Managing MAC Address Table

CHAPTERS

This guide applies to:

T1500G-8T v2 or above, T1500G-10PS v2 or above, T1500G-10MPS v2 or above, T1500-28PCT v3 or above, T1600G-18TS v2 or above, T1600G-28TS v3 or above, T1600G-28PS v3 or above, T1600G-52TS v3 or above, T1600G-52PS v3 or above, T1700X-16TS v3 or above, T1700G-28TQ v3 or above, T2500G-10TS v2 or above, T2600G-18TS v2 or above, T2600G-28TS v3 or above, T2600G-28MPS v3 or above, T2600G-28SQ v1 or above, T2600G-52TS v3 or above.

1 MAC Address Table

1.1 Overview

The MAC address table contains address information that the switch uses to forward packets. As shown below, the table lists map entries of MAC addresses, VLAN IDs and ports. These entries can be manually added or automatically learned by the switch. Based on the MAC-address-to-port mapping in the table, the switch can forward packets only to the associated port.

Table 1-1 The MAC Address Table

MAC Address	VLAN ID	Port	Type	Aging Status
00:00:00:00:00:01	1	1	Dynamic	Aging
00:00:00:00:00:01	1	2	Static	No-Aging
...				

1.2 Supported Features

The address table of the switch contains dynamic addresses, static addresses and filtering addresses. You can add or remove these entries according to your needs. Furthermore, you can configure notification traps and limit the number of MAC addresses in a VLAN for traffic safety.

Address Configurations

- Dynamic address

Dynamic addresses are addresses learned by the switch automatically, and the switch regularly ages out those that are not in use. That is, the switch removes the MAC address entries related to a network device if no packet is received from the device within the aging time. And you can specify the aging time if needed.

- Static address

Static addresses are manually added to the address table and do not age. For some relatively fixed connection, for example, frequently visited server, you can manually set the MAC address of the server as a static entry to enhance the forwarding efficiency of the switch.

- Filtering address

Filtering addresses are manually added and determine the packets with specific source or destination MAC addresses that will should dropped by the switch.

Security Configurations

Note:

T1500/T1600G series switches do not support MAC Notification or MAC VLAN Security.

- Configuring MAC Notification Traps

You can configure traps and SNMP (Simple Network Management Protocol) to monitor and receive notifications of the usage of the MAC address table and the MAC address change activity. For example, you can configure the switch to send notifications when a new MAC address is learned, so the administrator knows a new users accesses the network.

- Limiting the Number of MAC Addresses in VLANs

You can configure VLAN Security to limit the number of MAC addresses that can be learned in specified VLANs. The switch will not learn addresses when the number of learned addresses has reached the limit, preventing the address table from being used up by broadcasting packets of MAC address attacks.

2 Address Configurations

With MAC address table, you can:

- Add static MAC address entries
- Change the address aging time
- Add filtering address entries
- View address table entries

