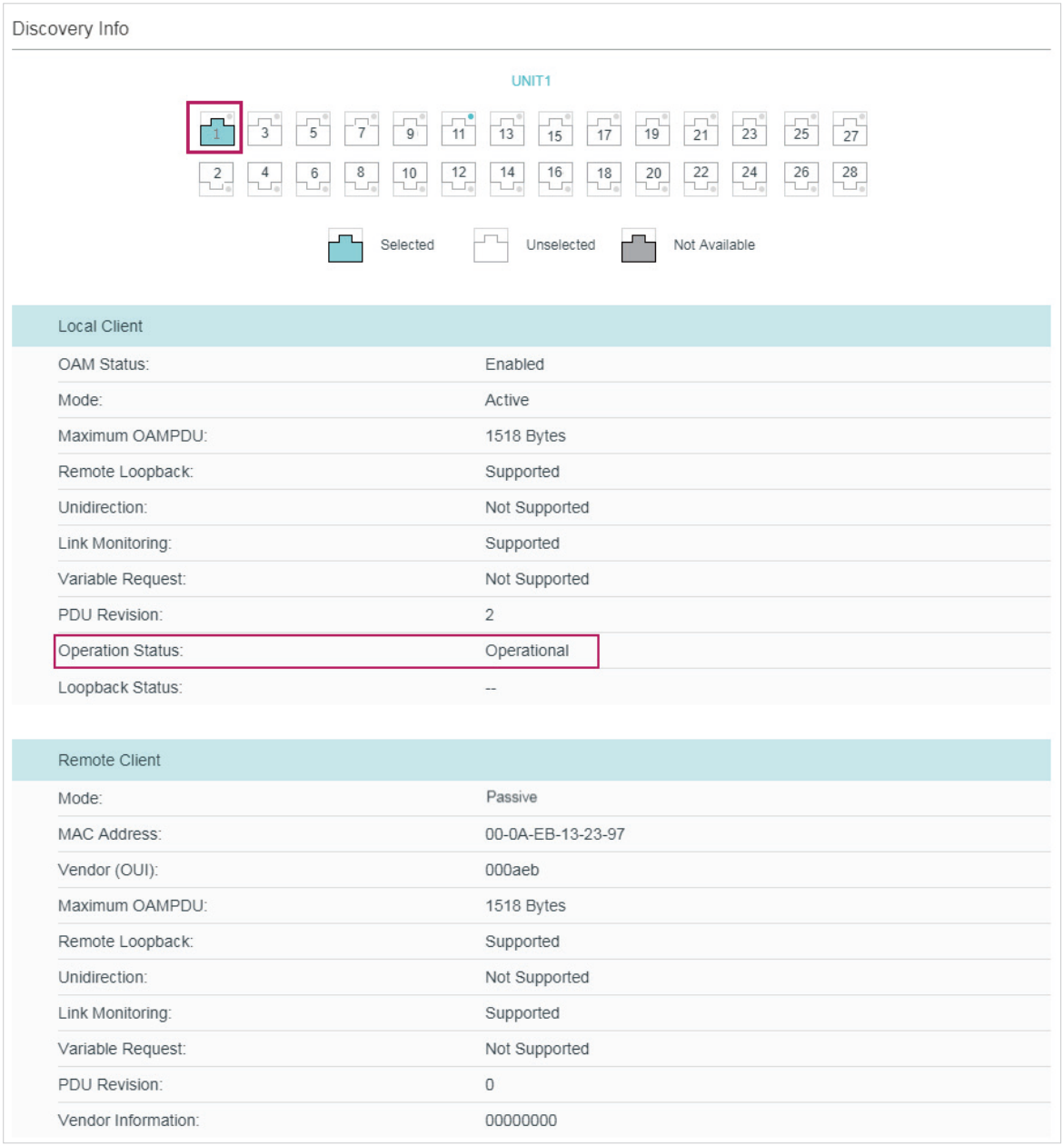
3) Choose the menu **MAINTENANCE > Ethernet OAM > Remote Failure Indication** to load the following page. Select port 1/0/1 and enable Dying Gasp Notification and Critical Event Notification. Click **Apply**.

Figure 4-4 Remote Failure Indication Configuration



4) Choose the menu **MAINTENANCE > Ethernet OAM > Basic Config > Discovery Info** to load the following page. Select port 1/0/1 to check the OAM status. When the connection status becomes **Operational**, it indicates that OAM connection has been established and OAM works normally.

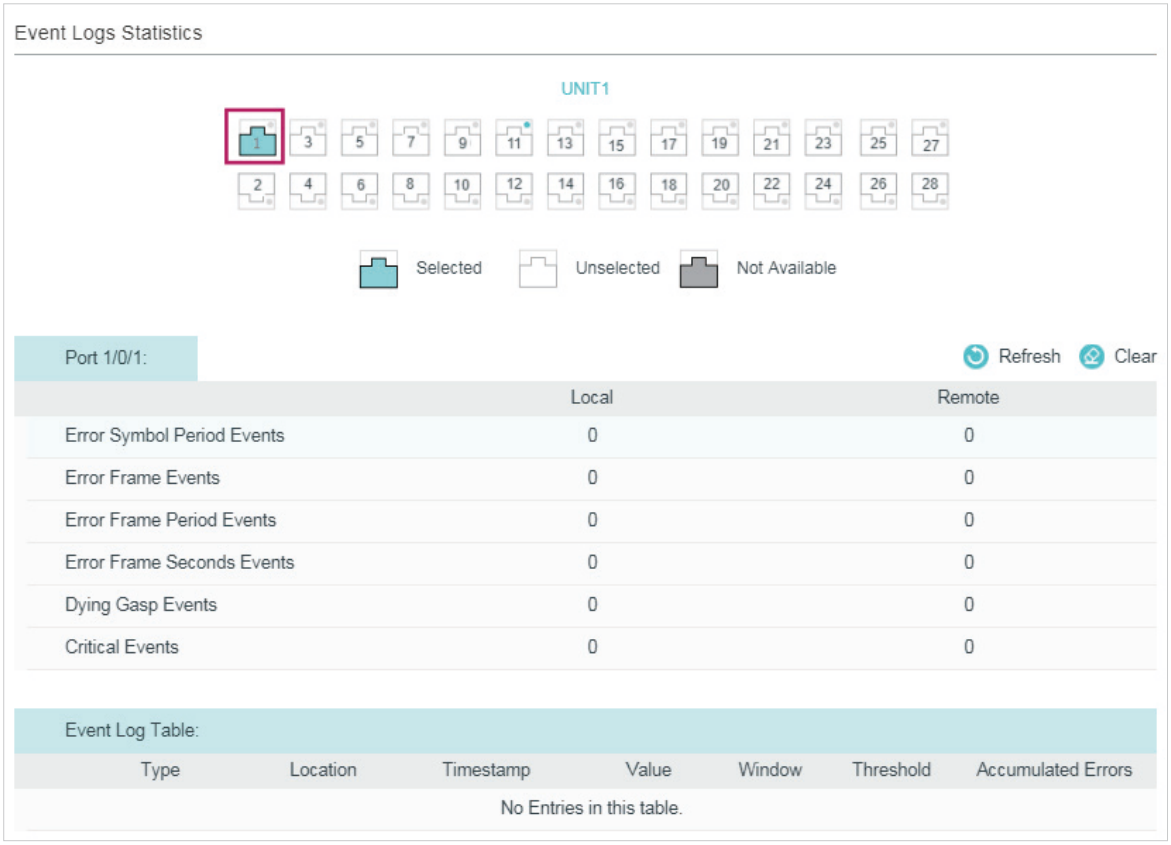
Figure 4-5 Discovery Infomation



5) Click Save to save the settings.

6) Choose the menu **MAINTENANCE > Ethernet OAM > Statistics > Event Log** to load the following page. Select port 1/0/1 to view the event logs on the port.

Figure 4-6 OAM Event Logs



4.1.3 Using the CLI

1) Enable OAM and configure OAM mode as active on port 1/0/1.

   Switch_A#configure

   Switch_A(config)# interface gigabitEthernet 1/0/1

   Switch_A(config-if)#ethernet-oam

   Switch_A(config-if)#ethernet-oam mode active

2) Configure Link Monitoring on the port. Enable Event Notification and keep the threshold and window as the default.

   Switch_A(config-if)#ethernet-oam link-monitor symbol-period notify enable

   Switch_A(config-if)#ethernet-oam link-monitor frame-period notify enable

   Switch_A(config-if)#ethernet-oam link-monitor frame notify enable

   Switch_A(config-if)#ethernet-oam link-monitor frame-seconds notify enable

3) Configure Remote Failure Indication on the port. Enable Dying Gasp Notification and Critical Event Notification.

   Switch_A(config-if)#ethernet-oam remote-failure critical-event notify enable

   Switch_A(config-if)#ethernet-oam remote-failure dying-gasp notify enable

```
Switch_A(config-if)#ethernet-oam link-monitor frame-period notify enable
Switch_A(config-if)#ethernet-oam link-monitor frame notify enable
Switch_A(config-if)#end
Switch_A#copy running-config startup-config
```

Verify the Configuration

Verify the configuration of OAM:

```
Switch_A#show ethernet-oam configuration interface gigabitEthernet 1/0/1
Gi1/0/1
------------------------------------------------------------
OAM             : Enabled
Mode            : Active
Dying Gasp      : Enabled
Critical Event  : Enabled
Remote Loopback OAMPDU : Not Processed

Symbol Period Error
 Notify State   : Enabled
 Window         : 1000 milliseconds
 Threshold      : 1 Error Symbol

Frame Error
 Notify State   : Enabled
 Window         : 1000 milliseconds
 Threshold      : 1 Error Frame

Frame Period Error
 Notify State   : Enabled
 Window         : 148810 Frames
 Threshold      : 1 Error Frame
```

Frame Seconds Error

Notify State : Enabled

Window : 60000 milliseconds

Threshold : 1 Error Seconds

Verify the OAM connection:

Switch_A#show ethernet-oam status interface gigabitEthernet 1/0/1

Gi1/0/1

Local Client

OAM : Enabled

Mode : Active

Max OAMPDU : 1518 Bytes

Remote Loopback : Supported

Unidirection : Not Supported

Link Monitoring : Supported

Variable Request : Not Supported

PDU Revision : 2

Operation Status : Operational

Loopback Status : No Loopback

Remote Client

Mode : Passive

MAC Address : 18-A6-F7-DB-63-81

Vendor(OUI) : 000aeb

Max OAMPDU : 1518 Bytes

Remote Loopback : Supported

Unidirection : Not Supported

Link Monitoring : Supported

Variable Request : Not Supported

PDU Revision : 1

Loopback Status : No Loopback

Vendor Information : 00000000

View the OAM event logs:

Switch_A#show ethernet-oam event-log interface gigabitEthernet 1/0/1

Gi1/0/1

Event Listing

Type	Location	Time Stamp
Critical Event	Remote	2016-01-01 08:08:00

Local Event Statistics

Error Symbol Event : 0

Error Frame Event : 0

Error Frame Period Event : 0

Error Frame Seconds Event : 0

Dying Gasp : 0

Critical Event : 0

Remote Event Statistics

Error Symbol Event : 0

Error Frame Event : 0

Error Frame Period Event : 0

Error Frame Seconds Event : 0

Dying Gasp : 0

Critical Event : 1

5 Appendix: Default Parameters

Default settings of Ethernet OAM are listed in the following tables.

Table 5-1 Ethernet OAM

Parameter	Default Setting
Basic Config	
Mode	Active
Status	Disabled
Link Monitoring	
Error Symbol Period	Threshold : 1 error symbol Window: 10*100 ms Event Notification: Enabled
Error Frame	Threshold : 1 error frame Window: 10*100 ms Event Notification: Enabled
Error Frame Period	Threshold : 1 error frame Window: 1488100 frames Event Notification: Enabled
Error Frame Seconds	Threshold : 1 error second Window: 600*100 ms Event Notification: Enabled
Remote Failure Indication	
Dying Gasp Notification	Enabled
Critical Event Notification	Enabled
Remote Loopback	
Received Remote Loopback	Ignore

Part 37

Configuring DLDP

CHAPTERS

1. Overview
2. DLDP Configuration
3. Appendix: Default Parameters

1 Overview

DLDP (Device Link Detection Protocol) is a Layer 2 protocol that enables devices connected through fiber or twisted-pair Ethernet cables to detect whether a unidirectional link exists.

A unidirectional link occurs whenever traffic sent by a local device is received by its peer device but traffic from the peer device is not received by the local device.

Unidirectional links can cause a variety of problems, such as spanning-tree topology loops. Once detecting a unidirectional link, DLDP can shut down the related port automatically or inform users.

2 DLDP Configuration

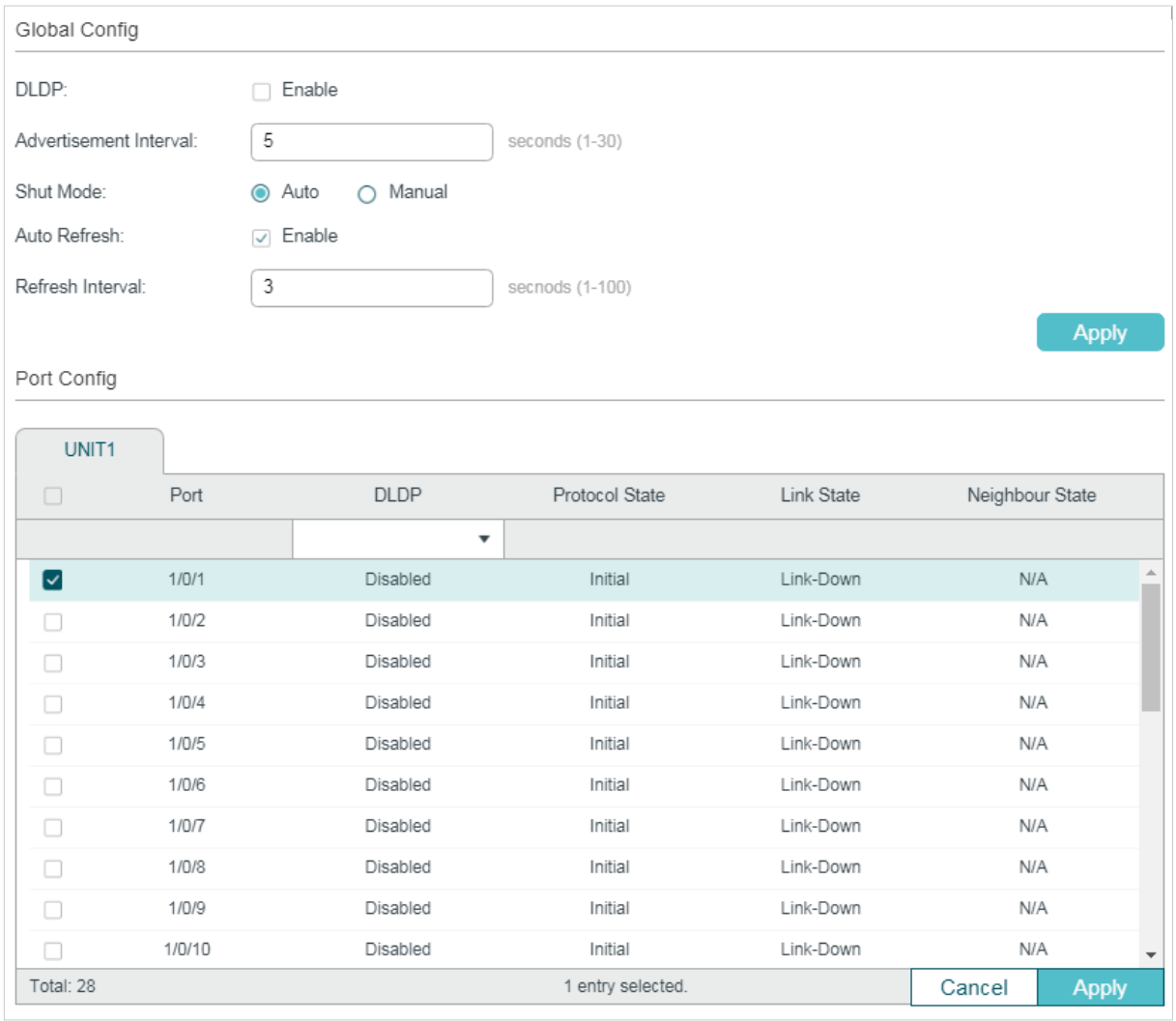
Configuration Guidelines

- A DLDP-capable port cannot detect a unidirectional link if it is connected to a DLDP-incapable port of another switch.
- To detect unidirectional links, make sure DLDP is enabled on both sides of the links.

2.1 Using the GUI

Choose the menu **MAINTENANCE > DLDP** to load the following page.

Figure 2-1 Configure DLDP



Follow these steps to configure DLDP:

1) In the **Global Config** section, enable DLDP and configure the relevant parameters. Click **Apply**.

DLDP State	Enable or disable DLDP globally.
Advertisement Interval	Configure the interval to send advertisement packets. Valid values are from 1 to 30 seconds, and the default value is 5 seconds.
Shut Mode	Choose how to shut down the port when a unidirectional link is detected: **Auto**: When a unidirectional link is detected on a port, DLDP will generate logs and traps then shut down the port, and DLDP on this port will change to Disabled. **Manual**: When a unidirectional link is detected on a port, DLDP will generate logs and traps, and then users can manually shut down the unidirectional link ports.
Auto Refresh	With this option enabled, the switch will automatically refresh the DLDP information.
Refresh Interval	Specify the time interval at which the switch will refresh the DLDP information. Valid values are from 1 to 100 seconds, and the default value is 3 seconds.

2) In the **Port Config** section, select one or more ports, enable DLDP and click **Apply**. Then you can view the relevant DLDP information in the table.

DLDP	Enable or disable DLDP on the port.
Protocol State	Displays the DLDP protocol state. **Initial**: DLDP is disabled. **Inactive**: DLDP is enabled but the link is down. **Active**: DLDP is enabled and the link is up, or the neighbor entries in this device are empty. **Advertisement**: No unidirectional link is detected (the device has established bidirectional links with all its neighbors) or DLDP has remained in an Active status for more than 5 seconds. **Probe**: In this state, the device will send out Probe packets to detect whether the link is unidirectional. The port enters this state from the Active state if it receives a packet from an unknown neighbor. **Disable**: A unidirectional link is detected.
Link State	Displays the link state. **Link-Down**: The link is down. **Link-Up**: The link is up.
Neighbour State	Displays the neighbour state. **Unknown**: Link detection is in progress. **Unidirectional**: The link between the port and the neighbor is unidirectional. **Bidirectional**: The link between the port and the neighbor is bidirectional.

2.2 Using the CLI

Follow these steps to configure DLDP:

Step 1	**configure** Enter global configuration mode.
Step 2	**dldp** Globally enable DLDP.
Step 3	**dldp interval** *interval-time* Configure the interval of sending advertisement packets on ports that are in the advertisement state. *interval-time*: Specify the interval time. The valid values are from 1 to 30 seconds. By default, it is 5 seconds.
Step 3	**dldp shut-mode** { auto | manual } Configure the DLDP shutdown mode when a unidirectional link is detected. auto: The switch automatically shuts down ports when a unidirectional link is detected. It is the default setting. manual: The switch displays an alert when a unidirectional link is detected. Then the users can manually shut down the unidirectional link ports.
Step 4	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 5	**dldp** Enable DLDP on the specified port.
Step 6	**show dldp** Verify the global DLDP configuration.
Step 7	**show dldp interface** Verify the DLDP configuration of the ports.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DLDP globally, configure the DLDP interval as 10 seconds and specify the shutdown mode as auto.

Switch#configure

Switch(config)#dldp

Switch(config)#dldp interval 10

Switch(config)#dldp shut-mode auto

Switch(config)#show dldp

DLDP Global State: Enable

DLDP Message Interval: 10

DLDP Shut Mode: Auto

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to enable DLDP on port 1/0/1.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#dldp

Switch(config-if)#show dldp interface

Port	DLDP State	Protocol State	Link State	Neighbor State
----	----------	--------------	----------	--------------
Gi1/0/1	Enable	Inactive	Link-Down	N/A
Gi1/0/2	Disable	Initial	Link-Down	N/A

...