2.1 Using the GUI

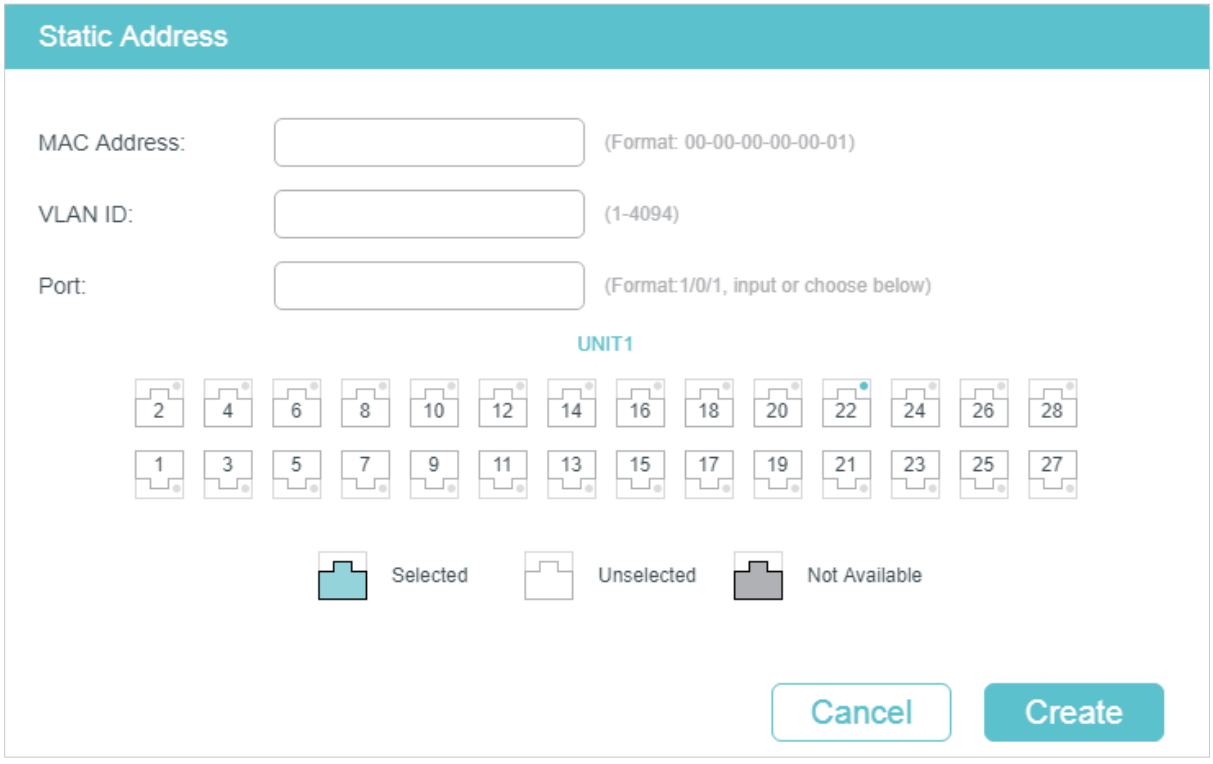
2.1.1 Adding Static MAC Address Entries

You can add static MAC address entries by manually specifying the desired MAC address or binding dynamic MAC address entries.

- Adding MAC Addresses Manually

Choose the menu **L2 FEATURES > Switching > MAC Address > Static Address** and click Add to load the following page.

Figure 2-1 Adding MAC Addresses Manually



Follow these steps to add a static MAC address entry:

1) Enter the MAC address, VLAN ID and select a port to bind them together as an address entry.

MAC Address	Enter the static MAC address to be added to the static MAC address entry.
VLAN ID	Specify an existing VLAN in which packets with the specific MAC address are received.
Port	Specify a port to which packets with the specific MAC address are forwarded. The port must belong to the specified VLAN. After you have added the static MAC address, if the corresponding port number of the MAC address is not correct, or the connected port (or the device) has been changed, the switch cannot forward the packets correctly. Please reset the static address entry appropriately.

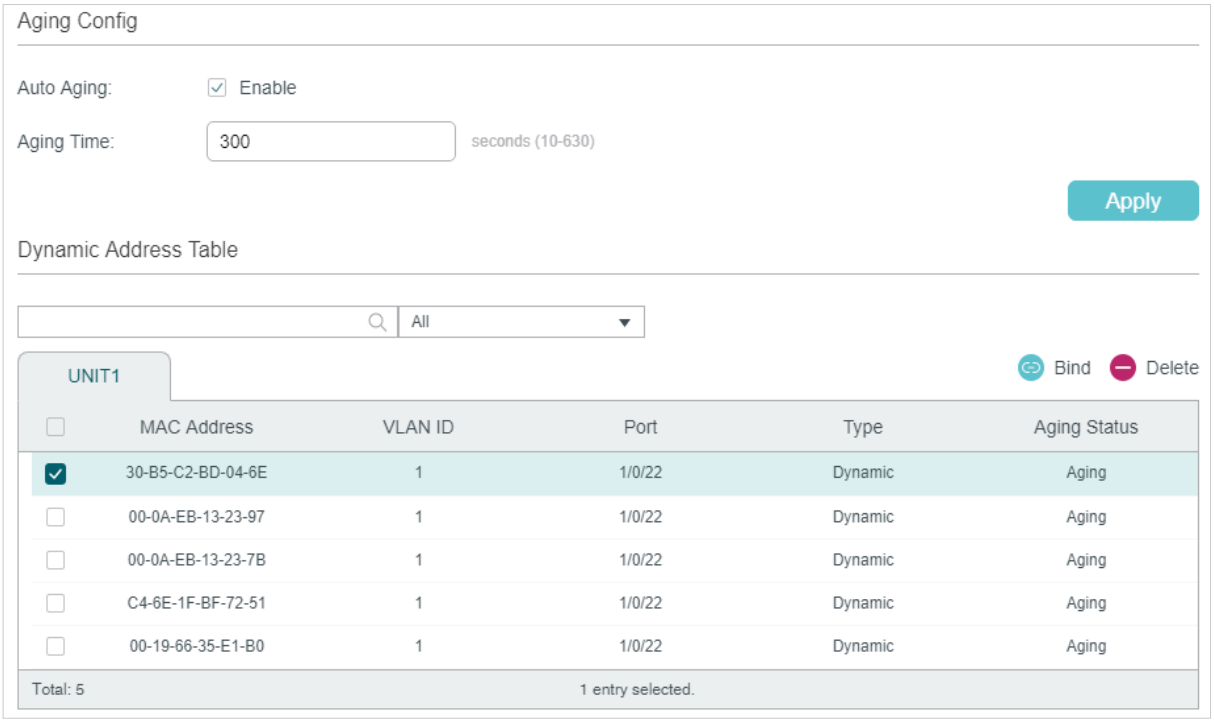
2) Click **Create**.

Binding Dynamic Address Entries

If some dynamic address entries are frequently used, you can bind these entries as static entries.

Choose the menu **L2 FEATURES > Switching > MAC Address > Dynamic Address** to load the following page.

Figure 2-2 Binding Dynamic MAC Address Entries



Follow these steps to bind dynamic MAC address entries:

1) In the **Dynamic Address Table**section, Select your desired MAC address entries.
2) Click **Bind, and** then the selected entries will become static MAC address entries.

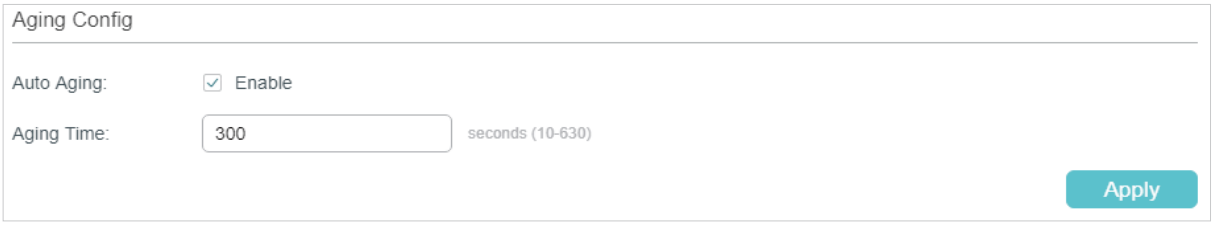
Note:

- In the same VLAN, once an address is configured as a static address, it cannot be set as a filtering address, and vice versa.
- Multicast or broadcast addresses cannot be set as static addresses.
- Ports in LAGs (Link Aggregation Group) are not supported for static address configuration.

2.1.2 Modifying the Aging Time of Dynamic Address Entries

Choose the menu **L2 FEATURES > Switching > MAC Address > Dynamic Address** to load the following page.

Figure 2-3 Modifying the Aging Time of Dynamic Address Entries



Follow these steps to modify the aging time of dynamic address entries:

1) In the **Aging Config** section, enable Auto Aging, and enter your desired length of time.

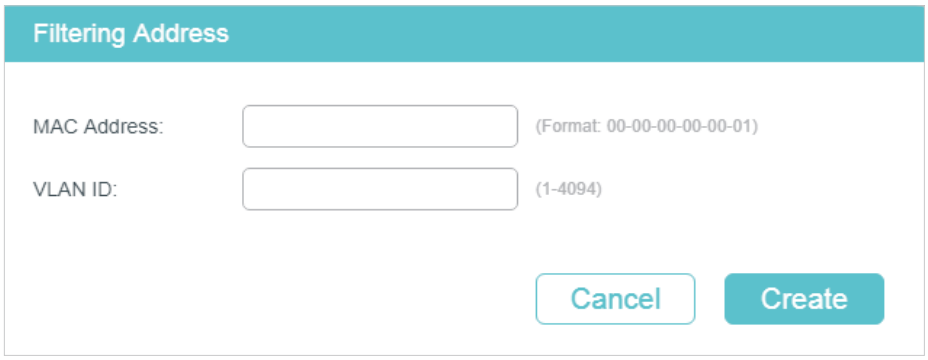
Auto Aging	Enable Auto Aging, then the switch automatically updates the dynamic address table with the aging mechanism. By default, it is enabled.
Aging Time	Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The valid values are from 10 to 630 seconds, and the default value is 300. A short aging time is applicable to networks where network topology changes frequently, and a long aging time is applicable to stable networks. We recommend that you keep the default value if you are unsure about settings in your case.