Switch(config-if)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

Default settings of DLDP are listed in the following table.

Table 3-1 Default Settings of DLDP

Parameter	Default Setting
Global Config	
DLDP State	Disabled
Advertisement Interval	5 seconds
Shut Mode	Auto
Auto Refresh	Disabled
Refresh Interval	3 seconds
Port Config	
DLDP	Disabled

Part 38

Configuring SNMP & RMON

CHAPTERS

1. SNMP
2. SNMP Configurations
3. Notification Configurations
4. RMON
5. RMON Configurations
6. Configuration Example
7. Appendix: Default Parameters

1 SNMP

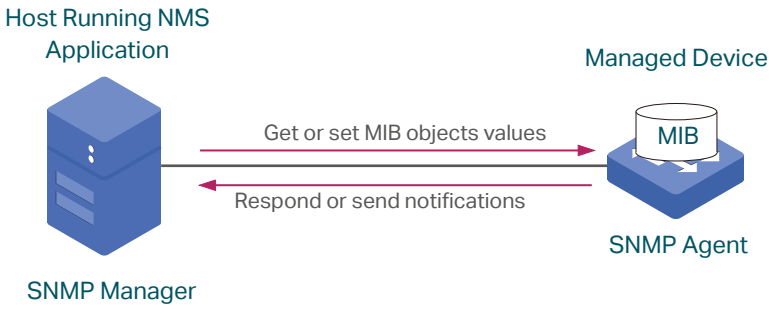
1.1 Overview

SNMP (Simple Network Management Protocol) is a standard network management protocol, widely used on TCP/IP networks. It facilitates device management using NMS (Network Management System) applications. With SNMP, network managers can view or modify the information of network devices, and timely troubleshoot according to notifications sent by those devices.

As the following figure shows, the SNMP system consists of an SNMP manager, an SNMP agent, and a MIB (Management Information Base).

The SNMP manager is a host that runs NMS applications. The agent and MIB reside on the managed device, such as the switch, router, host or printer. By configuring SNMP on the switch, you define the relationship between the manager and the agent.

Figure 1-1 SNMP System



1.2 Basic Concepts

The following basic concepts of SNMP will be introduced: SNMP manager, SNMP agent, MIB (Management Information Base), SNMP entity, SNMP engine, Notification types and SNMP version.

SNMP Manager

The SNMP manager uses SNMP to monitor and control SNMP agents, providing a friendly management interface for the administrator to manage network devices conveniently. It can get values of MIB objects from an agent or set values for them. Also, it receives notifications from the agents so as to learn the condition of the network.

SNMP Agent

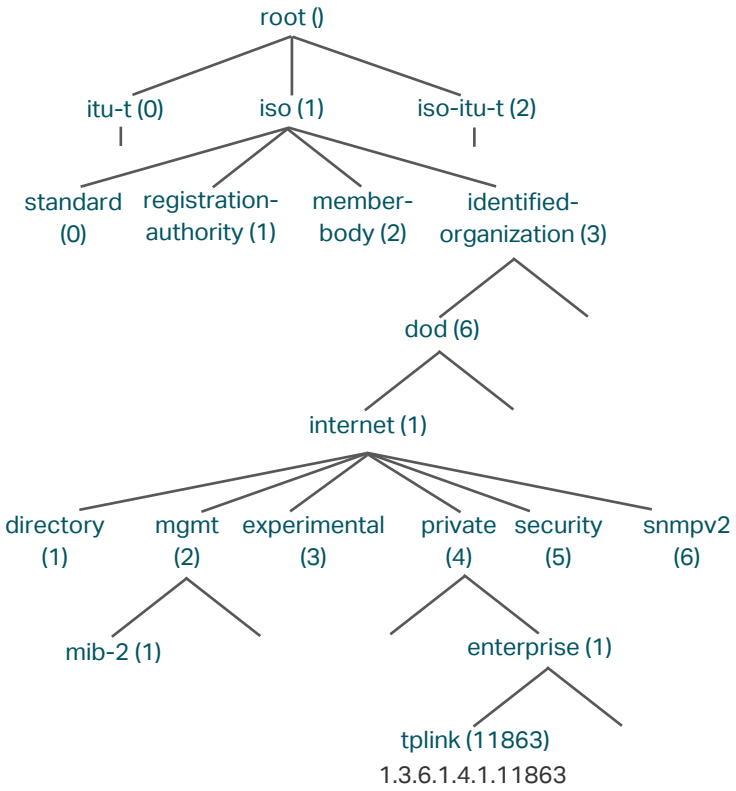
An SNMP agent is a process running on the managed device. It contains MIB objects whose values can be requested or set by the SNMP manager. An agent can send unsolicited trap messages to notify the SNMP manager that a significant event has occurred on the agent.

MIB

A MIB is a collection of managed objects that is organized hierarchically. The objects define the attributes of the managed device, including the names, status, access rights, and data types. Each object can be addressed through an object identifier (OID).

As the following figure shows, the MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. The top-level MIB object IDs belong to different standard organizations, while lower-level object IDs are allocated by associated organizations. Vendors can define private branches that include managed objects for their own products.

Figure 1-2 MIB Tree



TP-Link switches provide private MIBs that can be identified by the OID 1.3.6.1.4.1.11863. The MIB file can be found on the provided CD or in the download center of our official website: https://www.tp-link.com/download-center.html.

Also, TP-Link switches support the following public MIBs:

- LLDP.mib
- LLDP-Ext-Dot1.mib
- LLDP-Ext-MED.mib
- RFC1213.mib
- RFC1493-Bridge.mib
- RFC1757-RMON.mib
- RFC2618-RADIUS-Auth-Client.mib

- RFC2620-RADIUS-Acc-Client.mib
- RFC2674-pBridge.mib
- RFC2674-qBridge.mib
- RFC2863-pBridge.mib
- RFC2925-Disman-Ping.mib
- RFC2925-Disman-Traceroute.mib

For detail information about the supported public MIBs, see Supported Public MIBs for TP-Link Switches.

SNMP Entity

An SNMP entity is a device running the SNMP protocol. Both the SNMP manager and SNMP agent are SNMP entities.

SNMP Engine

An SNMP engine is a part of the SNMP entity. Every SNMP entity has one and only one engine. An SNMP engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine can be uniquely identified by an engine ID within an administrative domain. Since there is a one-to-one association between SNMP engines and SNMP entities, we can also use the engine ID to uniquely identify the SNMP entity within that administrative domain.

Notification Types

Notifications are messages that the switch sends to the NMS host when important events occur. Notifications facilitate the monitoring and management of the NMS. There are two types of notifications:

- **Trap:** When the NMS host receives a Trap message, it will not send a response to the switch. Thus the switch cannot tell whether a message is received or not, and the messages that are not received will not be resent.
- **Inform:** When the NMS host receives an Inform message, it sends a response to the switch. If the switch does not receive any response within the timeout interval, it will resend the Inform message. Therefore, Inform is more reliable than Trap.

SNMP Version

The device supports three SNMP versions with the security level from low to high: SNMPv1, SNMPv2c and SNMPv3. Table 1-1 lists features supported by different SNMP versions, and Table 1-2 shows corresponding application scenarios.

Table 1-1 Features Supported by Different SNMP Versions

Feature	SNMPv1	SNMPv2c	SNMPv3
Access Control	Based on SNMP Community and MIB View	Based on SNMP Community and MIB View	Based on SNMP User, Group, and MIB View
Authentication and Privacy	Based on Community Name	Based on Community Name	Supported authentication and privacy modes are as follows: Authentication: MD5/SHA Privacy: DES
Trap	Supported	Supported	Supported
Inform	Not supported	Supported	Supported

Table 1-2 Application Scenarios of Different Versions

Version	Application Scenario
SNMPv1	SNMPv1 is applicable to small-scale networks with simple networking, good stability and low security requirements, such as campus networks and small enterprise networks.
SNMPv2c	SNMPv2c is applicable to medium and large-scale networks with low security requirements (or are already secure enough like VPN networks) and heavy traffic. The added feature Inform helps to ensure that the notifications from the switch are received by the NMS host even when network congestion occurs.
SNMPv3	SNMPv3 is applicable to networks of various scales, particularly those that have high security requirements and require devices to be managed by authenticated administrators (such as when data needs to be transferred on public networks).

2 SNMP Configurations

To complete the SNMP configuration, choose an SNMP version according to network requirements and supportability of the NMS application, and then follow these steps:

- Choose SNMPv1 or SNMPv2c

1) Enable SNMP.
2) Create an SNMP view for managed objects.
3) Create a community, specify the accessible view and the corresponding access rights.

- Choose SNMPv3

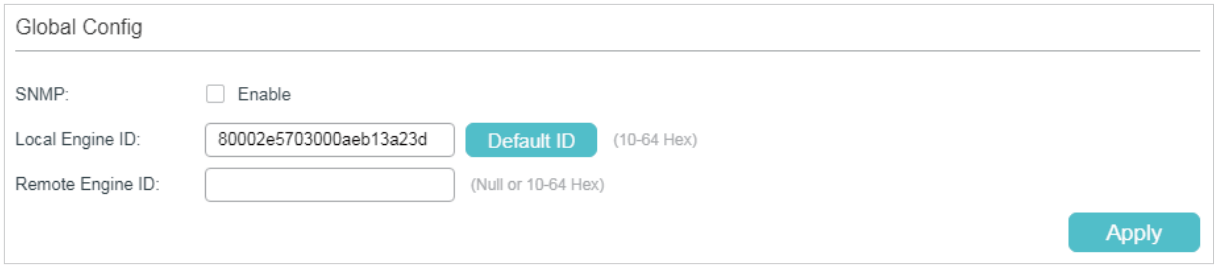
1) Enable SNMP.
2) Create an SNMP view for managed objects.
3) Create an SNMP group, and specify the security level and accessible view.
4) Create SNMP users, and configure the authentication mode, privacy mode and corresponding passwords.

2.1 Using the GUI

2.1.1 Enabling SNMP

Choose the **MAINTENANCE > SNMP > Global Config** to load the following page.

Figure 2-1 Configuring Global Parameters



Follow these steps to configure SNMP globally:

1) In the **Global Config** section, enable SNMP and configure the local and remote engine ID.

SNMP	Enable or disable SNMP globally.

Local Engine ID	Set the engine ID of the local SNMP agent (the switch) with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. By default, the switch generates the engine ID using TP-Link's enterprise number (80002e5703) and its own MAC address. The local engine ID is a unique alphanumeric string used to identify the SNMP engine. As an SNMP agent contains only one SNMP engine, the local engine ID can uniquely identify the SNMP agent.
Remote Engine ID	Set the engine ID of the remote SNMP manager with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. If no remote SNMP manager is needed, you can leave this field empty. The remote engine ID is a unique alphanumeric string. It is used to identify the SNMP engine on the remote device that receives Inform messages from the switch.

2) Click **Apply**.

Note:

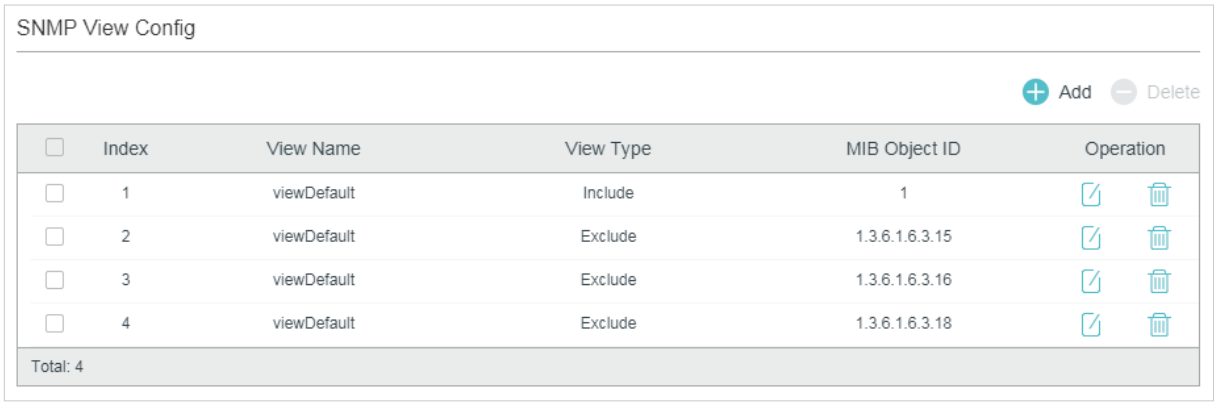
In SNMPv3, changing the value of the SNMP engine ID has important side effects. A user's password is converted to an MD5 or SHA security digest based on the password itself and the engine ID. If the value of local engine ID changes, the switch will automatically delete all SNMPv3 local users as their security digests become invalid. Similarly, all SNMPv3 remote users will be deleted if the value of remote engine ID changes.

2.1.2 Creating an SNMP View

An SNMP view is a subnet of a MIB. NMS manages MIB objects based on the view. The system has a default view named viewDefault. You can create a new one or edit the default view according to your needs.

Choose the menu **MAINTENANCE > SNMP > Global Config** to load the following page.

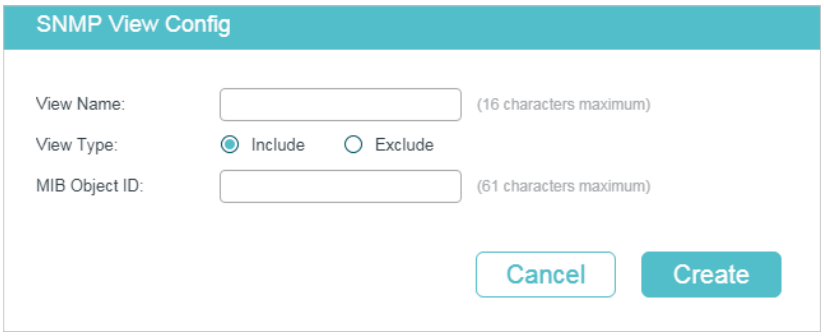
Figure 2-2 SNMP View Config



Follow these steps to create an SNMP view:

1) Click Add to load the following page. Enter a view name, and specify the view type and a MIB object ID that is related to the view.

Figure 2-3 Creating an SNMP View



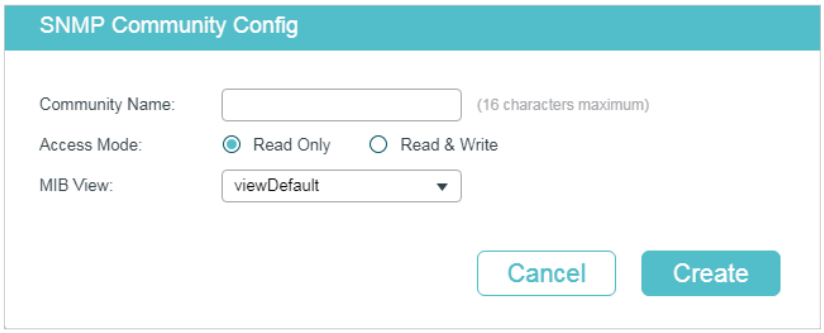
View Name	Set the view name with 1 to 16 characters. A complete view consists of all MIB objects that have the same view name.
View Type	Set the view to include or exclude the related MIB object. **Include:** The NMS can view or manage the function indicated by the object. **Exclude:** The NMS cannot view or manage the function indicated by the object.
MIB Object ID	Enter a MIB Object ID to specify a specific function of the device. When a MIB Object ID is specified, all its child Object IDs are specified. For specific ID rules, refer to the device related MIBs.

2) Click **Create**.

2.1.3 Creating SNMP Communities (For SNMP v1/v2c)

Choose the menu **MAINTENANCE > SNMP > SNMP v1/v2c** and click Add to load the following page.

Figure 2-4 Creating an SNMP Community



Follow these steps to create an SNMP community:

1) Set the community name, access rights and the related view.

Community Name	Configure the community name. This community name is used like a password and the NMS can access the specified MIB objects of the switch using the same community name.

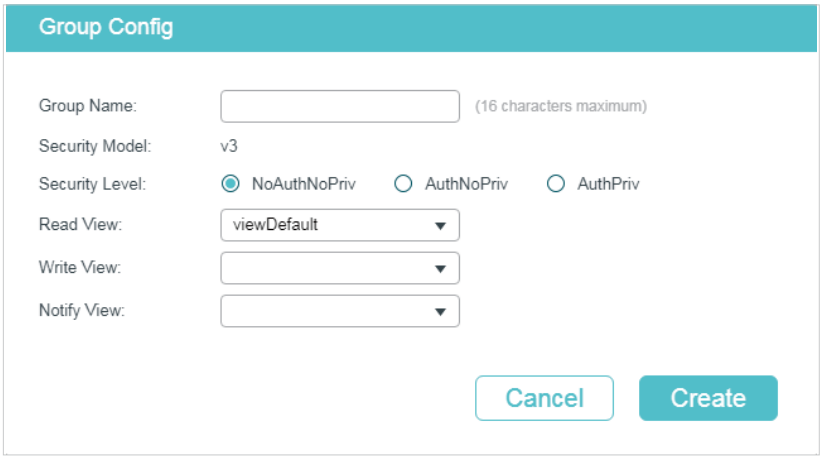
Access Mode	Specify the access right to the related view. **Read Only:** The NMS can view but not modify parameters of the specified view. **Read & Write:** The NMS can view and modify parameters of the specified view.
MIB View	Choose an SNMP view that allows the community to access.

2) Click **Create**.

2.1.4 Creating an SNMP Group (For SNMP v3)

Choose the menu **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** and click Add to load the following page.

Figure 2-5 Creating an SNMP Group



Follow these steps to create an SNMP Group and configure related parameters.

1) Assign a name to the group, then set the security level and the read view, write view and notify view.

Group Name	Set the SNMP group name using 1 to 16 characters. The identifier of a group consists of a group name, security model and security level. Groups of the same identifier are recognized as being in the same group.
Security Model	Displays the security model. SNMPv3 uses v3, the most secure model.
Security Level	Set the security level for the SNMPv3 group. **NoAuthNoPriv:** No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them. **AuthNoPriv:** An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them. **AuthPriv:** An authentication algorithm and a privacy algorithm are applied to check and encrypt packets.

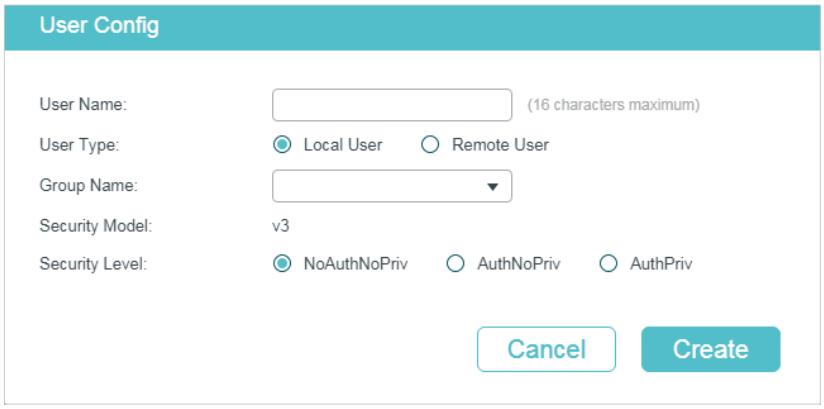
Read View	Choose a view to allow parameters to be viewed but not modified by the NMS. The view is necessary for any group.
Write View	Choose a view to allow parameters to be modified by the NMS. The view in Write View should also be added to Read View.
Notify View	Choose a view to allow it to send notifications to the NMS.

2) Click **Create**.

2.1.5 Creating SNMP Users (For SNMP v3)

Choose the menu **MAINTENANCE > SNMP > SNMP v3 > SNMP User** and click Add to load the following page.

Figure 2-6 Creating an SNMP User



Follow these steps to create an SNMP user:

1) Specify the user name and user type as well as the group which the user belongs to. Then configure the security level.

User Name	Set the SNMP user name using 1 to 16 characters. For different entries, user names cannot be the same.
User Type	Choose a user type based on the location of the user. **Local User:** The user resides on the local engine, which is the SNMP agent of the switch. **Remote User:** The user resides on the NMS. Before configuring a remote user, you need to set the remote engine ID first. The remote engine ID and user password are used when computing the authentication and privacy digests.
Group Name	Choose the name of the group that the user belongs to. Users with the same Group Name, Security Model and Security Level will be in the same group.
Security Model	Displays the security model. SNMPv3 uses v3, the most secure model.

Security Level	Set the security level. The security level from lowest to highest is: NoAuthNoPriv, AuthNoPriv, AuthPriv. The security level of the user should not be lower than the group it belongs to. **NoAuthNoPriv:** No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them. **AuthNoPriv:** An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them. **AuthPriv:** An authentication algorithm and a privacy algorithm are applied to check and encrypt packets.

2) If you have chosen **AuthNoPriv** or **AuthPriv** as the security level, you need to set corresponding Authentication Mode or Privacy Mode. If not, skip this step.

Authentication Mode	With AuthNoPriv or AuthPriv selected, configure the authentication mode and password for authentication. Two authentication modes are provided: **MD5:** Enable the HMAC-MD5 algorithm for authentication. **SHA:** Enable the SHA (Secure Hash Algorithm) algorithm for authentication. SHA algorithm is securer than MD5 algorithm.
Authentication Password	Set the password for authentication.
Privacy Mode	With AuthPriv selected, configure the privacy mode and password for encryption. The switch uses the DES (Data Encryption Standard) algorithm for encryption.
Privacy Password	Set the password for encryption.

3) Click **Create**.

2.2 Using the CLI

2.2.1 Enabling SNMP

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**snmp-server** Enabling SNMP.

Step 3	**snmp-server engineID** {[**local** *local-engineID*] [**remote** *remote-engineID*]} Configure the local engine ID and the remote engine ID. *local-engineID:* Enter the engine ID of the local SNMP agent (the switch) with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. By default, the switch generates the engine ID using TP-Link's enterprise number (80002e5703) and its own MAC address. The local engine ID is a unique alphanumeric string used to identify the SNMP engine. As an SNMP agent contains only one SNMP engine, the local engine ID can uniquely identify the SNMP agent. *remote-engineID:* Enter the remote engine ID with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. The remote engine ID is a unique alphanumeric string. It is used to identify the SNMP engine on the remote device that receives inform messages from switch. *Note:* In SNMPv3, changing the value of the SNMP engine ID has important side effects. A user's password is converted to an MD5 or SHA security digest based on the password itself and the engine ID. If the value of local engine ID changes, the switch will automatically delete all SNMPv3 local users as their security digests become invalid. Similarly, all SNMPv3 remote users will be deleted if the value of remote engine ID changes.
Step 4	**show snmp-server** Displays the global settings of SNMP.
Step 5	**show smnp-server engineID** Displays the engine ID of SNMP.
Step 6	**end** Return to Privileged EXEC Mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable SNMP and set 123456789a as the remote engine ID:

Switch#configure

Switch(config)#snmp-server

Switch(config)#snmp-server engineID remote 123456789a

Switch(config)#show snmp-server

SNMP agent is enabled.

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 SNMP packets output

0 Too big errors (Maximum packet size 1500)

0 No such name errors

0 Bad value errors

0 General errors

0 Response PDUs

0 Trap PDUs

Switch(config)#show snmp-server engineID

Local engine ID: 80002e5703000aeb13a23d

Remote engine ID: 123456789a

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Creating an SNMP View

Specify the OID (Object Identifier) of the view to determine objects to be managed.

Step 1	**configure** Enter Global Configuration Mode.

Step 2	**snmp-server view** *name mib-oid* {include | exclude} Configure the view. *name:* Enter a view name with 1 to 16 characters. You can create multiple entries with each associated to a MIB object. A complete view consists of all MIB objects that have the same view name. *mib-oid:* Enter the MIB object ID with 1 to 61 characters. When a MIB Object ID is specified, all its child Object IDs are specified. For specific ID rules, refer to the device related MIBs. include | exclude: Specify a view type. Include indicates that objects of the view can be managed by the NMS, while exclude indicates that objects of the view cannot be managed by the NMS.
Step 3	**show snmp-server view** Displays the view table.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set a view to allow the NMS to manage all function. Name the view as View:

Switch#configure

Switch(config)#snmp-server view View 1 include

Switch(config)#show snmp-server view

No. View Name Type MOID

--- ---------- ------- ----

1 viewDefault include 1

2 viewDefault exclude 1.3.6.1.6.3.15

3 viewDefault exclude 1.3.6.1.6.3.16

4 viewDefault exclude 1.3.6.1.6.3.18

5 View include 1

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Creating SNMP Communities (For SNMP v1/v2c)

For SNMPv1 and SNMPv2c the Community Name is used for authentication, functioning as the password.

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**snmp-server community** *name* { read-only | read-write } [*mib-view*] Configure the community. *name:* Enter a group name with 1 to 16 characters. *read-only* | *read-write:* Choose an access permissions for the community. Read-only indicates that the NMS can view but cannot modify parameters of the view, while read-write indicates that the NMS can both view and modify. *mib-view:* Enter a view to allow it to be accessed by the community. The name contains 1 to 61 characters. The default view is viewDefault.
Step 3	**show snmp-server community** Displays community entries.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set an SNMP community. Name the community as the nms-monitor, and allow the NMS to view and modify parameters of View:

Switch#configure

Switch(config)#snmp-server community nms-monitor read-write View

Switch(config)#show snmp-server community

Index	Name	Type	MIB-View
-----	----------	----------	--------
1	nms-monitor	read-write	View

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Creating an SNMP Group (For SNMPv3)

Create an SNMP group and set user access control with read, write and notify views. Meanwhile, set the authentication and privacy modes to secure the communication between the NMS and managed devices.

Step 1	**configure** Enter Global Configuration Mode.

Step 2	**snmp-server group** *name* [**smode** v3] [**slev** {noAuthNoPriv | authNoPriv | authPriv}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] Create an SNMP group. *name:* Enter the group name with 1 to 16 characters. The identifier of a group consists of a group name, security model and security level. Groups of the same identifier are recognized as being in the same group. v3: Configure the security model for the group. v3 indicates SNMPv3, the most secure model. noAuthNoPriv | authNoPriv | authPriv: Choose a security level. The security levels are sorted from low to high, and the default is noAuthNoPriv. noAuthNoPriv indicates no authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them. authNoPriv indicates an authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them. authPriv indicates an authentication algorithm and a privacy algorithm are applied to check and encrypt packets. *read-view:* Set the view to be the Read view. Then the NMS can view parameters of the specified view. *write-view:* Set the view to be the Write view. Then the NMS can modify parameters of the specified view. Note that the view in the Write view should also be in the Read view. *notify-view:* Set the view to be the Notify view. Then the NMS can get notifications of the specified view from the agent.
Step 3	**show snmp-server group** Displays SNMP group entries.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an SNMPv3 group with the group name as nms1, the security level as authPriv, and the Read and Notify view are both View:

Switch#configure

Switch(config)#snmp-server group nms1 **smode** v3 **slev** authPriv **read** View **notify** View

Switch(config)#show snmp-server group

No.	Name	Sec-Mode	Sec-Lev	Read-View	Write-View	Notify-View
---	--------	----------	----------	----------	----------	----------
1	nms1	v3	authPriv	View		View

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Creating SNMP Users (For SNMPv3)

Create SNMP users and add them to the SNMP group. Users in the same group have the same access rights which are controlled by the read, write and notify views of the group.

Step 1	**configure** Enter Global Configuration Mode.
Step 2	Choose a security level for the user and run the corresponding command to create the user. The security levels from low to high are NoAuthNoPriv, AuthNoPriv, and AuthPriv. The security level of a user should not be lower than that of the group it belongs to. To create a user with the security level as NoAuthNoPriv: **snmp-server user** *name* { local | remote } *group-name* [**smode** v3] **slev** noAuthNoPriv *name:* Enter the user name with 1 to 16 characters. local | remote: Choose a user type based on the location of the user. Local indicates that the user resides on the local SNMP engine (the switch), while remote indicates that the user resides on the NMS. Before configuring a remote user, you need to set the remote engine ID first. The remote engine ID and user password are used when computing the authentication and privacy digests. *group-name:* Enter the name of the group which the user belongs to. Users with the same Group Name, Security Model and Security Level will be in the same group. v3*:* Configure the security model for the user. v3 indicates SNMPv3, the most secure model. noAuthNoPriv: Configure the security level as noAuthNoPriv. For this level, no authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them. To create a user with the security level as AuthNoPriv: **snmp-server user** *name* { local | remote } *group-name* [**smode** v3] **slev** authNoPriv **cmode** {MD5 | SHA } **cpwd** *confirm-pwd* authNoPriv: Configure the security level as authNoPriv. For this level, an authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them. MD5 | SHA: Choose an authentication algorithm when the security level is set as **authNoPriv** or **authPriv**. SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is none. *confirm-pwd:* Enter an authentication password with 1 to 16 characters excluding question mark and space. This password in the configuration file will be displayed in the symmetric encrypted form. To create a user with the security as AuthPriv: **snmp-server user** *name* { local | remote } *group-name* [**smode** v3] **slev** authPriv **cmode** {MD5 | SHA } **cpwd** *confirm-pwd* **emode** DES **epwd** *encrypt-pwd* authPriv: Configure the security level as authPriv. For this level, an authentication algorithm and a privacy algorithm are applied to check and encrypt packets. DES: Configure the privacy mode as DES. The switch will use the DES algorithm to encrypt the packets. By default, the Privacy Mode is none. *encrypt-pwd:* Enter a privacy password with 1 to 16 characters excluding question mark and space. This password in the configuration file will be displayed in the symmetric encrypted form.

Step 3	**show snmp-server user** Displays the information of SNMP users.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a remote SNMP user named admin and add it to group nms1. The security settings are as Table 2-1:

Table 2-1 Security Settings for the User

Parameter	Value
Security Level	v3
Authentication Mode	SHA
Authentication Password	1234
Privacy Mode	DES
Privacy Password	5678

Switch#configure

Switch(config)#snmp-server user admin remote nms1 **smode** v3 **slev** authPriv **cmode** SHA **cpwd** 1234 **emode** DES **epwd** 5678

Switch(config)#show snmp-server user

No.	U-Name	U-Type	G-Name	S-Mode	S-Lev	A-Mode	P-Mode
---	------	------	------	------	-----	------	------
1	admin	remote	nms1	v3	authPriv	SHA	DES

Switch(config)#end

Switch#copy running-config startup-config

3 Notification Configurations

With Notification enabled, the switch can send notifications to the NMS about important events relating to the device's operation. This facilitates the monitoring and management of the NMS.

To configure SNMP notification, follow these steps:

1) Configure the information of NMS hosts.
2) Enable SNMP traps.

Configuration Guidelines

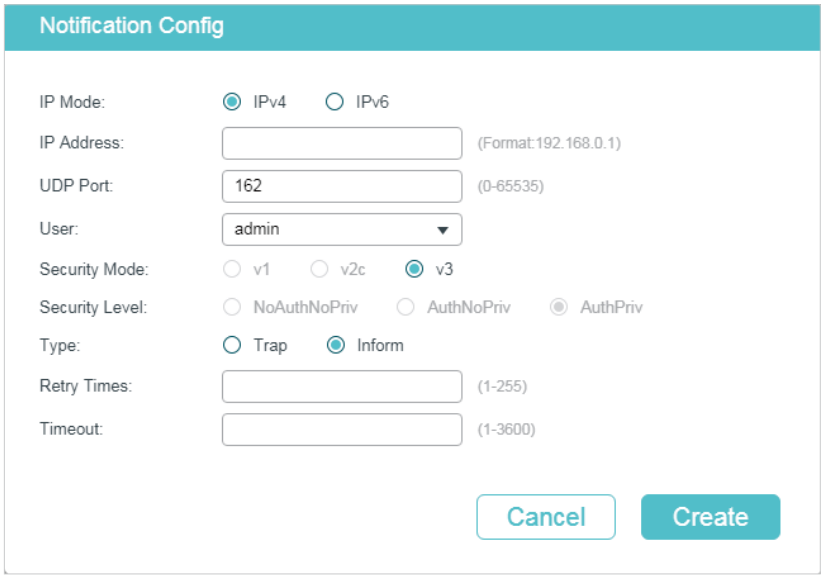
To guarantee the communication between the switch and the NMS, ensure the switch and the NMS can reach one another.

3.1 Using the GUI

3.1.1 Configuring the Information of NMS Hosts

Choose the menu **MAINTENANCE > SNMP > Notification > Notification Config** and click Add to load the following page.

Figure 3-1 Adding an NMS Host



Follow these steps to add an NMS host:

1) Choose the IP mode according to the network environment, and specify the IP address of the NMS host and the UDP port that receives notifications.

IP Mode	Choose an IP mode for the NMS host.
IP Address	If you set IP Mode as IPv4, specify an IPv4 address for the NMS host. If you set IP Mode as IPv6, specify an IPv6 address for the NMS host.
UDP Port	Specify a UDP port on the NMS host to receive notifications. For security, we recommend that you change the port number under the condition that communications on other UDP ports are not affected.

2) Specify the user name or community name used by the NMS host, and configure the security model and security level based on the user or community.

User	Choose the user name or community name used by the NMS host.
Security Model	If a community name (created for SNMPv1/v2c) is selected in User, specify the security model as v1 or v2c. If a user name (created for SNMPv3) is selected in User, here displays the security model as v3. *Note:* The NMS host should use the corresponding SNMP version.
Security Level	If Security model is v3, here displays the security level of the user.

3) Choose a notification type based on the SNMP version. If you choose the Inform type, you need to set retry times and timeout interval.

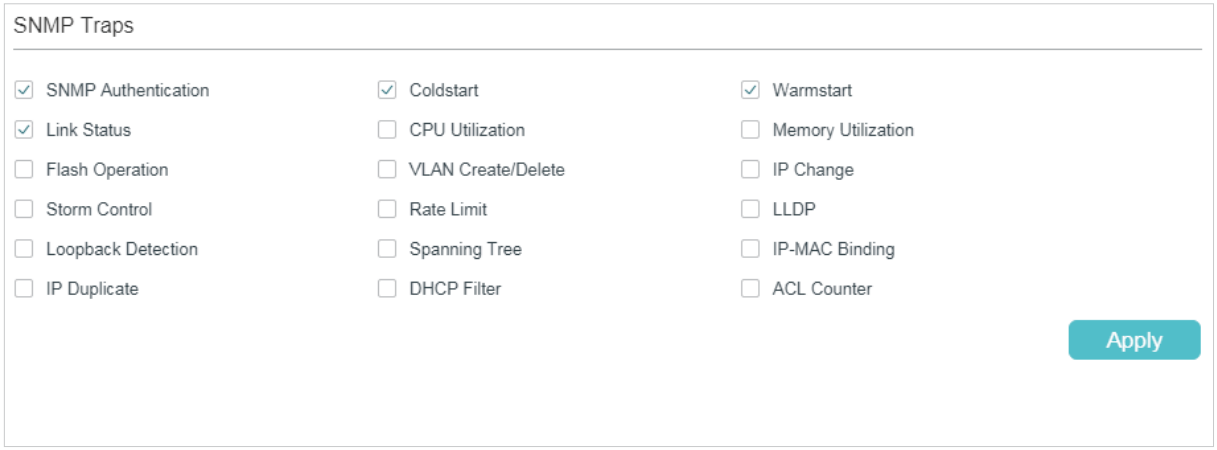
Type	Choose a notification type for the NMS host. For SNMPv1, the supported type is Trap. For SNMPv2c and SNMPv3, you can configure the type as Trap or Inform. **Trap:** The switch will send Trap messages to the NMS host when certain events occur. When the NMS host receives a Trap message, it will not send a response to the switch. Thus the switch cannot tell whether a message is received or not, and the messages that are not received will not be resent. **Inform:** The switch will send Inform messages to the NMS host when certain events occur. When the NMS host receives an Inform message, it sends a response to the switch. If the switch does not receive any response within the timeout interval, it will resend the Inform message. Therefore, Inform is more reliable than Trap.
Retry	Set the retry times for Informs. The switch will resend the Inform message if it does not receive any response from the NMS host within the timeout interval. It will stop sending Inform messages when the retry time reaches the limit.
Timeout	Set the time that the switch waits for a response from the NMS host after sending an inform message.

4) Click **Create**.

3.1.2 Enabling SNMP Traps

Choose the menu **MAINTENANCE > SNMP > Notification > Trap Config** to load the following page.

Figure 3-2 Enabling SNMP Traps



Follow these steps to enable some or all of the supported traps:

1) Select the traps to be enabled according to your needs. With a trap enabled, the switch will send the corresponding trap message to the NMS when the trap is triggered.

SNMP Authentication	Triggered when a received SNMP request fails the authentication.
Coldstart	Indicates that the SNMP entity is reinitializing itself such that its configurations may be changed. The trap can be triggered when you reboot the switch.
Warmstart	Indicates that the SNMP entity is reinitializing itself with its configurations unchanged. For a switch running SNMP, the trap can be triggered if you disable and then enable SNMP without changing any parameters.
Link Status	Enable or disable Link Status Trap globally. The trap includes the following two sub-traps: **Linkup Trap**: Indicates that a port status changes from linkdown to linkup. **Linkdown Trap**: Indicates that a port status changes from linkup to linkdown. Link Status Trap can be triggered when it is enabled both globally and on the port, and you connect a new device to the port or disconnect a device from the port. To enable the trap on a port, run the command **snmp-server traps link-status** in Interface Configuration Mode of the port. To disable it, run the corresponding no command. By default, the trap is enabled both globally and on all ports, which means that link status changes on any ports will trigger the trap. If you do not want to receive notification messages about some specific ports, disable the trap on those ports.

CPU Utilization	Triggered when the CPU utilization exceeds 80%.
Memory Utilization	Triggered when the memory utilization exceeds 80%.
Flash Operation	Triggered when flash is modified during operations such as backup, reset, firmware upgrade, and configuration import.
VLAN Create/Delete	Triggered when certain VLANs are created or deleted successfully.
IP Change	Monitors the changes of interfaces' IP addresses. The trap can be triggered when the IP address of any interface is changed.
Storm Control	Monitors whether the storm rate has reached the limit that you have set. The trap can be triggered when the Strom Control feature is enabled and broadcast/multicast/unknown-unicast frames are sent to the port with a rate higher than what you have set.
Rate Limit	Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set.
LLDP	The trap includes the following sub-traps: **LLDP RemTablesChange**: Indicates that the switch senses an LLDP topology change. The trap can be triggered when adding or removing a remote device, and when the information of some remote devices is aged out or cannot be stored into the switch because of insufficient resources. This trap can be used by an NMS to trigger LLDP remote systems table maintenance polls. **LLDP TopologyChange**: Indicates that the switch senses an LLDP-MED topology change (the topology change of media endpoints). The trap can be triggered when adding or removing a media endpoint that supports LLDP, such as an IP Phone. An LLDP Remtableschange trap will be also triggered every time LLDP Topologychange trap is triggered.
Loopback Detection	Triggered when the Loopback Detection feature is enabled and a loopback is detected or cleared.
Spanning Tree	Indicates spanning tree changes. The trap can be triggered in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a TCN (Topology Change Notification) BPDU or a Configuration BPDU with the TC (Topology Change) bit set.

PoE	The trap includes the following sub-traps: **Over-max-pwr-budget**: Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply. **Port-pwr-change**: Triggered when a port starts to supply power or stops supplying power. **Port-pwr-deny**: Triggered when the switch powers off PDs on low-priority PoE ports. The switch powers off them to ensure stable running of the other PDs when the total power required by the connected PDs exceeds the system power limit. **Port-pwr-over-30w**: Triggered when the power required by the connected PD exceeds 30 watts. **Port-pwr-overload**: Triggered when the power required by the connected PD exceeds the maximum power the port can supply. **Port-short-circuit**: Triggered when a short circuit is detected on a port. **Thermal-shutdown**: Triggered when the PSE chip overheats. The switch will stop supplying power in this case. *Note:* PoE trap is only available on certain devices.
IP-MAC Binding	Triggered in the following two situations: the ARP Inspection feature is enabled and the switch receives an illegal ARP packet; or the IPv4 Source Guard feature is enabled and the switch receives an illegal IP packet.
IP Duplicate	Triggered when the switch detects an IP conflict.
DHCP Filter	Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server.
DDM Temperature	Monitors the temperature of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the temperature of any SFP module has reached the warning or alarm threshold. *Note:* DDM Temperature is only available on certain devices.
DDM Voltage	Monitors the voltage of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the voltage of any SFP module has reached the warning or alarm threshold. *Note:* DDM Voltage is only available on certain devices.
DDM Bias Current	Monitors the bias current of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the bias current of any SFP module has reached the warning or alarm threshold. *Note:* DDM Bias Current is only available on certain devices.