2) Click **Apply.**

2.1.3 Adding MAC Filtering Address Entries

Choose the menu **L2 FEATURES > Switching > MAC Address > Filtering Address** and click Add to load the following page.

Figure 2-4 Adding MAC Filtering Address Entries



Follow these steps to add MAC filtering address entries:

1) Enter the MAC Address and VLAN ID.

MAC Address	Specify the MAC address to be used by the switch to filter the received packets.
VLAN ID	Specify an existing VLAN in which packets with the specific MAC address are dropped.

2) Click **Create**.

Note:

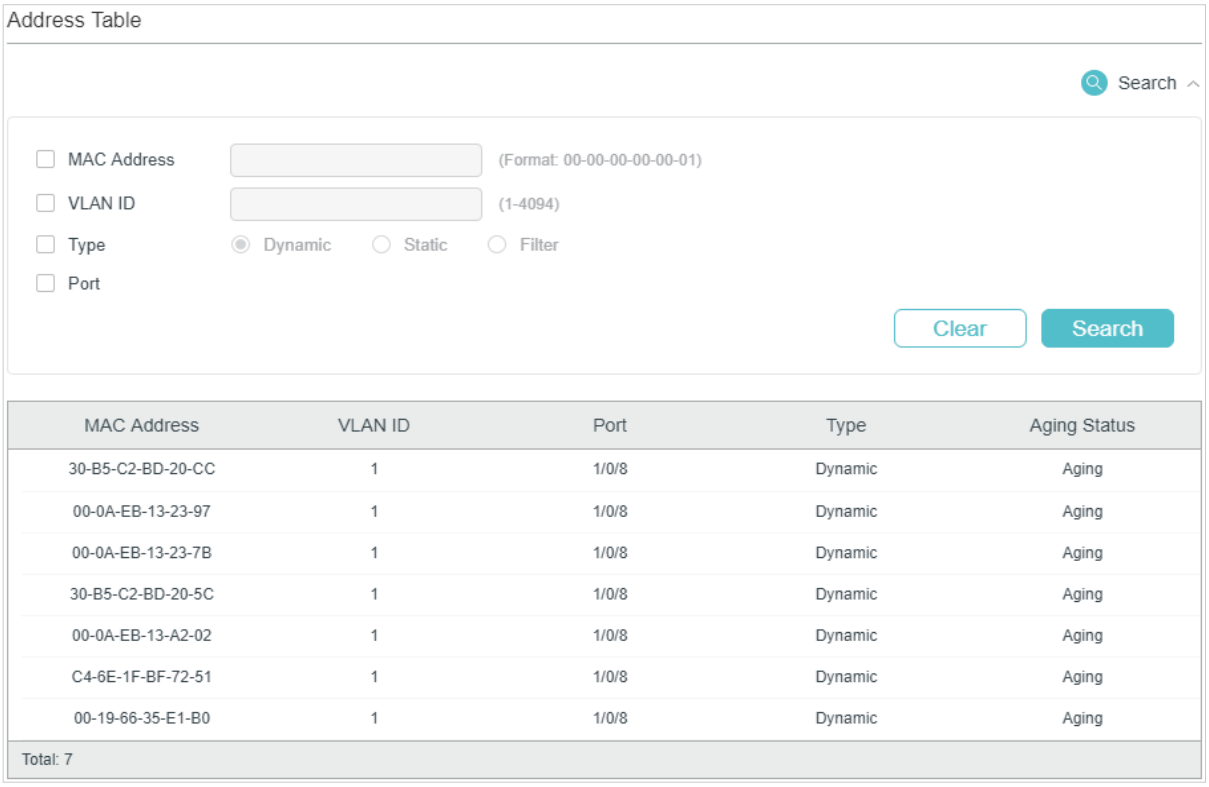
- In the same VLAN, once an address is configured as a filtering address, it cannot be set as a static address, and vice versa.
- Multicast or broadcast addresses cannot be set as filtering addresses.

2.1.4 Viewing Address Table Entries

You can view entries in MAC address table to check your former operations and address information.