DDM TX Power	Monitors the TX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the TX Power of any SFP module has reached the warning or alarm threshold. *Note:* DDM TX Power is only available on certain devices.
DDM RX Power	Monitors the RX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the RX Power of any SFP module has reached the warning or alarm threshold. *Note:* DDM RX Power is only available on certain devices.
ACL Counter	Monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the Logging feature in the ACL rule settings enabled, the switch will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.

2) Click **Apply**.

3.2 Using the CLI

3.2.1 Configuring the NMS Host

Configure parameters of the NMS host and packet handling mechanism.

Step 1	**configure** Enter Global Configuration Mode.

Step 2	**snmp-server host** *ip udp-port user-name* [**smode** { v1 | v2c | v3 }] [**slev** {noAuthNoPriv | authNoPriv | authPriv }] [**type** { trap | inform}] [**retries** *retries*] [**timeout** *timeout*] Configure parameters of the NMS host and packet handling mechanism. *ip:* Specify the IP address of the NMS host in IPv4 or IPv6. Make sure the NMS host and the switch can reach each other. *udp-port:* Specify a UDP port on the NMS host to receive notifications. The default is port 162. For communication security, we recommend that you change the port number under the condition that communications on other UDP ports are not affected. *user-name:* Enter the name used by the NMS host. When the NMS host uses SNMPv1 or SNMPv2c, enter the Community Name; when the NMS host uses SNMPv3, enter the User Name of the SNMP Group. v1 | v2c | v3: Choose the security model used by the user from the following: SNMPv1, SNMPv2c, SNMPv3. The NMS host should use the corresponding SNMP version. noAuthNoPriv | authNoPriv | authPriv: For SNMPv3 groups, choose a security level from noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption), authPriv (authorization and encryption). The default is noAuthNoPriv. Note that if you have chosen v1 or v2c as the security model, the security level cannot be configured. trap | inform: Choose a notification type for the NMS host. For SNMPv1, the supported type is Trap. For SNMPv2c and SNMPv3, you can configure the type as Trap or Inform. **Trap:** The switch will send Trap messages to the NMS host when certain events occur. When the NMS host receives a Trap message, it will not send a response to the switch. Thus the switch cannot tell whether a message is received or not, and the messages that are not received will not be resent. **Inform:** The switch will send Inform messages to the NMS host when certain events occur. When the NMS host receives an Inform message, it sends a response to the switch. If the switch does not receive any response within the timeout interval, it will resend the Inform message. Therefore, Inform is more reliable than Trap. *retries:* Set the retry times for Inform messages. The range is between 1 to 255 and the default is 3. The switch will resend the Inform message if it does not receive any response from the NMS host within the timeout interval. And it will stop sending Inform message when the retry times reaches the limit. *timeout:* Set the time that the switch waits for a response. Valid values are from 1 to 3600 seconds; the default is 100 seconds. The switch will resend the Inform message if it does not receive a response from the NMS host within the timeout interval.
Step 3	**show snmp-server host** Verify the information of the host.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure an NMS host with the parameters shown in Table 3-1.

Table 3-1 Parameters for the NMS Hosts

Parameter	Value
IP Address	172.16.1.222
UDP Port	162
User Name	admin
Security Model	v3
Security Level	authPriv
Notification Type	Inform
Retry Times	3
Timeout Interval	100 seconds

Switch#configure

Switch(config)#snmp-server host 172.16.1.222 162 admin **smode** v3 **slev** authPriv **type** inform **retries** 3 **timeout** 100

Switch(config)#show snmp-server host

No.	Des-IP	UDP	Name	SecMode	SecLev	Type	Retry	Timeout
---	------	-----	----	-------	------	----	-----	-------
1	172.16.1.222	162	admin	v3	authPriv	inform	3	100

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Enabling SNMP Traps

The switch supports many types of SNMP traps, like SNMP standard traps, ACL traps, and VLAN traps, and the corresponding commands are different. With a trap enabled, the switch will send the corresponding trap message to the NMS when the trap is triggered. Follow these steps to enable the traps according to your needs.

- Enabling the SNMP Standard Traps Globally

Step 1 **configure**

Enter Global Configuration Mode.

Step 2	**snmp-server traps snmp [** linkup | linkdown | warmstart | coldstart | auth-failure **]** Enable the corresponding SNMP standard traps. The command without any parameter enables all SNMP standard traps. By default, all SNMP standard traps are enabled. linkup | linkdown: Enable Linkup Trap and Linkdown Trap globally. Linkup Trap indicates that a port status changes from linkdown to linkup. The trap can be triggered when you connect a new device to the port, and the trap is enabled both globally and on the port. Linkdown Trap indicates that a port status changes from linkup to linkdown. The trap can be triggered when you disconnect a device from the port, and the trap is enabled both globally and on the port. To enable Linkup Trap and Linkdown Trap on a port, run the command **snmp-server traps link-status** in Interface Configuration Mode of the port. To disable them, run the corresponding no command. By default, the traps are enabled both globally and on all ports, which means that the traps will be triggered when a device is connected to or disconnected from any port of the switch. If you do not want to receive notification messages about some specific ports, disable the traps on those ports. warmstart: Indicates that the SNMP entity is reinitializing itself with its configurations unchanged. For a switch running SNMP, the trap can be triggered if you disable and then enable SNMP without changing any parameters. coldstart: Indicates that the SNMP entity is reinitializing itself such that its configurations may be changed. The trap can be triggered when you reboot the switch. auth-failure: Triggered when a received SNMP request fails the authentication.
Step 3	**end** Return to Privileged EXEC Mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to send linkup traps:

Switch#configure

Switch(config)#snmp-server traps snmp linkup

Switch(config)#end

Switch#copy running-config startup-config

■ Enabling the SNMP Extended Traps Globally

Step 1	**configure** Enter Global Configuration Mode.

Step 2	**snmp-server traps** { rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory } Enable the corresponding SNMP extended traps. By default, all SNMP extended traps are disabled. rate-limit: Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set. cpu: Monitors the load status of the switch CPU. The trap can be triggered when the utilization rate of the CPU exceeds 80%. flash: Triggered when flash is modified during operations such as backup, reset, firmware upgrade, and configuration import. lldp remtableschange: Indicates that the switch senses an LLDP topology change. The trap can be triggered when adding or removing a remote device, and when the information of some remote devices is aged out or cannot be stored into the switch because of insufficient resources. This trap can be used by an NMS to trigger LLDP remote systems table maintenance polls. lldp topologychange: Indicates that the switch senses an LLDP-MED topology change (the topology change of media endpoints). The trap can be triggered when adding or removing a media endpoint that supports LLDP, such as an IP Phone. An LLDP Remtableschange trap will be also triggered every time LLDP Topologychange trap is triggered. loopback-detection: Triggered when the Loopback Detection feature is enabled and a loopback is detected or cleared. storm-control: Monitors whether the storm rate has reached the limit that you have set. The trap can be triggered when the Strom Control feature is enabled and broadcast/multicast/unknown-unicast frames are sent to the port with a rate higher than what you have set. spanning-tree: Indicates spanning tree changes. The trap can be triggered in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a TCN (Topology Change Notification) BPDU or a Configuration BPDU with the TC (Topology Change) bit set. memory: Monitors the load status of the switch memory. The trap can be triggered when the memory utilization exceeds 80%.
Step 3	**end** Return to Privileged EXEC Mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable bandwidth-control traps:

Switch#configure

Switch(config)#snmp-server traps bandwidth-control

Switch(config)#end

Switch#copy running-config startup-config

Enabling the DDM Traps Globally

Note:

DDM Traps are only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**snmp-server traps ddm** [temperature | voltage | bias_current | tx_power | rx_power] Enable the corresponding DDM traps. DDM function is used to monitor the status of the SFP modules inserted into the SFP ports on the switch. The command without parameter enables all SNMP DDM traps. By default, all DDM traps are disabled. temperature: Monitors the temperature of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the temperature of any SFP module has reached the warning or alarm threshold. voltage: Monitors the voltage of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the voltage of any SFP module has reached the warning or alarm threshold. bias_current: Monitors the bias current of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the bias current of any SFP module has reached the warning or alarm threshold. tx_power: Monitors the TX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the TX Power of any SFP module has reached the warning or alarm threshold. rx_power: Monitors the RX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the RX Power of any SFP module has reached the warning or alarm threshold.
Step 3	**end** Return to Privileged EXEC Mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable DDM temperature trap:

Switch#configure

Switch(config)#snmp-server traps ddm temperature

Switch(config)#end

Switch#copy running-config startup-config

Enabling the VLAN Traps Globally

Step 1	**configure** Enter Global Configuration Mode.

Step 2	**snmp-server traps vlan** [create | delete] Enable the corresponding VLAN traps. The command without parameter enables all SNMP VLAN traps. By default, all VLAN traps are disabled. create: Triggered when certain VLANs are created successfully. delete: Triggered when certain VLANs are deleted successfully.
Step 3	**end** Return to Privileged EXEC Mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable all the SNMP VLAN traps:

Switch#configure

Switch(config)#snmp-server traps vlan

Switch(config)#end

Switch#copy running-config startup-config

■ Enabling the SNMP Security Traps Globally

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**snmp-server traps security** { dhcp-filter | ip-mac-binding } Enable the corresponding security traps. By default, all security traps are disabled. dhcp-filter: Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server. ip-mac-binding: Triggered when the ARP Inspection feature is enabled and the switch receives an illegal ARP packet, or the IPv4 Source Guard feature is enabled and the switch receives an illegal IP packet.
Step 3	**end** Return to Privileged EXEC Mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable DHCP filter trap:

Switch#configure

Switch(config)#snmp-server traps security dhcp-filter

Switch(config)#end

Switch#copy running-config startup-config

Enabling the ACL Trap Globally

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**snmp-server traps security acl** Enable the ACL trap. By default, it is disabled. The trap monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the Logging feature in the ACL rule settings enabled, the switch will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.
Step 3	**end** Return to Privileged EXEC Mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable ACL trap:

Switch#configure

Switch(config)#snmp-server traps acl

Switch(config)#end

Switch#copy running-config startup-config

Enabling the IP Traps Globally

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**snmp-server traps ip** { change | duplicate } Enable the IP traps. By default, all IP traps are disabled. change: Monitors the changes of interfaces' IP addresses. The trap can be triggered when the IP address of any interface is changed. duplicate: Triggered when the switch detects an IP conflict.
Step 3	**end** Return to Privileged EXEC Mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable IP-Change trap:

Switch#configure

Switch(config)#snmp-server traps ip change

Switch(config)#end

Switch#copy running-config startup-config

Enabling the SNMP PoE Traps Globally

Note:

PoE trap is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**snmp-server traps power** [over-max-pwr-budget | port-pwr-change | port-pwr-deny | port-pwr-over-30w | port-pwr-overload | port-short-circuit | thermal-shutdown] Enable the PoE traps. The command without any parameter enables all PoE traps. By default, all PoE traps are disabled. over-max-pwr-budget: Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply. port-pwr-change: Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply. port-pwr-deny: Triggered when the switch powers off PDs on low-priority PoE ports. The switch powers off them to ensure stable running of the other PDs when the total power required by the connected PDs exceeds the system power limit. port-pwr-over-30w: Triggered when the power required by the connected PD exceeds 30 watts. port-pwr-overload: Triggered when the power required by the connected PD exceeds the maximum power the port can supply. port-short-circuit: Triggered when a short circuit is detected on a port. thermal-shutdown: Triggered when the PSE chip overheats. The switch will stop supplying power in this case.
Step 3	**end** Return to Privileged EXEC Mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable all PoE traps:

Switch#configure

Switch(config)#snmp-server traps power

Switch(config)#end

Switch#copy running-config startup-config

Enabling the Link-status Trap for Ports

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Configure notification traps on the specified ports. *port/port-list:* The number or the list of the Ethernet ports that you desire to configure notification traps. To configure multiple ports, enter a list of port numbers separated by commas, or use a hyphen to indicates a range of port numbers. For example, 1-3, 5 indicates port 1, 2, 3, 5.
Step 3	**snmp-server traps link-status** Enable Link Status Trap for the port. By default, it is enabled. Link Status Trap (including Linkup Trap and Linkdown Trap) can be triggered when the link status of a port changes, and the trap is enabled both globally and on the port. To enable Linkup Trap and Linkdown Trap globally, run the command **snmp-server traps snmp [** linkup | linkdown **]** in Global Configuration Mode. To disable it, run the corresponding no command.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable link-status trap:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#snmp-server traps link-status

Switch(config-if)#end

Switch#copy running-config startup-config

4 RMON

RMON (Remote Network Monitoring) together with the SNMP system allows the network manager to monitor remote network devices efficiently. RMON reduces traffic flow between the NMS and managed devices, which is convenient to manage large networks.

RMON includes two parts: the NMS and the Agents running on every network device. The NMS is usually a host that runs the management software to manage Agents of network devices. The Agent is usually a switch or router that collects traffic statistics (such as the total number of packets on a network segment during a certain time period, or total number of correct packets that are sent to a host). Based on SNMP protocol, the NMS collects network data by communicating with Agents. However, the NMS cannot obtain every datum of RMON MIB because the device resources are limited. Generally, the NMS can only get information of the following four groups: Statistics, History, Event and Alarm.

- **Statistics:** Collects Ethernet statistics (like the total received bytes, the total number of broadcast packets, and the total number of packets with specified size) on an interface.
- **History:** Collects a history group of statistics on Ethernet ports for a specified polling interval.
- **Event:** Specifies the action to be taken when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.
- **Alarm:** Monitors a specific MIB object for a specified interval, and triggers an event at a specified value (rising threshold or falling threshold).

5 RMON Configurations

With RMON configurations, you can:

- Configuring the Statistics group.
- Configuring the History group.
- Configuring the Event group.
- Configuring the Alarm group.

Configuration Guidelines

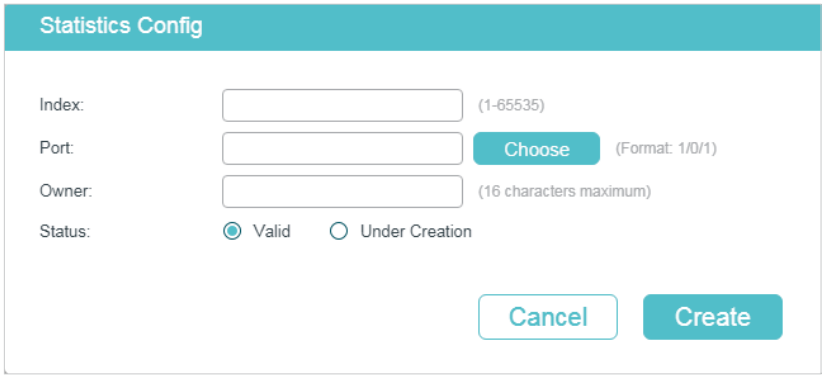
To ensure that the NMS receives notifications normally, complete configurations of SNMP and SNMP Notification before configuring RMON.

5.1 Using the GUI

5.1.1 Configuring the Statistics Group

Choose the menu **MAINTENANCE > SNMP > RMON > Statistics** and click Add to load the following page.

Figure 5-1 Creating a Statistics Entry



Follow these steps to configure the Statistics group:

1) Specify the entry index, the port to be monitored, and the owner name of the entry. Set the entry as Valid or Under Creation.

Index	Enter the index of the entry.
Port	Specify an Ethernet port to be monitored in the entry. You can click **Choose** to choose a port from the list or manually enter the port number, for example, 1/0/1 in the input box.
Owner	Enter the owner name of the entry with1 to 16 characters.

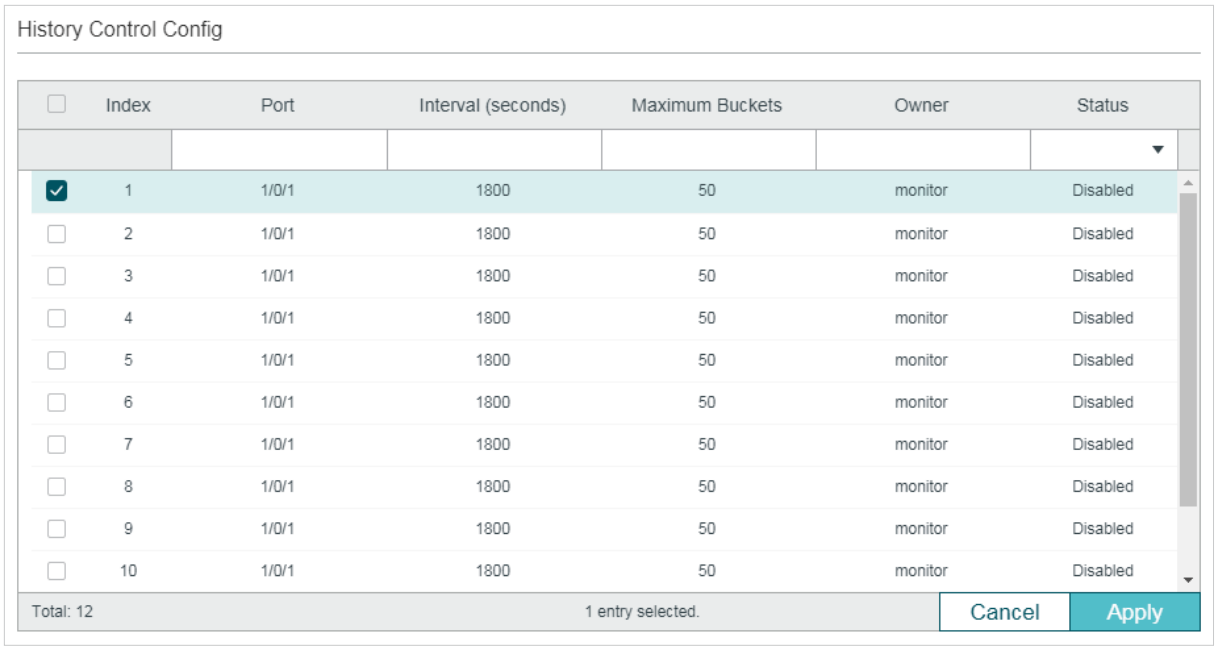
Status	Set the entry as Valid or Under Creation. By default, it is Valid. The switch start to collect Ethernet statistics for a Statistics entry since the entry status is configured as valid. **Valid**: The entry is created and valid. **Under Creation**: The entry is created but invalid.

2) Click **Create**.

5.1.2 Configuring History Group

Choose the menu **MAINTENANCE > SNMP > RMON > History** to load the following page.

Figure 5-2 Configuring the History Entry



Follow these steps to configure the History group:

1) Select a History entry, and specify a port to be monitored.

Index	Displays the index of History entries. The switch supports up to 12 History entries.
Port	Specify a port to be monitored.

2) Set the sample interval and the maximum buckets of History entries.

Interval (seconds)	Specify the number of seconds in each polling cycle. Valid values are from 10 to 3600 seconds. Every history entry has its own timer. For the monitored port, the switch samples packet information and generates a record in every interval.
Maximum Buckets	Set the maximum number of records for the History entry. Valid values are from 10 to 130. When the number of records exceeds the limit, the earliest record will be overwritten.

3) Enter the owner name, and set the status of the entry. Click **Apply**.

Owner	Enter the owner name of the entry with 1 to 16 characters. By default, it is monitor.
Status	Enable or disable the entry. By default, it is disabled. **Enable**: The entry is enabled. **Disable**: The entry is disabled.

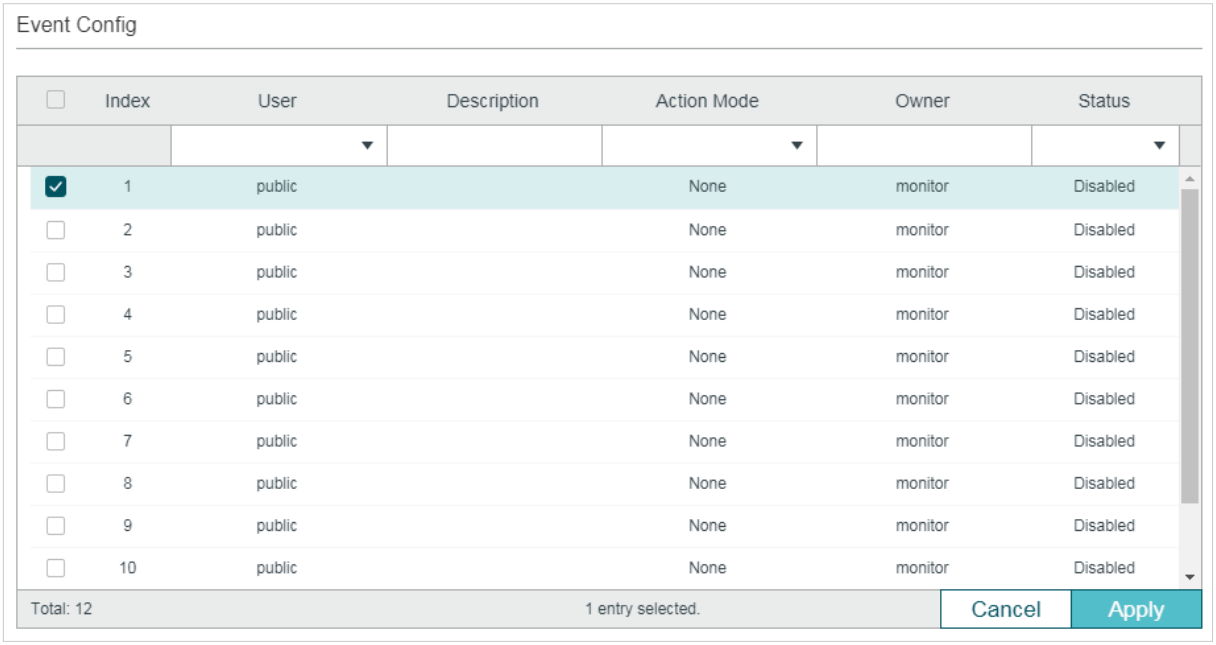
Note:

To change the parameters of a History entry, enable the entry at the same time; otherwise, the change cannot take effect.

5.1.3 Configuring Event Group

Choose the menu **MAINTENANCE > SNMP > RMON > Event** to load the following page.

Figure 5-3 Configuring the Event Entry



Follow these steps to configure the Event group:

1) Choose an Event entry, and specify an SNMP User for the entry.

Index	Displays the index of Event entries. The switch supports up to 12 Event entries.
User	Choose an SNMP user name or community name for the entry. Only the specified user can access the log messages or receive the notification messages related to the event.

2) Set the description and action to be taken when the event is triggered.

Description	Enter an brief description of this event to make it easier to be identified.

Action Mode	Specify the action for the switch to take when the event is triggered. **None**: No action. **Log**: The switch records the event in the log, and the NMS should initiate requests to get notifications. **Notify**: The switch sends notifications to the NMS. **Log & Notify**: The switch records the event in the log and sends notifications to the NMS.

3) Enter the owner name, and set the status of the entry. Click **Apply**.

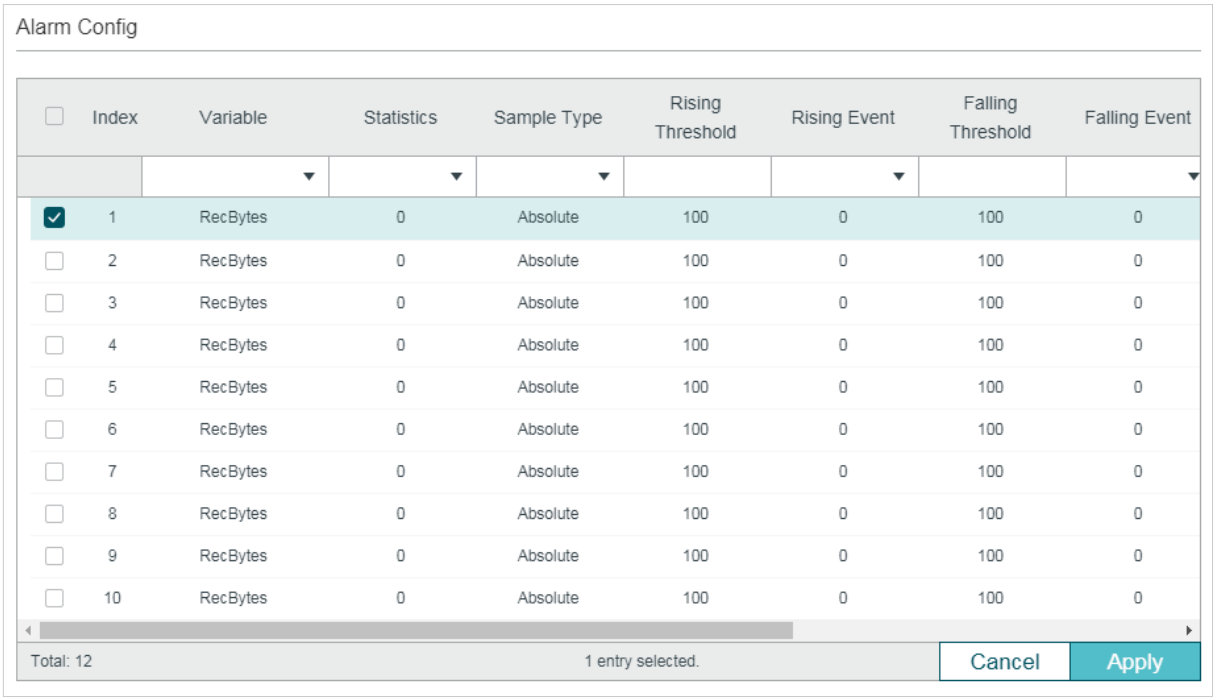
Owner	Enter the owner name of the entry with 1 to 16 characters.
Status	Enable or disable the entry. **Enable**: The entry is enabled. **Disable**: The entry is disabled.

5.1.4 Configuring Alarm Group

Before you begin, complete configurations of Statistics entries and Event entries, because the Alarm entries must be associated with Statistics and Event entries.

Choose the menu **MAINTENANCE > SNMP > RMON > Alarm** to load the following page.

Figure 5-4 Configuring the Alarm Entry



Follow these steps to configure the Alarm group:

1) Select an alarm entry, choose a variable to be monitored, and associate the entry with a statistics entry.

Index	Displays the index of Alarm entries. The switch supports up to 12 Alarm entries.
Variable	Set the alarm variable to be monitored. The switch will monitor the specified variable in sample intervals and act in the set way when the alarm is triggered. **RecBytes**: Total number of received bytes. **RecPackets**: Total number of received packets. **BPackets**: Total number of broadcast packets. **MPackets**: Total number of multicast packets. **CRC&Align ERR**: Packets that contain FCS Error or Alignment Error, within a size of 64 to 1518 bytes. **Undersize**: Packets that are smaller than 64 bytes. **Oversize**: Packets that are larger than 1518 bytes. **Jabbers**: Packets that are sent when port collisions occur. **Collisions**: Collision times in the network segment. **64, 65-127, 128-255, 256-511, 512-1023, 1024-1518**: Total number of packets of the specified size.
Statistics	Associate the Alarm entry with a Statistics entry. Then the switch monitors the specified variable of the Statistics entry.

2) Set the sample type, the rising and falling threshold, the corresponding event entries, and the alarm type of the entry.

Sample Type	Specify the sampling method of the specified variable. **Absolute**: Compare the sampling value against the preset threshold. **Delta**: The switch obtains the difference between the sampling values of the current interval and the previous interval, and then compares the difference against the preset threshold.
Rising Threshold	Specify the rising threshold of the variable. Valid values are from 1 to 2147483647. When the sampling value or the difference value exceeds the threshold, the system will trigger the corresponding Rising Event. *Note:* The rising threshold should be larger than the falling threshold.
Rising Event	Specify the index of the Event entry that will be triggered when the sampling value or the difference value exceeds the preset threshold. The Event entry specified here should be enabled first.

Falling Threshold	Set the falling threshold of the variable. Valid values are from 1 to 2147483647. When the sampling value or the difference value is below the threshold, the system will trigger the corresponding Falling Event. *Note:* The falling threshold should be less than the rising threshold.
Falling Event	Specify the index of the Event entry that will be triggered when the sampling value or the difference value is below the preset threshold. The Event entry specified here should be enabled first.
Alarm Type	Specify the alarm type for the entry. **Rising**: The alarm is triggered only when the sampling value or the difference value exceeds the rising threshold. **Falling**: The alarm is triggered only when the sampling value or the difference value is below the falling threshold. **All**: The alarm is triggered when the sampling value or the difference value exceeds the rising threshold or is below the falling threshold.

3) Enter the owner name, and set the status of the entry. Click **Apply**.

Interval (seconds)	Set the sampling interval. Valid values are from 10 to 3600 seconds.
Owner	Enter the owner name of the entry with 1 to 16 characters.
Status	Enable or disable the entry. **Enable**: The entry is enabled. **Disable**: The entry is disabled.

5.2 Using the CLI

5.2.1 Configuring Statistics

Step 1	**configure** Enter Global Configuration Mode.

Step 2	**rmon statistics** *index* **interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } [**owner** *owner-name*] [**status** { underCreation | valid }] Configure RMON Statistic entries. *index:* Specify the index of the Statistics entry, which ranges from 1 to 65535. To configure multiple indexes, enter a list of indexes separated by commas, or use a hyphen to indicates a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5. *port:* Specify the port to be bound to the entry. *owner-name:* Enter the owner name of the entry with 1 to 16 characters. The default name is monitor. underCreation | valid: Enter the status of the entry. UnderCreation indicates that the entry is created but invalid, while Valid indicates the entry is created and valid. By default, it is valid. The switch start to collect Ethernet statistics for a Statistics entry since the entry status is configured as valid.
Step 3	**show rmon statistics** [*index*] Displays the statistics entries and their configurations. *index:* Enter the index of statistics entry that you want to view. Valid values are from 1 to 65535. The command without any parameters displays all existing statistics entries.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create Statistics entries 1 and 2 on the switch to monitor port 1/0/1 and 1/0/2, respectively. The owner of the entries are both monitor and the status are both valid:

Switch#configure

Switch(config)#rmon statistics 1 **interface gigabitEthernet** 1/0/1 **owner** monitor **status** valid

Switch(config)#rmon statistics 2 **interface gigabitEthernet** 1/0/2 **owner** monitor **status** valid

Switch(config)#show rmon statistics

Index	Port	Owner	State
-----	----	-----	-----
1	Gi1/0/1	monitor	valid
2	Gi1/0/2	monitor	valid

Switch(config)#end

Switch#copy running-config startup-config

5.2.2 Configuring History

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**rmon history** *index* **interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*} [**interval** *seconds*] [**owner** *owner-name*] [**buckets** *number*] Configuring RMON History entries. *index:* Specify the index of the History entry, which ranges from 1 to 12. To configure multiple indexes, enter a list of indexes separated by commas, or use a hyphen to indicates a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5. *port:* Specify the port to be bound to the entry. *seconds:* Set the sample interval. The values are from 10 to 3600 seconds, and the default is 1800 seconds. *owner-name:* Enter the owner name of the entry with 1 to 16 characters. The default name is monitor. *number:* Set the maximum number of records for the history entry. When the number of records exceeds the limit, the earliest record will be overwritten. The values are from 10 to 130; the default is 50.
Step 3	**show rmon history** [*index*] Displays the specified History entry and related configurations. To show multiple entries, enter a list of indexes separated by commas, or use a hyphen to indicates a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5. *index:* Enter the index of History entry that you want to view. Valid values are from 1 to 12. The command without any parameters displays all existing statistics entries.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a History entry on the switch to monitor port 1/0/1. Set the sample interval as 100 seconds, maximum buckets as 50, and the owner as monitor:

Switch#configure

Switch(config)#rmon history 1 **interface gigabitEthernet** 1/0/1 **interval** 100 **owner** monitor **buckets** 50

Switch(config)#show rmon history

Index	Port	Interval	Buckets	Owner	State
1	Gi1/0/1	100	50	monitor	Enable

Switch(config)#end

Switch#copy running-config startup-config

5.2.3 Configuring Event

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**rmon event** *index* [**user** *user-name*] [**description** *description*] [**type** { none | log | notify | log-notify }] [**owner** *owner-name*] Configuring RMON Event entries. *index:* Specify the index of the Event entry, which ranges from 1 to 12. To configure multiple indexes, enter a list of indexes separated by commas, or use a hyphen to indicates a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5. *user-name:* Enter the SNMP user name or community name of the entry. The name should be what you have set in SNMP previously. The default name is public. *description:* Give a description to the entry with 1 to 16 characters. By default, the description is empty. none | log | notify | log-notify*:* Specify the action type of the event; then the switch will take the specified action to deal with the event. By default, the type is none. None indicates the switch takes no action, log indicates the switch records the event only, notify indicates the switch sends notifications to the NMS only, and log-notify indicates the switch records the event and sends notifications to the NMS. *owner-name:* Enter the owner name of the entry with 1 to 16 characters. The default name is monitor.
Step 3	**show rmon event** [*index*] Displays the specified Event entry and related configurations. To show multiple entries, enter a list of indexes separated by commas, or use a hyphen to indicates a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5. *index:* Enter the index of Event entry that you want to view. Valid values are from 1 to 12. The command without any parameters displays all existing statistics entries.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an Event entry on the switch. Set the user name as admin, the event type as Notify (set the switch to initiate notifications to the NMS), and the owner as monitor:

Switch#configure

Switch(config)#rmon event 1 **user** admin **description** rising-notify **type** notify **owner** monitor

Switch(config)#show rmon event

Index	User	Description	Type	Owner	State
1	admin	rising-notify	Notify	monitor	Enable

Switch(config)#end

Switch#copy running-config startup-config

5.2.4 Configuring Alarm

Step 1	**configure** Enter Global Configuration Mode.
Step 2	**rmon alarm** *index* **stats-index** *sindex* [**alarm-variable** { revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | jabber | collision | 64 | 65-127 | 128-255 | 256-511 | 512-1023 | 1024-1518}] [**s-type** {absolute | delta}] [**rising-threshold** *r-threshold*] [**rising-event-index** *r-event*] [**falling-threshold** *f-threshold*] [**falling-event-index** *f-event*] [**a-type** {rise | fall | all}] [**owner** *owner-name*] [**interval** *interval*] Configuring RMON alarm entries. *index:* Specify the index of the Alarm entry, which ranges from 1 to 12. To configure multiple indexes, enter a list of indexes separated by commas, or use a hyphen to indicates a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5. *sindex:* Specify the index of the related Statistics entry, which ranges from 1 to 65535. *revbyte / revpkt / bpkt / mpkt / crc-align / undersize / oversize / jabber / collision / 64 / 65-127 / 128-255 / 256-511 / 512-1023 / 1024-1518:* Choose an alarm variable to monitor. The switch will monitor the specified variable in sample intervals and act in the set way when the alarm is triggered. The default variable is revbyte. revbyte means total number of received bytes; revpkt means total number of received packets; bpkt means total number of broadcast packets. mpkt means total number of multicast packets; crc-align means packets that contain FCS Error or Alignment Error, within a size of 64 to 1518 bytes; undersize means packets that are smaller than 64 bytes; oversize means packets that are larger than 1518 bytes; jabber means packets that are sent when port collisions occur; collision means the collision times in the network segment; 64 | 65-127 | 128-255 | 256-511 | 512-1023 | 1024-1518 means total number of packets of the specified size.

absolute | delta: Choose the sampling method of the specified variable. The default is absolute. In the absolute mode, the switch compares the sampling value against the preset threshold; in the delta mode, the switch obtains the difference between the sampling values of the current interval and the previous interval, and then compares the difference against the preset threshold.

r-threshold: Enter the rising threshold. Valid values are from 1 to 2147483647, and the default is 100. The rising threshold should be larger than the falling threshold.

r-event: Enter the index of the Event entry that will be triggered when the sampling value or the difference value exceeds the preset threshold. Valid values are from 1 to 12. The Event entry specified here should be enabled first.

f-threshold: Enter a falling threshold. Valid values are from 1 to 2147483647, and the default is 100. The falling threshold should be less than the rising threshold.

f-event: Enter the index of the Event entry that will be triggered when the sampling value or the difference value is below the preset threshold. Valid values are from 1 to 12. The Event entry specified here should be enabled first.

rise | fall | all: Choose an alarm type; the default is all. Rise indicates that the alarm is triggered only when the sampling value or difference value exceeds the rising threshold. Fall indicates that the alarm is triggered only when the sampling value or difference value is below the falling threshold. All indicates that the alarm is triggered when the sampling value or difference value either exceeds the rising threshold or is below the falling threshold.

owner-name: Enter the owner name of the entry using 1 to 16 characters. The default name is monitor.

interval: Set the sampling interval. The value ranges from 10 to 3600 seconds; the default is 1800 seconds.

Step 3	**show rmon alarm** [*index*] Displays the specified alarm entry and related configurations. To show multiple entries, enter a list of indexes separated by commas, or use a hyphen to indicates a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5. *index:* Enter the index of Alarm entry that you want to view. Valid values are from 1 to 12. The command without any parameters displays all existing statistics entries.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set an alarm entry to monitor BPackets on the switch. Set the related Statistics entry index as 1, the sample type as Absolute, the rising threshold as 3000, the related rising event entry index as 1, the falling threshold as 2000, the related falling event index as 2, the alarm type as all, the notification interval as 10 seconds, and the owner of the entry as monitor:

Switch#configure

Switch(config)#rmon alarm 1 **stats-index** 1 **alarm-variable** bpkt **s-type** absolute **rising-threshold** 3000 **rising-event-index** 1 **falling-threshold** 2000 **falling-event-index** 2 **a-type** all **interval** 10 **owner** monitor

Switch(config)#show rmon alarm

Index-State: 1-Enabled

Statistics index: 1

Alarm variable: BPkt

Sample Type: Absolute

RHold-REvent: 3000-1

FHold-FEvent: 2000-2

Alarm startup: All

Interval: 10

Owner: monitor

Switch(config)#end

Switch#copy running-config startup-config

6 Configuration Example

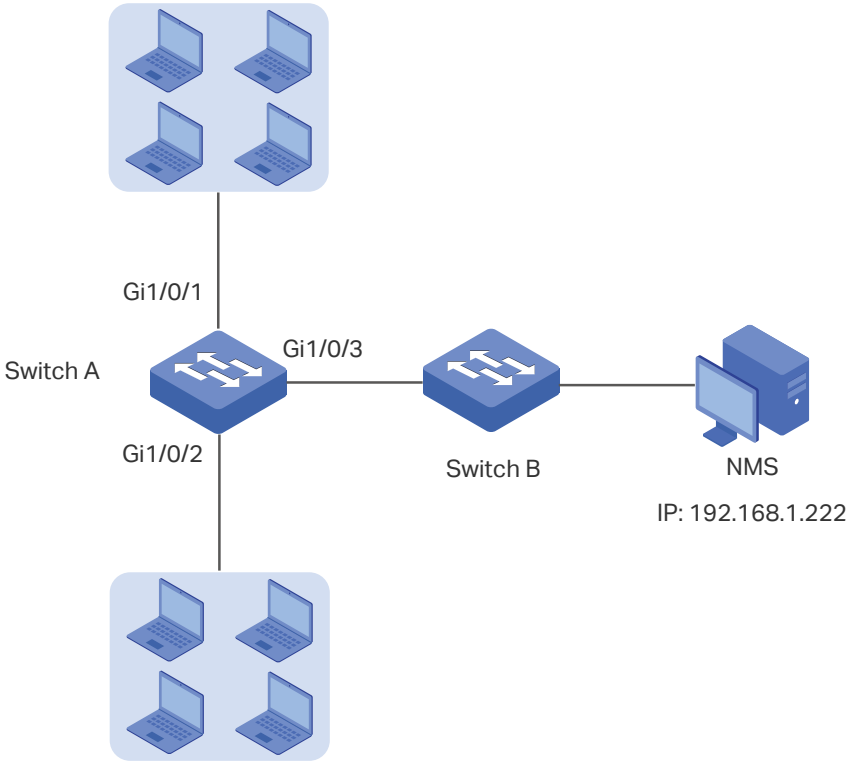
6.1 Network Requirements

The following figure shows the network topology of a company. The company has requirements as follows:

1) Monitor storm traffic of ports 1/0/1 and 1/0/2 on Switch A, and send notifications to the NMS when the actual rate of broadcast, multicast or unknown-unicast packets exceeds the preset threshold.
2) Monitor the traffic of ports 1/0/1 and 1/0/2 on Switch A, and regularly collect and save data for follow-up checks. Specifically, Switch A should notify the NMS when the number of packets transmitted and received on the ports during the sample interval exceeds the preset rising threshold, and should record but not notify the NMS when that is below the preset falling threshold.