Choose the menu **L2 FEATURES > Switching > MAC Address > Address Table** and click Search to load the following page.

Figure 2-5 Viewing Address Table Entries



2.2 Using the CLI

2.2.1 Adding Static MAC Address Entries

Follow these steps to add static MAC address entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**mac address-table static** *mac-addr* **vid** *vid* **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Bind the MAC address, VLAN and port together to add a static address to the VLAN. *mac-addr*: Enter the MAC address, and packets with this destination address received in the specified VLAN are forwarded to the specified port. The format is xx:xx:xx:xx:xx:xx, for example, 00:00:00:00:00:01. *vid*: Specify an existing VLAN in which packets with the specific MAC address are received. *port:* Specify a port to which packets with the specific MAC address are forwarded. The port must belong to the specified VLAN.

Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

Note:

- In the same VLAN, once an address is configured as a static address, it cannot be set as a filtering address, and vice versa.
- Multicast or broadcast addresses cannot be set as static addresses.
- Ports in LAGs (Link Aggregation Group) are not supported for static address configuration.

The following example shows how to add a static MAC address entry with MAC address 00:02:58:4f:6c:23, VLAN 10 and port 1. When a packet is received in VLAN 10 with this address as its destination, the packet will be forwarded only to port 1/0/1.

Switch#configure

Switch(config)# mac address-table static 00:02:58:4f:6c:23 **vid** 10 **interface gigabitEthernet** 1/0/1

Switch(config)#show mac address-table static

MAC Address Table

MAC	VLAN	Port	Type	Aging
00:02:58:4f:6c:23	10	Gi1/0/1	config static	no-aging

Total MAC Addresses for this criterion: 1

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Modifying the Aging Time of Dynamic Address Entries

Follow these steps to modify the aging time of dynamic address entries:

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

Step 2	**mac address-table aging-time** *aging-time* Set your desired length of address aging time for dynamic address entries. *aging-time:* Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The valid values are from10 to 630. Value 0 means the Auto Aging function is disabled. The default value is 300 and we recommend you keep the default value if you are unsure.
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 modify the aging time to 500 seconds. A dynamic entry remains in the MAC address table for 500 seconds after the entry is used or updated.

Switch#configure

Switch(config)# mac address-table aging-time 500

Switch(config)#show mac address-table aging-time

Aging time is 500 sec.

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Adding MAC Filtering Address Entries

Follow these steps to add MAC filtering address entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**mac address-table filtering** *mac-addr* **vid** *vid* Add the filtering address to the VLAN. *mac-addr:* Specify a MAC address to be used by the switch to filter the received packets. The switch will drop packets of which the source address or destination address is the specified MAC address. The format is xx:xx:xx:xx:xx:xx, for example, 00:00:00:00:00:01. *vid:* Specify an existing VLAN in which packets with the specific MAC address will be dropped.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

Note:

- In the same VLAN, once an address is configured as a filtering address, it cannot be set as a static address, and vice versa.
- Multicast or broadcast addresses cannot be set as filtering addresses.

The following example shows how to add the MAC filtering address 00:1e:4b:04:01:5d to VLAN 10. Then the switch will drop the packet that is received in VLAN 10 with this address as its source or destination.

Switch#configure

Switch(config)# mac address-table filtering 00:1e:4b:04:01:5d **vid** 10

Switch(config)#show mac address-table filtering

MAC Address Table

MAC	VLAN	Port	Type	Aging
00:1e:4b:04:01:5d	10		filter	no-aging

Total MAC Addresses for this criterion: 1

Switch(config)#end

Switch#copy running-config startup-config

3 Security Configurations

Note:

T1500/T1600G series switches do not support MAC Notification or MAC VLAN Security.

With security configurations of the MAC address table, you can:

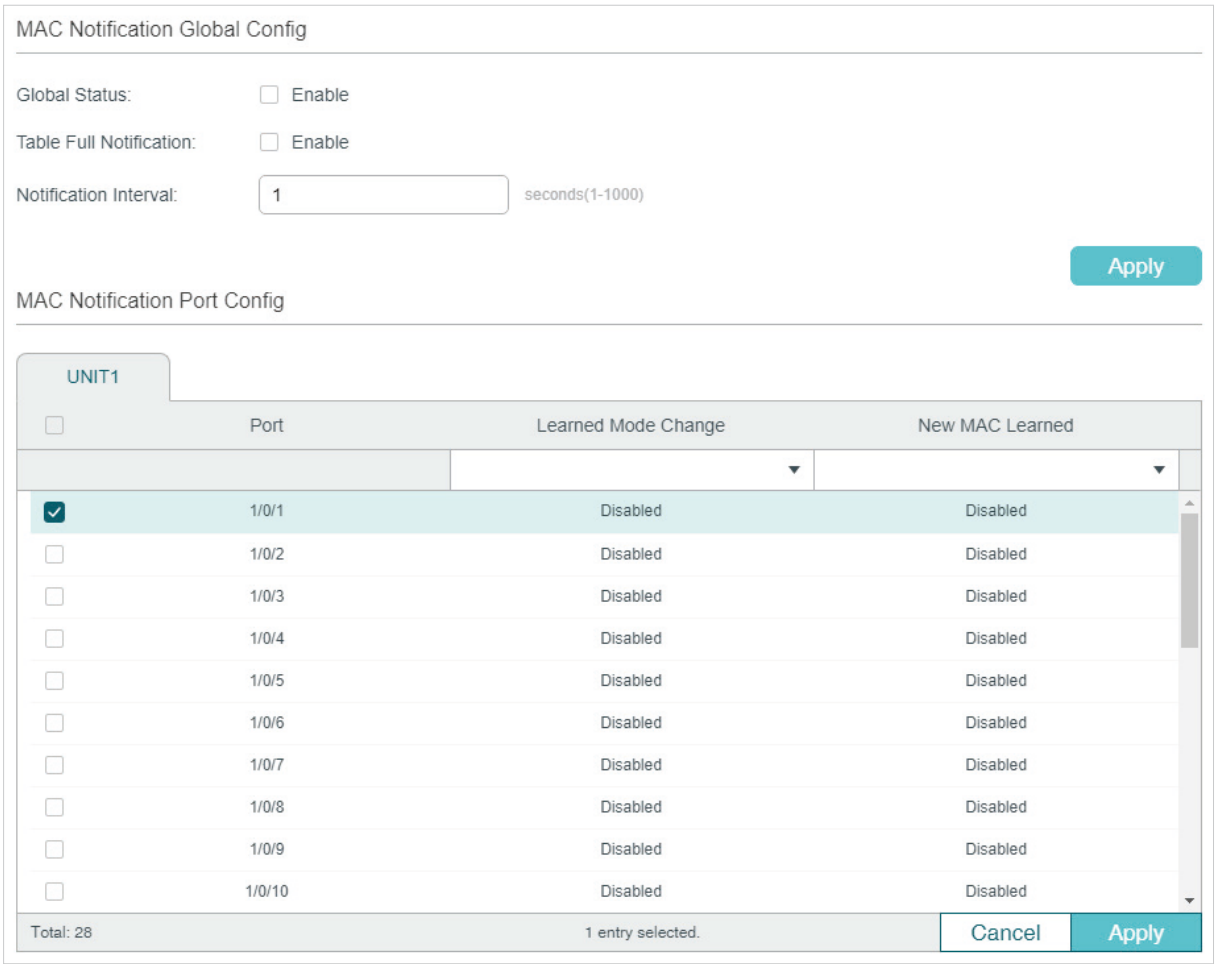
- Configure MAC notification traps.
- Configure MAC VLAN Security to limit the number of MAC addresses in VLANs.

3.1 Using the GUI

3.1.1 Configuring MAC Notification Traps

Choose the menu **L2 FEATURES > Switching > MAC Address > MAC Notification** to load the following page.

Figure 3-1 Configuring MAC Notification Traps



Follow these steps to configure MAC notification traps:

1) In the **MAC Notification Global Config** section, enable this feature, configure the relevant options, and click **Apply**.

Global Status	Enable MAC notification feature globally.
Table Full Notification	Enable Table Full Notification, and when address table is full, a notification will be generated and sent to the management host.
Notification Interval	Specify the time value of Notification Interval. Notification Interval is the interval at which the New MAC Learned notifications are continuously sent.

2) In the **MAC Notification Port Config** section, select one or more ports to configure the notification status. Click **Apply**.