The NMS host with IP address 192.168.1.222 is connected to the core switch, Switch B. Switch A is connected to Switch B via port 1/0/3. Port 1/0/3 and the NMS can reach one another.

Figure 6-1 Network Topology



6.2 Configuration Scheme

1) On Switch A, set thresholds for broadcast, multicast and unknown-unicast packets on ports 1/0/1 and 1/0/2. Enable SNMP and configure the corresponding parameters. Enable Trap notifications on the ports. Switch A can then send notifications to the NMS when the rate of storm traffic exceeds the preset threshold.
2) After SNMP and Notification configurations, create Statistic entries on the ports to monitor the real-time transmitting and receiving of packets and create History entries to regularly collect and save related data. Create two Event entries: one is the Notify type used to notify the NMS, and the other is the Log type used to record related events.
3) Create an Alarm entry to monitor RecPackets (Received Packets). Configure the rising and falling thresholds. Configure the rising event as the Notify event entry, and the falling event as the Log event entry.

Demonstrated with T1600G-52TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

6.3 Using the GUI

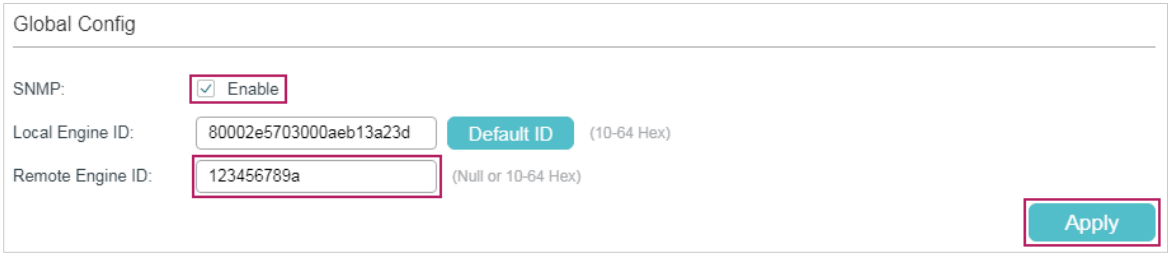
- Configuring Storm Control on Ports

  Configure Storm Control on the required ports. For detailed configuration, refer to Configuring QoS.

- Configuring SNMP

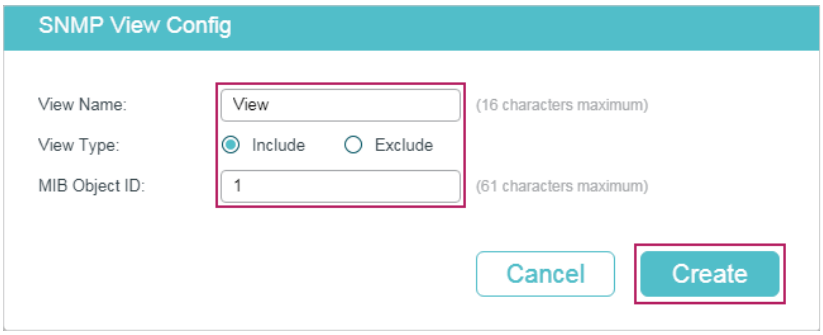
1) Choose **MAINTENANCE > SNMP > Global Config** to load the following page. In the **Global Config** section, enable SNMP, and set the Remote Engine ID as 123456789a. Click **Apply**.

Figure 6-2 Enabling SNMP



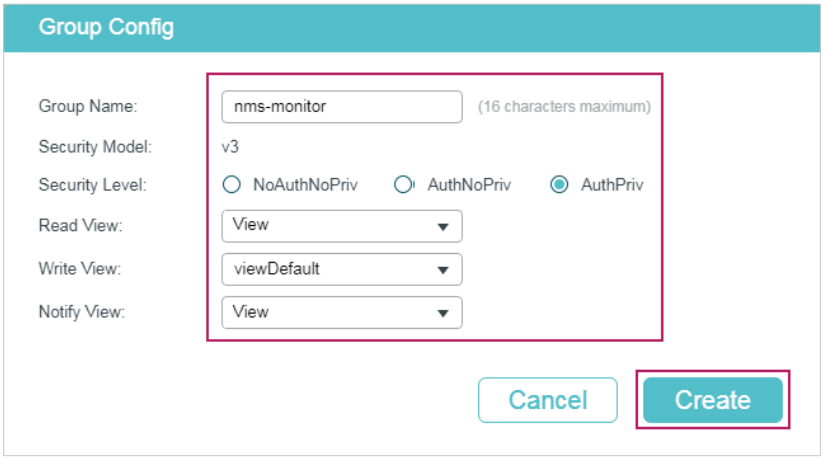
2) In the **SNMP View Config** section, click Add to load the following page. Name the SNMP view as View, set the view type as Include, and set MIB Object ID as 1 (which means all functions). Click **Create**.

Figure 6-3 Creating an SNMP View



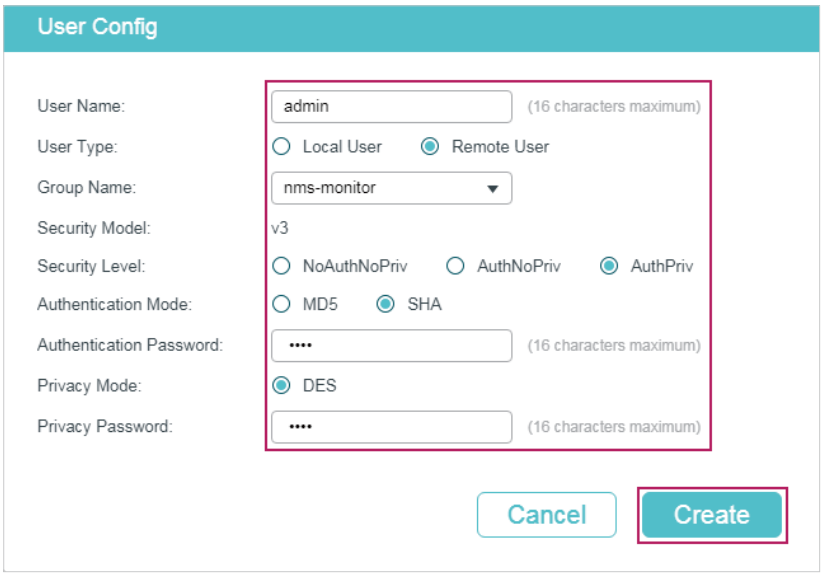
3) Choose **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** and click Add to load the following page. Create a group named nms-monitor, enable authentication and privacy, and add View to Read View and Notify View. Click **Create**.

Figure 6-4 Configuring an SNMP Group



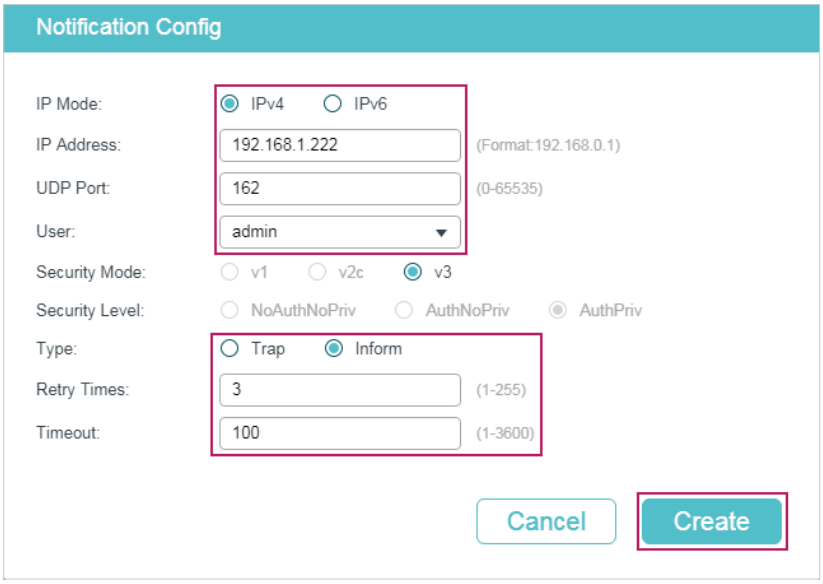
4) Choose **MAINTENANCE > SNMP > SNMP v3 > SNMP User** and click Add to load the following page. Create a user named admin for the NMS, set the user type as Remote User and specify the group name. Set the Security Level in accordance with that of the group nms-monitor. Choose SHA authentication algorithm and DES privacy algorithm, and set corresponding passwords. Click **Create**.

Figure 6-5 Creating an SNMP User



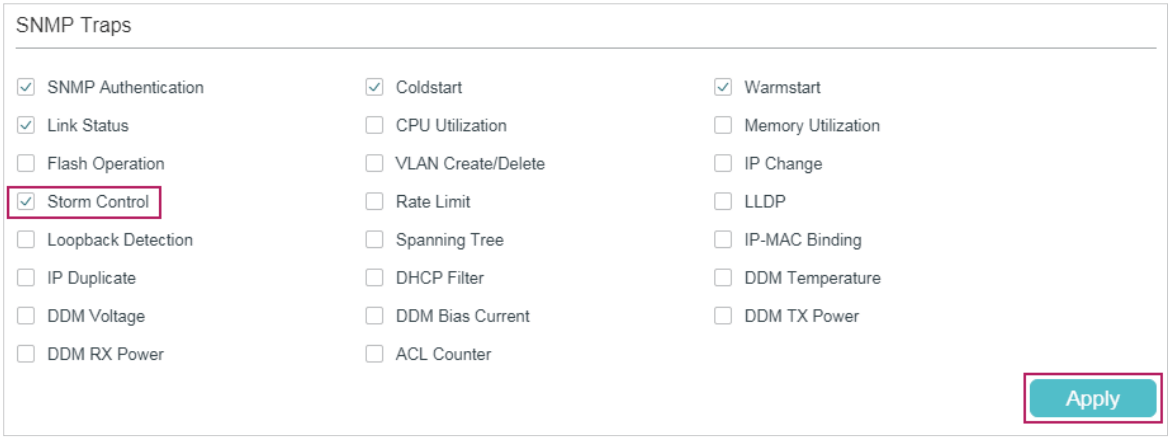
5) Choose **MAINTENANCE > SNMP > Notification > Notification Config** and click Add to load the following page. Choose the IP Mode as IPv4, and specify the IP address of the NMS host and the port of the host for transmitting notifications. Specify the User as admin and choose the type as Inform. Set the retry times as 3, with the timeout period as 100 seconds. Click **Create**.

Figure 6-6 Creating an SNMP Notification Entry



6) Choose **MAINTENANCE > SNMP > Notification > Trap Config** to load the following page. Enable Storm Control trap and click **Apply**.

Figure 6-7 Enabling Storm Control Trap



7) Click Save to save the settings.

Configuring RMON

1) Choose **MAINTENANCE > SNMP > RMON > Statistics** and click Add to load the following page. Create Statistics entries 1 and 2, and bind them to ports 1/0/1 and 1/0/2, respectively. Set the owner of the entries as monitor and the status as Valid.

Figure 6-8 Configuring Statistics Entry 1

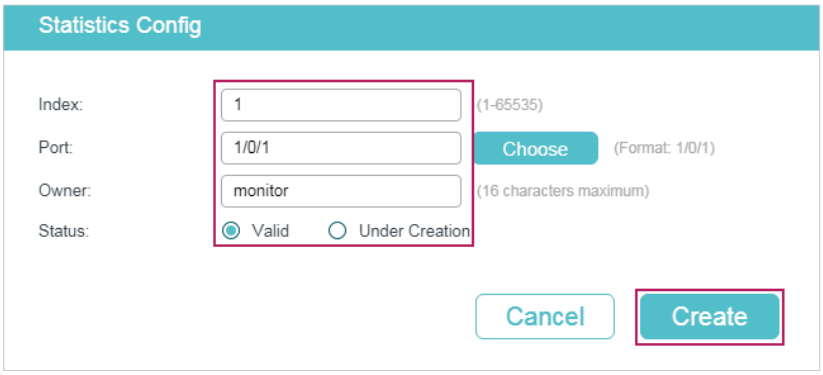
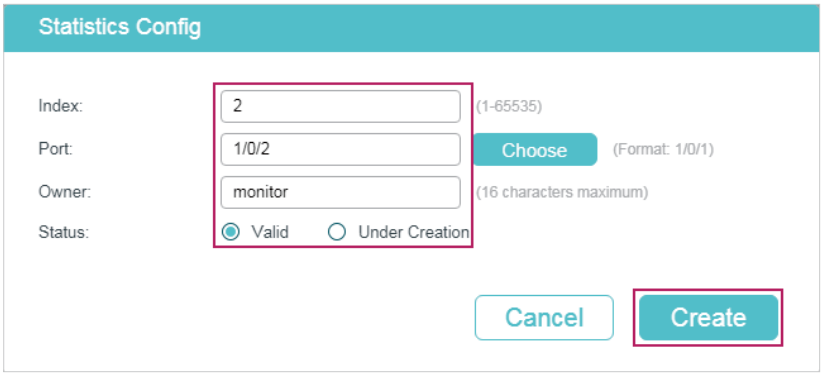
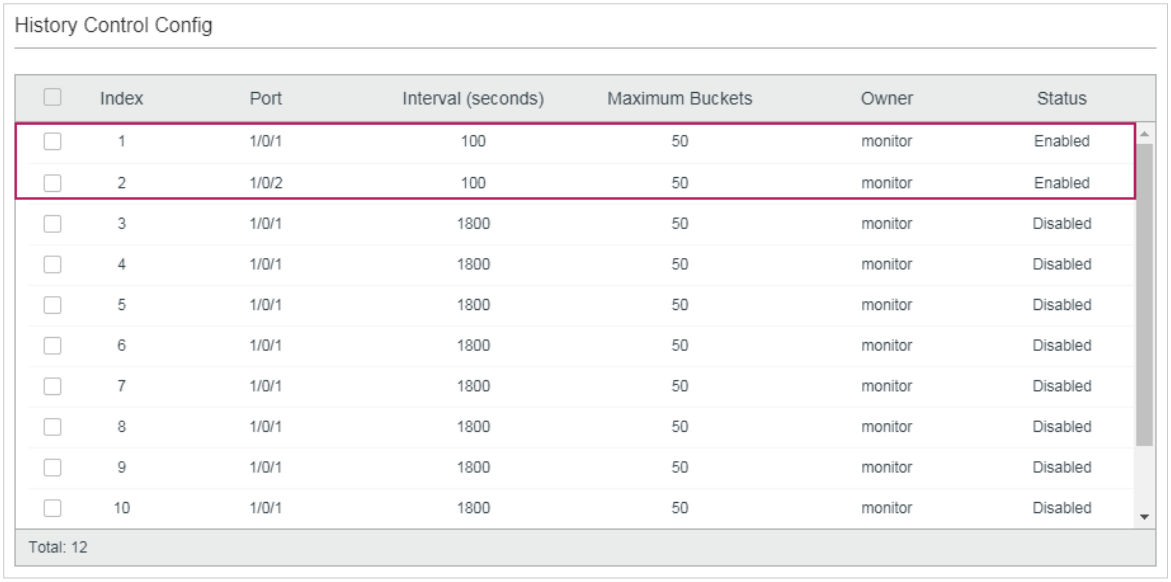


Figure 6-9 Configuring Statistics Entry 2



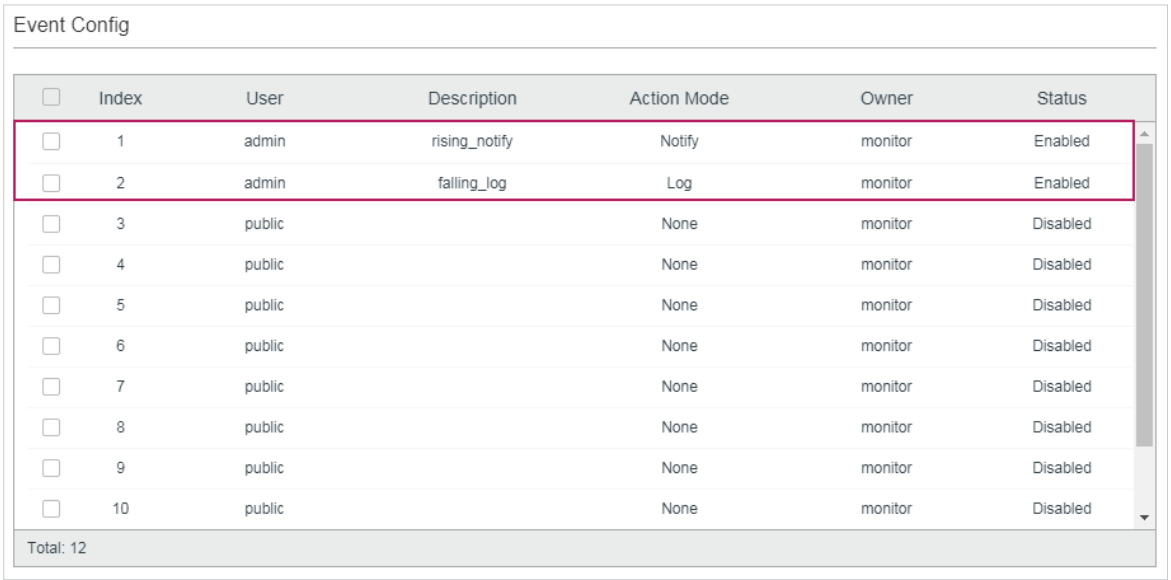
2) Choose the menu **MAINTENANCE > SNMP > RMON > History** to load the following page. Configure entries 1 and 2. Bind entries 1 and 2 to ports 1/0/1 and 1/0/2, respectively. Set the Interval as 100 seconds, Maximum Buckets as 50, the owner of the entries as monitor, and the status as enabled.

Figure 6-10 Configuring the History Entries



3) Choose the menu **MAINTENANCE > SNMP > RMON > Event** to load the following page. Configure entries 1 and 2. For entry 1, set the SNMP user name as admin, type as Notify, description as "rising_notify", owner as monitor, and status as enable. For entry 2, set the SNMP user name as admin, type as Log, description as "falling_log", owner as monitor, and status as enabled.

Figure 6-11 Configuring the Event Entries



4) Choose **MAINTENANCE > SNMP > RMON > Alarm** to load the following page. Configure entries 1 and 2. For entry 1, set the alarm variable as RecPackets, related statistics entry ID as 1 (bound to port 1/0/1), the sample type as Absolute, the rising threshold as 3000, associated rising event entry ID as 1 (which is the notify type), the falling threshold as 2000, the associated falling event entry ID as 2 (which is the log type), the alarm type as All, the interval as 10 seconds, the owner name as monitor. For entry 2, set the associated statistics entry ID as 2 (bound to port 1/0/2). Other configurations are the same as those of entry 1.

Figure 6-12 Configuring the Alarm Entries

5) Click Save to save settings.

6.4 Using the CLI

Configuring Storm Control on ports

Configure the Storm Control on the required ports of Switch A. For detailed configuration, refer to Configuring QoS.

Configuring SNMP

1) Enable SNMP and specify the remote engine ID.

   Switch_A#configure

   Switch_A(config)#snmp-server

   Switch_A(config)#snmp-server engineID remote 123456789a

2) Create a view with the name View; set the MIB Object ID as 1 (which represents all functions), and the view type as Include.

   Switch_A(config)#snmp-server view View 1 include

3) Create a group of SNMPv3 with the name of nms-monitor. Enable Auth Mode and Privacy Mode, and set both the Read and Notify views as View.

   Switch_A(config)#snmp-server group nms-monitor smode v3 slev authPriv read View notify View

4) Create an SNMP user named admin. Set the user as a remote user and configure the security model and security level based on the group. Set the Auth Mode as SHA algorithm, password as 1234, the Privacy Mode as DES, and password as 1234.

   Switch_A(config)#snmp-server user admin remote nms-monitor smode v3 slev authPriv cmode SHA cpwd 1234 emode DES epwd 1234

5) To configure Notification, specify the IP address of the NMS host and UDP port. Set the User, Security Model and Security Level according to configurations of the SNMP User.

Choose the type as Inform, and set the retry times as 3, and the timeout period as 100 seconds.

Switch_A(config)#snmp-server host 192.168.1.222 162 admin smode v3 slev authPriv type inform retries 3 timeout 100

- Enable storm-control Trap

Switch_A(config)#snmp-server traps storm-control

- Configuring RMON

1) Create Statistics entries 1 and 2 to monitor ports 1/0/1 and 1/0/2, respectively. The owner of the entries is set as monitor, and the status is set as valid.

Switch_A(config)#rmon statistics 1 interface gigabitEthernet 1/0/1 owner monitor status valid

Switch_A(config)#rmon statistics 2 interface gigabitEthernet 1/0/2 owner monitor status valid

2) Create History entries 1 and 2 and bind them to ports 1/0/1 and 1/0/2, respectively. Set the sample interval as 100 seconds, max buckets as 50, and the owner as monitor.

Switch_A(config)#rmon history 1 interface gigabitEthernet 1/0/1 interval 100 owner monitor buckets 50

Switch_A(config)#rmon history 2 interface gigabitEthernet 1/0/2 interval 100 owner monitor buckets 50

3) Create Event entries 1 and 2 for the SNMP user admin. Set entry 1 as the Notify type and its description as "rising_notify". Set entry 2 as the Log type and its description as "falling_log". Set the owner of them as monitor.

Switch_A(config)#rmon event 1 user admin description rising_notify type notify owner monitor

Switch_A(config)#rmon event 2 user admin description falling_log type log owner monitor

4) Create Alarm entries 1 and 2. For entry 1, set the alarm variable as RecPackets, associated Statistics entry ID as 1 (bound to port 1/0/1), the sample type as Absolute, the rising threshold as 3000, the associated rising event entry ID as 1 (Notify type), the falling threshold as 2000, the associated falling event entry ID as 2 (the log type), the alarm type as all, the interval as 10 seconds, and the owner name as monitor. For entry 2, set the associated statistics entry ID as 2 (bound to port 1/0/2), while all other configurations are the same as those of entry 1.

Switch_A(config)#rmon alarm 1 stats-index 1 alarm-variable revpkt s-type absolute rising-threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2 a-type all interval 10 owner monitor

Switch_A(config)#rmon alarm 2 stats-index 2 alarm-variable revpkt s-type absolute rising-threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2 a-type all interval 10 owner monitor

Verify the Configurations

Verify global SNMP configurations:

Switch_A(config)#show snmp-server

SNMP agent is enabled.

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 SNMP packets output

0 Too big errors(Maximum packet size 1500)

0 No such name errors

0 Bad value errors

0 General errors

0 Response PDUs

0 Trap PDUs

Verify SNMP engine ID:

Switch_A(config)#show snmp-server engineID

Local engine ID: 80002e5703000aeb13a23d

Remote engine ID: 123456789a

Verify SNMP view configurations:

```
Switch_A(config)#show snmp-server view
No.  View Name    Type      MOID
---  ------------  -------   ------------------
1    viewDefault   include   1
2    viewDefault   exclude   1.3.6.1.6.3.15
3    viewDefault   exclude   1.3.6.1.6.3.16
4    viewDefault   exclude   1.3.6.1.6.3.18
5    View          include   1
```

Verify SNMP group configurations:

```
Switch_A(config)#show snmp-server group
No.  Name          Sec-Mode   Sec-Lev    Read-View     Write-View   Notify-View
---  ------------  ---------- ---------- ------------- ------------ ----------
1    nms-monitor   v3         authPriv   View                       View
```

Verify SNMP user configurations:

```
Switch_A(config)#show snmp-server user
No.  U-Name     U-Type   G-Name        S-Mode   S-Lev      A-Mode   P-Mode
---  ---------- ------   ------        ------   -----      ------   ------
1    admin      remote   nms-monitor   v3       authPriv   SHA      DES
```

Verify SNMP host configurations:

```
Switch_A(config)#show snmp-server host
No.  Des-IP          UDP   Name    SecMode   SecLev     Type    Retry  Timeout
---  --------------- ----- ------- --------- ---------- ------- -----  --------
1    172.168.1.222   162   admin   v3        authPriv   inform  3      100
```

Verify RMON statistics configurations:

```
Switch_A(config)#show rmon statistics
```

```
Index  Port        Owner      State
-----  ----------  ---------  -------
1      Gi1/0/1     monitor    valid
2      Gi1/0/2     monitor    valid
```

Verify RMON history configurations:

```
Switch_A(config)#show rmon history
Index  Port        Interval  Buckets   Owner      State
-----  ---------   --------  ---------  ----------  ---------
1      Gi1/0/1     100       50         monitor    Enable
2      Gi1/0/2     100       50         monitor    Enable
```

Verify RMON event configurations:

```
Switch_A(config)#show rmon event
Index  User       Description       Type       Owner       State
-----  ------     -----------       --------   ----------  ----------
1      admin      rising_notify     Notify     monitor     Enable
2      admin      falling_log       Log        monitor     Enable
```

Verify RMON alarm configurations:

```
Switch_A(config)#show rmon alarm
  Index-State:        1-Enabled
  Statistics index:   1
  Alarm variable:     RevPkt
  Sample Type:        Absolute
  RHold-REvent:       3000-1
  FHold-FEvent:       2000-2
  Alarm startup:      All
  Interval:           10
  Owner:              monitor
```

Index-State: 2-Enabled

Statistics index: 2

Alarm variable: RevPkt

Sample Type: Absolute

RHold-REvent: 3000-1

FHold-FEvent: 2000-2

Alarm startup: All

Interval: 10

Owner: monitor

7 Appendix: Default Parameters

Default settings of SNMP are listed in the following tables.

Table 7-1 Default Global Config Settings

Parameter	Default Setting
SNMP	Disabled
Local Engine ID	Automatically
Remote Engine ID	None

Table 7-2 Default SNMP View Table Settings

View Name	View Type	MIB Object ID
viewDefault	Include	1
viewDefault	Exclude	1.3.6.1.6.3.15
viewDefault	Exclude	1.3.6.1.6.3.16
viewDefault	Exclude	1.3.6.1.6.3.18

Table 7-3 Default SNMP v1/v2c Settings

Parameter	Default Setting
Community Entry	No entries
Community Name	None
Access	Read-only
MIB View	viewDefault

Table 7-4 Default SNMP v3 Settings

Parameter	Default Setting
SNMP Group	
Group Entry	No entries
Group Name	None
Security Model	v3
Security Level	NoAuthNoPriv
Read View	viewDefault
Write View	None
Notify View	None

Parameter	Default Setting
SNMP User	
User Entry	No entries
User Name	None
User Type	Local User
Group Name	None
Security Model	v3
Security Level	noAuthNoPriv
Authentication Mode	MD5 (when Security Level is configured as AuthNoPriv or AuthPriv)
Authentication Password	None
Privacy Mode	DES (when Security Level is configured as AuthPriv)
Privacy Password	None

Default settings of Notification are listed in the following table.

Table 7-5 Default Notification Settings

Parameter	Default Setting
Notification Config	
Notification Entry	No entries
IP Mode	IPv4
IP Address	None
UDP Port	162
User	None
Security Model	v1
Security Level	noAuthNoPriv
Type	Trap
Retry	None
Timeout	None
Trap Config	
Enabled SNMP Traps	SNMP Authentication, Coldstart, Warmstart, Link Status

Default settings of RMON are listed in the following tables.

Table 7-6 Default Statistics Config Settings

Parameter	Default Setting
Statistics Entry	No entries
ID	None
Port	None
Owner	None
IP Mode	Valid

Table 7-7 Default Settings for History Entries

Parameter	Default Setting
Port	1/0/1
Interval	1800 seconds
Max Buckets	50
Owner	monitor
Status	Disabled

Table 7-8 Default Settings for Event Entries

Parameter	Default Setting
User	public
Description	None
Type	None
Owner	monitor
Status	Disabled

Table 7-9 Default Settings for Alarm Entries

Parameter	Default Setting
Variable	RecBytes
Statistics	0, means no Statistics entry is selected.
Sample Type	Absolute
Rising Threshold	100
Rising Event	0, means no event is selected.
Falling Threshold	100
Falling Event	0, means no event is selected.
Alarm Type	All

Parameter	Default Setting
Interval	1800 seconds
Owner	monitor
Status	Disabled

Part 39

Diagnosing the Device & Network

CHAPTERS

1. Diagnosing the Device
2. Diagnosing the Network
3. Appendix: Default Parameters

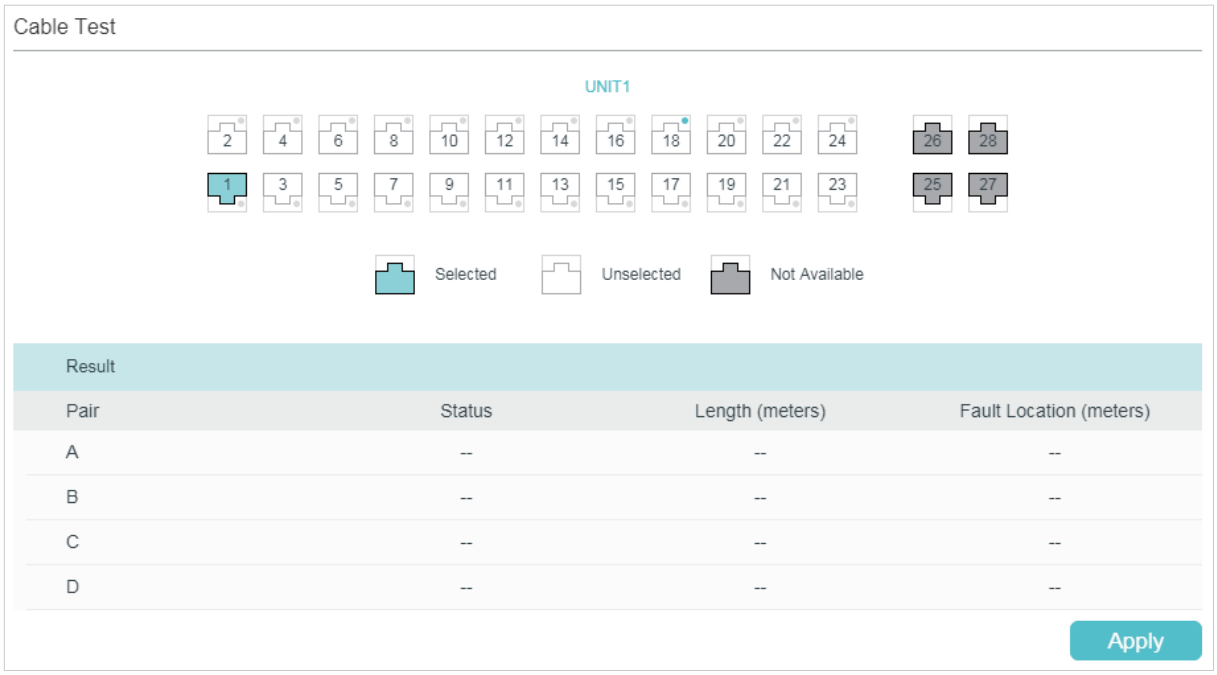
1 Diagnosing the Device

The device diagnostics feature provides cable testing, which allows you to troubleshoot based on the connection status, cable length and fault location.

1.1 Using the GUI

Choose the menu **MAINTENANCE > Device Diagnostics** to load the following page.

Figure 1-1 Diagnosing the Cable



Follow these steps to diagnose the cable:

1) Select your desired port for the test and click **Apply**.
2) Check the test results in the **Result** section.

Pair	Displays the Pair number.
Status	Displays the cable status. Test results include normal, closed, open and crosstalk. Normal : The cable is connected normally. Closed: A short circuit is being caused by abnormal contact of wires in the cable. Open: No device is connected to the other end or the connection is broken. Crosstalk: Impedance mismatch due to the poor quality of the cable.
Length	If the connection status is normal, the length range of the cable is displayed.

Fault Location	If the connection status is short, close or crosstalk, here displays the length from the port to the trouble spot.

1.2 Using the CLI

On privileged EXEC mode or any other configuration mode, you can use the following command to check the connection status of the cable that is connected to the switch.

show cable-diagnostics interface { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* }

View the cable diagnostics of the connected Ethernet Port.

port: Enter the port number in 1/0/1 format to check the result of the cable test.

show cable-diagnostics careful interface { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* }

View the cable diagnostics of the connected Ethernet Port. When taking the careful cable test, the switch will only test the cable for the port which is in the link-down status.

port: Enter the port number in 1/0/1 format to check the result of the cable test.

The following example shows how to check the cable diagnostics of port 1/0/2:

Switch#show cable-diagnostics interface gigabitEhternet 1/0/2

Port	Pair	Status	Length	Error
Gi1/0/2	Pair-A	Normal	2 (+/- 10m)	---
	Pair-B	Normal	2 (+/- 10m)	---
	Pair-C	Normal	0 (+/- 10m)	---
	Pair-D	Normal	2 (+/- 10m)	---

2 Diagnosing the Network

The network diagnostics feature provides Ping testing and Tracert testing. You can test connectivity to remote hosts, or to the gateways from the switch to the destination.

With Network Diagnostics, you can:

- Troubleshoot with Ping testing.
- Troubleshoot with Tracert testing.

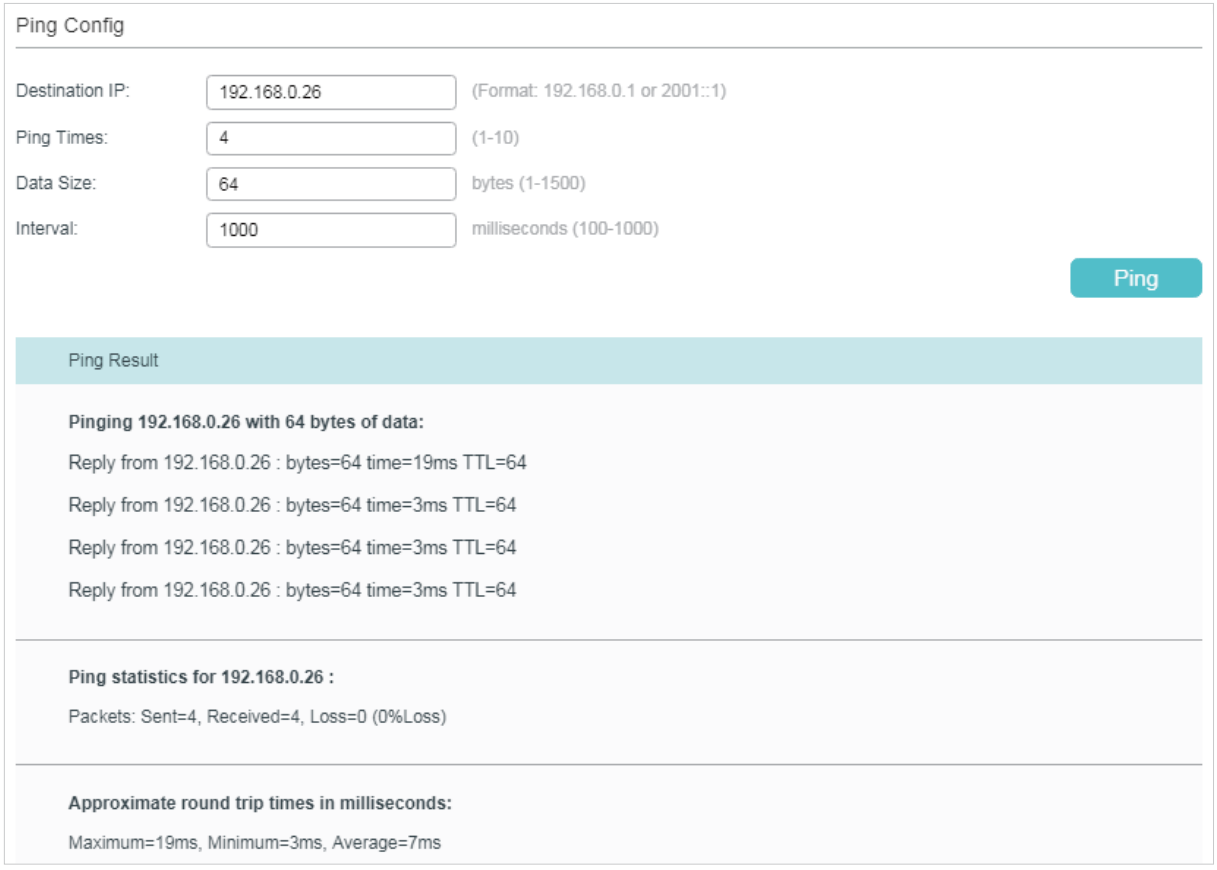
2.1 Using the GUI

2.1.1 Troubleshooting with Ping Testing

You can use the Ping tool to test connectivity to remote hosts.

Choose the menu **MAINTENANCE > Network Diagnostics > Ping** to load the following page.

Figure 2-1 Troubleshooting with Ping Testing



Follow these steps to test the connectivity between the switch and another device in the network:

1) In the **Ping Config** section, enter the IP address of the destination device for Ping test, set Ping times, data size and interval according to your needs, and then click **Ping** to start the test.

Destination IP	Enter the IP address of the destination node for Ping test. Both IPv4 and IPv6 are supported.
Ping Times	Enter the number of times test data will be sent for Ping testing. It is recommended to use the default value of 4.
Data Size	Enter the size of the data sent for Ping testing. It is recommended to keep the default value of 64 bytes.
Interval	Specify the interval at which ICMP request packets are sent. It is recommended to keep the default value of 1000 milliseconds.

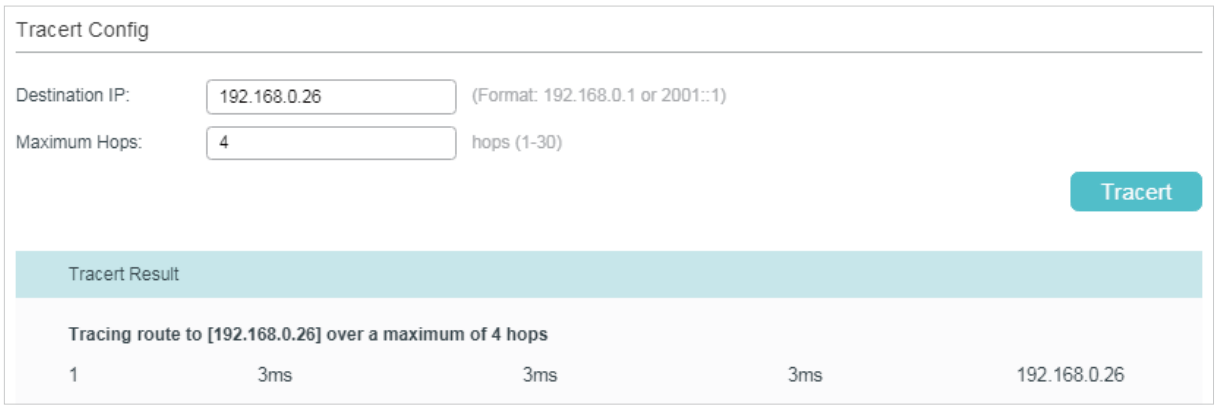
2) In the **Ping Result** section, check the test results.

2.1.2 Troubleshooting with Tracert Testing

You can use the Tracert tool to find the path from the switch to the destination, and test connectivity between the switch and routers along the path.

Choose the menu **MAINTENANCE > Network Diagnostics > Tracert** to load the following page.

Figure 2-1 Troubleshooting with Tracert Testing



Follow these steps to test connectivity between the switch and routers along the path from the source to the destination:

1) In the **Tracert Config** section, enter the IP address of the destination, set the max hop, and then click **Tracert** to start the test.

Destination IP	Enter the IP address of the destination device. Both IPv4 and IPv6 are supported.
Maximum Hops	Specify the maximum number of the route hops the test data can pass through.

2) In the **Tracert Result** section, check the test results.

2.2 Using the CLI

2.2.1 Configuring the Ping Test

On privileged EXEC mode, you can use the following command to test the connectivity between the switch and one node of the network.

ping [ip | ipv6 **] {** *ip_addr* **} [-n** *count* **] [-l** *size* **] [-i** *interval* **]**

Test the connectivity between the switch and destination device.

ip: The type of the IP address for ping test should be IPv4.

ipv6: The type of the IP address for ping test should be IPv6.

ip_addr: The IP address of the destination node for ping test. If the parameter ip/ipv6 is not selected, both IPv4 and IPv6 addresses are supported, such as 192.168.0.100 or fe80::1234.

count: Specify the amount of times to send test data for Ping testing. The values are from 1 to 10 times; the default is 4 times.

size: Specify the size of the sending data for ping testing. The values are from 1 to 1500 bytes; the default is 64 bytes.

interval: Specify the interval to send ICMP request packets. The values are from 100 to 1000 milliseconds; the default is 1000 milliseconds.

The following example shows how to test the connectivity between the switch and the destination device with the IP address 192.168.0.10. Specify the ping times as 3, the data size as 1000 bytes and the interval as 500 milliseconds:

Switch#ping ip 192.168.0.10 **-n** 3 **-l** 1000 **-i** 500

Pinging 192.168.0.10 with 1000 bytes of data :

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Ping statistics for 192.168.0.10:

Packets: Sent = 3 , Received = 3 , Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms , Maximum = 0ms , Average = 0ms

2.2.2 Configuring the Tracert Test

On privileged EXEC mode, you can use the following command to test the connectivity between the switch and routers along the path from the source to the destination:

tracert [ip | ipv6] **ip_addr** [maxHops]

Test the connectivity of the gateways along the path from the source to the destination.

ip: The type of the IP address for tracert test should be IPv4.

ipv6: The type of the IP address for tracert test should be IPv6.

ip_addr: Enter the IP address of the destination device. If the parameter ip/ipv6 is not selected, both IPv4 and IPv6 addresses are supported, such as 192.168.0.100 or fe80::1234.

maxHops: Specify the maximum number of the route hops the test data can pass though. The range is 1 to 30 hops; the default is 4 hops.

The following example shows how to test the connectivity between the switch and the network device with the IP address 192.168.0.100. Set the maxhops as 2:

Switch#tracert 192.168.0.100 2

Tracing route to 192.168.0.100 over a maximum of 2 hops

1 8 ms 1 ms 2 ms 192.168.1.1

2 2 ms 2 ms 2 ms 192.168.0.100

Trace complete.

3 Appendix: Default Parameters

Default settings of Network Diagnostics are listed in the following tables.

Table 3-1 Default Settings of Ping Config

Parameter	Default Setting
Destination IP	192.168.0.1
Ping Times	4
Data Size	64 bytes
Interval	1000 milliseconds

Table 3-2 Default Settings of Tracert Config

Parameter	Default Setting
Destination IP	192.168.0.100
Maximum Hops	4 hops

Part 40

Configuring System Logs

CHAPTERS

1. Overview
2. System Logs Configurations
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

The switch generates messages in response to events, faults, or errors occurred, as well as changes in configuration or other occurrences. You can check system messages for debugging and network management.

System logs can be saved in various destinations, such as the log buffer, log file or remote log servers, depending on your configuration. Logs saved in the log buffer and log file are called local logs, and logs saved in remote log servers are called remote logs. Remote logs facilitate you to remotely monitor the running status of the network.

You can set the severity level of the log messages to control the type of log messages saved in each destination.

2 System Logs Configurations

System logs configurations include:

- Configure the local logs.
- Configure the remote logs.
- Backing up the logs.
- Viewing the log table.

Configuration Guidelines

Logs are classified into the following eight levels. Messages of levels 0 to 4 mean the functionality of the switch is affected. Please take actions according to the log message.

Table 2-1 Levels of Logs

Severity	Level	Description	Example
Emergencies	0	The system is unusable and you have to reboot the switch.	Software malfunctions affect the functionality of the switch.
Alerts	1	Actions must be taken immediately.	The memory utilization reaches the limit.
Critical	2	Cause analysis or actions must be taken immediately.	The memory utilization reaches the warning threshold.
Errors	3	Error operations or unusual processing that will not affect subsequent operations but that should be noted and analyzed.	Wrong command or password is entered.
Warnings	4	Conditions that may cause process failure and that should be noted.	Error protocol packets are detected.
Notifications	5	Normal but significant conditions.	The **shutdown** command is applied to a port.
Informational	6	Normal messages for your information.	The **display** command is used.
Debugging	7	Debug-level messages that you can ignore.	General operational information.

2.1 Using the GUI

2.1.1 Configuring the Local Logs

Choose the menu **MAINTENANCE > Logs > Local Logs** to load the following page.

Figure 2-1 Configuring the Local Logs

Follow these steps to configure the local logs:

1) Select your desired channel and configure the corresponding severity and status.

Channel	Local logs includes 2 channels: log buffer and log file. Log buffer indicates the RAM for saving system logs. The channel is enabled by default. Information in the log buffer is displayed on the **MAINTENANCE > Logs > Logs Table** page. It will be lost when the switch is restarted. Log file indicates the flash sector for saving system logs. Information in the log file will not be lost after the switch is restarted and can be exported on the **MAINTENANCE > Logs > Back Up Logs** page.
Severity	Specify the severity level of the log messages that are saved to the selected channel. Only log messages with a severity level value that is the same or lower than this will be saved. There are eight severity levels marked from 0 to 7. A lower value indicates a higher severity.
Status	Enable or disable the channel.
Sync-Periodic	By default, the log information is saved in the log buffer immediately, and synchronized to the log file every 24 hours. If necessary, you can modify the log synchronization frequency using the CLI.

2) Click **Apply**.

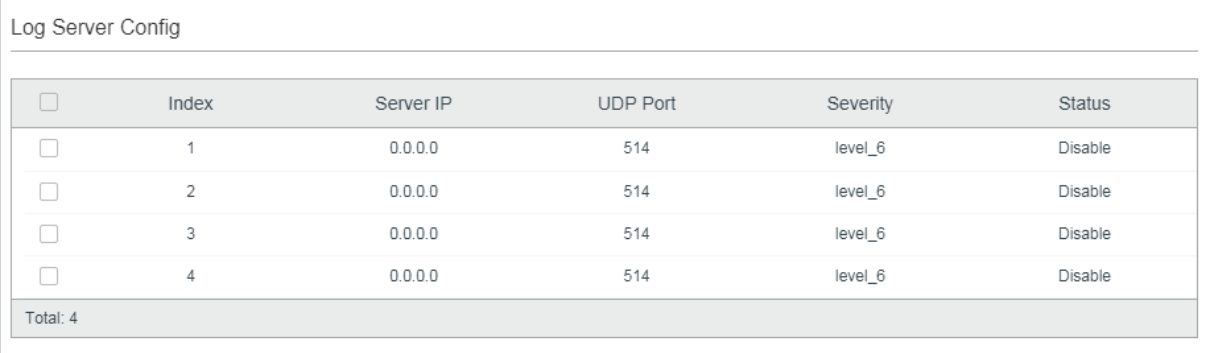
2.1.2 Configuring the Remote Logs

You can configure up to four hosts to receive the switch's system logs. These hosts are called Log Servers. The switch will forward the log message to the servers once a log

message is generated. To display the logs, the servers should run a log server software that complies with the syslog standard.

Choose the menu **MAINTENANCE > Logs > Remote Logs** to load the following page.

Figure 2-2 Configuring the Remote Logs



Follow these steps to configure the information of remote log servers:

1) Select an entry to enable the server, and then set the server IP address and severity.

Server IP	Specify an IP address of the log server.
UDP Port	Displays the UDP port used by the server to receive the log messages. The switch uses standard port 514 to send log messages.
Severity	Specify the severity level of the log messages sent to the selected log server. Only log messages with a severity level value that is the same or lower than this will be saved.
Status	Enable or disable the log server.

2) Click **Apply**.

2.1.3 Backing up the Logs

Choose the menu **MAINTENANCE > Logs > Back Up Logs** to load the following page.

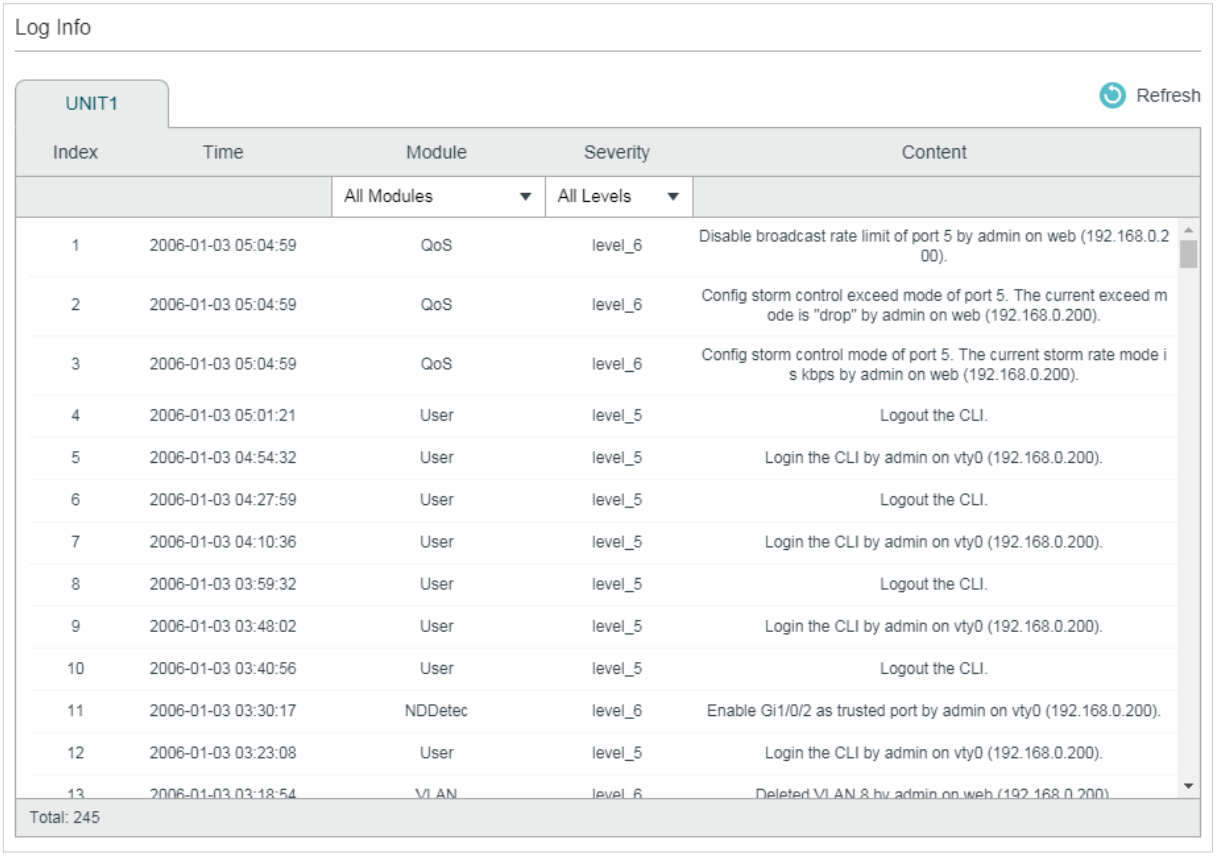
Figure 2-3 Backing up the Log File

Click **Back Up Logs** to save the system logs as a file on your computer. If the switch system breaks down, you can check the file for troubleshooting.

2.1.4 Viewing the Log Table

Choose the menu **MAINTENANCE > Logs > Log Table** to load the following page.

Figure 2-4 View the Log Table



Select a module and a severity to view the corresponding log information.

Time	Displays the time the log event occurred. To get the exact time when the log event occurs, you need to configure the system time on the **SYSTEM > System Info > System Time** Web management page.
Module	Select a module from the drop-down list to display the corresponding log information.
Severity	Select a severity level to display the log information whose severity level value is the same or smaller.
Content	Displays the detailed information of the log event.

2.2 Using the CLI

2.2.1 Configuring the Local Logs

Follow these steps to configure the local logs:

Step 1	**configure** Enter global configuration mode.
Step 2	**logging buffer** Configure the switch to save system messages in log buffer. Log buffer indicates the RAM for saving system logs. Information in the log buffer will be lost when the switch is restarted. You can view the logs with **show logging buffer** command.
Step 3	**logging buffer level** *level* Specify the severity level of the log information that should be saved to the buffer. *level*: Enter the severity level ranging from 0 to 7. A lower value indicates a higher severity. Only log messages with a severity level value that is the same or lower than this will be saved. The default level is 6, indicating that the log information of levels 0 to 6 will be saved in the log buffer.
Step 4	**logging file flash** Configure the switch to save system messages in log file. Log file indicates the flash sector for saving system logs. Information in the log file will not be lost after the switch is restarted. You can view the logs with **show logging flash** command.
Step 5	**logging file flash frequency** { **periodic** *periodic* | **immediate** } Specify the frequency to synchronize the system logs in the log buffer to the flash. *periodic*: Specify the frequency ranging from 1 to 48 hours. By default, the synchronization process takes place every 24 hours. **immediate**: The system log file in the buffer will be synchronized to the flash immediately. This option means frequent operations on the flash and is not recommended.
Step 6	**logging file flash level** *level* Specify the severity level of the log information that should be saved to the flash. *level*: Enter the severity level ranging from 0 to 7. A lower value indicates a higher severity. Only log messages with a severity level value that is the same or lower than this will be saved to the flash. The default level is 3, indicating that the log messages of levels 0 to 3 will be saved in the log flash.
Step 7	**show logging local-config** View the configuration information of the local logs.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the local logs on the switch. Save logs of levels 0 to 5 to the log buffer, and synchronize logs of levels 0 to 2 to the flash every 10 hours:

Switch#configure

Switch(config)#logging buffer

Switch(config)#logging buffer level 5

Switch(config)#logging file flash

Switch(config)#logging file flash frequency periodic 10

Switch(config)#logging file flash level 2

Switch(config)#show logging local-config

Channel	Level	Status	Sync-Periodic
-------	-----	------	-------------
Buffer	5	enable	Immediately
Flash	2	enable	10 hour(s)
Console	5	enable	Immediately
Monitor	5	enable	Immediately

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring the Remote Logs

You can configure up to four hosts to receive the switch's system logs. These hosts are called Log Servers. The switch will forward the log message to the servers once a log message is generated. To display the logs, the servers should run a log server software that complies with the syslog standard.

Follow these steps to set the remote log:

Step 1	**configure** Enter global configuration mode.

Step 2	**logging host index** *idx host-ip level* Configure a remote host to receive the switch's system logs. The host is called Log Server. You can remotely monitor the settings and operation status of the switch through the log server. *idx*: Enter the index of the log server. The switch supports 4 log servers at most. *host-ip*: Enter the IP address of the log server. *level*: Specify the severity level of the log messages sent to the log server. The range is from 0 to 7, and a lower value indicates a higher severity. Only log messages with a severity level value that is the same or lower than this will be sent. The default is 6, indicating that the log information of levels 0 to 6 will be sent to the log server.
Step 3	**show logging loghost** [*index*] View the configuration information of the log server. *index*: Enter the index of the log server to view the corresponding configuration information. If no value is specified, information of all log hosts will be displayed.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the remote log on the switch. Enable log server 2, set its IP address as 192.168.0.148, and allow logs of levels 0 to 5 to be sent to the server:

Switch#configure

Switch(config)# logging host index 2 192.168.0.148 5

Switch(config)# show logging loghost

Index	Host-IP	Severity	Status
1	0.0.0.0	6	disable
2	192.168.0.148	5	enable
3	0.0.0.0	6	disable
4	0.0.0.0	6	disable

Switch(config)#end

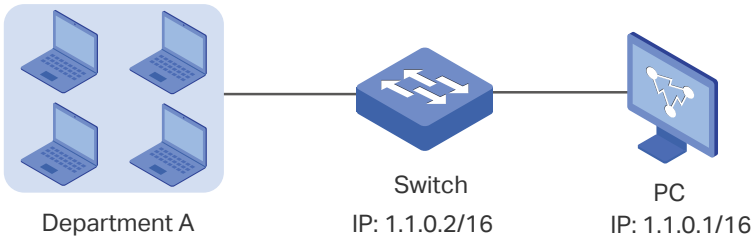
Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

The company network manager needs to monitor network of department A for troubleshooting.

Figure 3-1 Network Topology



3.2 Configuration Scheme

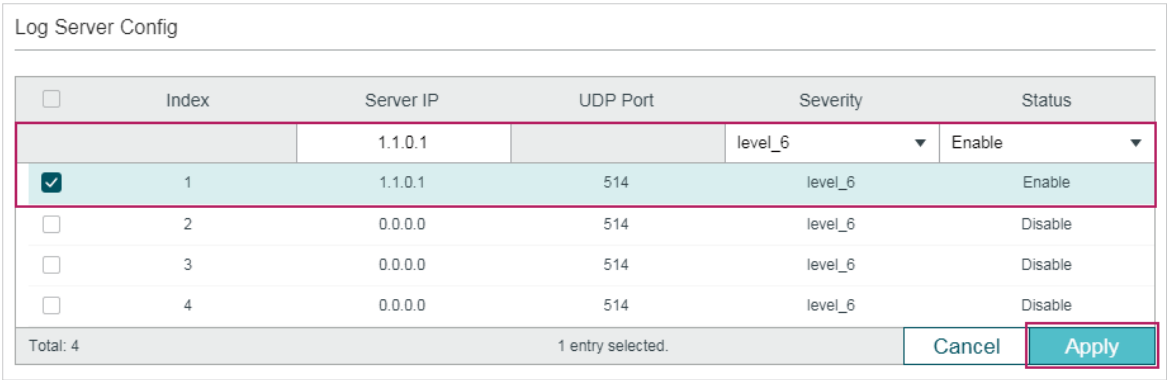
The network manager can configure the PC as a log server to receive the switch's system logs. Make sure the switch and the PC are reachable to each other; configure a log server that complies with the syslog standard on the PC and set the PC as the log server.

Demonstrated with T1600G-52TS, this chapter provides configuration procedures in two ways: using the GUI and Using the CLI.

3.3 Using the GUI

1) Choose the menu **MAINTENANCE > Logs > Remote Logs** to load the following page. Enable host 1, and set the PC's IP address 1.1.0.1 as the server IP address, and the severity as level_5; click **Apply**.

Figure 3-2 Configuring the Log Server



2) Click Save to save the settings.

3.4 Using the CLI

Configure the remote log host.

Switch#configure

Switch(config)# logging host index 1 1.1.0.1 5

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configurations

Switch# show logging loghost

Index	Host-IP	Severity	Status
1	1.1.0.1	5	enable
2	0.0.0.0	6	disable
3	0.0.0.0	6	disable
4	0.0.0.0	6	disable

4 Appendix: Default Parameters

Default settings of maintenance are listed in the following tables.

Table 4-1 Default Settings of Local Logs

Parameter	Default Setting
Status of Log Buffer	Enabled
Severity of Log Buffer	Level_6
Sync-Periodic of Log Buffer	Immediately
Status of Log File	Disabled
Severity of Log File	Level_3
Sync-Periodic of Log File	24 hours

Table 4-2 Default Settings of Remote Logs

Parameter	Default Setting
Server IP	0.0.0.0
UDP Port	514
Severity	Level_6
Status	Disabled

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. tp-link is a registered trademark of TP-Link Corporation Limited. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Corporation Limited. Copyright © 2020 TP-Link Corporation Limited. All rights reserved.

https://www.tp-link.com