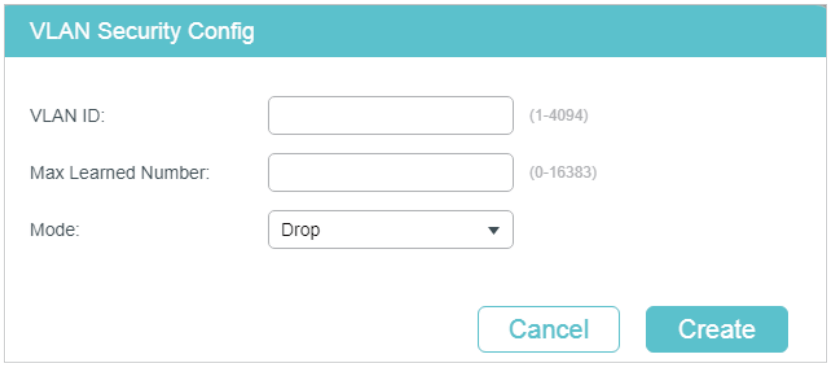
Learned Mode Change	Enable Learned Mode Change, and when the learned mode of the specified port is changed, a notification will be generated and sent to the management host.
New MAC Learned	Enable New MAC Learned, and when the specified port learns a new MAC address, a notification will be generated and sent to the management host.

3) Configure SNMP and set a management host. For detailed SNMP configurations, please refer to *Configuring SNMP & RMON.*

3.1.2 Limiting the Number of MAC Addresses Learned in VLANs

Choose the menu **L2 FEATURES > Switching > MAC Address > MAC VLAN Security** and click Add to load the following page.

Figure 3-2 Limiting the Number of MAC Addresses in VLANs



Follow these steps to limit the number of MAC addresses in VLANs:

1) Enter the VLAN ID to limit the number of MAC addresses that can be learned in the specified VLAN.

VLAN ID	Specify an existing VLAN in which you want to limit the number of MAC addresses.

2) Enter your desired value in **Max Learned Number** to set a threshold.

Max Learned Number	Set the maximum number of MAC addresses in the specific VLAN. It ranges from 0 to 16383. You can control the available address table space by setting maximum learned MAC number for VLANs. However, an improper maximum number can cause unnecessary floods in the network or a waste of address table space. Therefore, before you set the number limit, please be sure you are familiar with the network topology and the switch system configuration.

3) Choose the mode that the switch adopts when the maximum number of MAC addresses in the specified VLAN is exceeded.

Drop	Packets with new source MAC addresses in the VLAN will be dropped when the maximum number of MAC addresses in the specified VLAN is exceeded.
Forward	Packets of new source MAC addresses will be forwarded but the addresses will not be learned when the maximum number of MAC addresses in the specified VLAN is exceeded.

4) Click **Create**.

3.2 Using the CLI

3.2.1 Configuring MAC Notification Traps

Follow these steps to configure MAC notification traps:

Step 1	**configure** Enter global configuration mode.
Step 2	**mac address-table notification global-status {**enable | disable**}** Enable MAC Notification globally. enable | disable: Enable or disable MAC Notification globally.
Step 3	**mac address-table notification table-full-status [**enable | disable**]** (Optional) Enable Table Full Notification. enable | disable: With Table Full Notification enabled, when address table is full, a notification will be generated and sent to the management host.
Step 4	**mac address-table notification interval** *time* Specify the time value of Notification Interval. Notification Interval is the interval at which the New MAC Learned notifications are continuously sent. *time:* Specify the Notification Interval in seconds between 1to 1000. By default, it is 1 second.
Step 5	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **}** Configure notification traps on the specified port. *port/ port-list:* The number or the list of the Ethernet port that you want to configure notification traps.

Step 6	**mac address-table notification {[learn-mode-change** enable | disable] **[new-mac-learned** enable | disable]**}** Enable learn-mode-change, exceed-max-learned, or new-MAC-learned notification traps on the specified port. enable | disable:Enable or disable learn-mode-change, exceed-max-learned, or new-MAC-learned notification traps on the specified port. **learn-mode-change**: With learn-mode-change enabled, when the learned mode of the specified port is changed, a notification will be generated and sent to the management host. **new-mac-learned**: With new-mac-learned enabled, when the specified port learns a new MAC address, a notification will be generated and sent to the management host.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

Now you have configured MAC notification traps. To receive notifications, you need to further enable SNMP and set a management host. For detailed SNMP configurations, please refer to *Configuring SNMP & RMON.*

The following example shows how to enable new-MAC-learned trap on port 1, and set the interval time as 10 seconds. After you have further configured SNMP, the switch will bundle notifications of new addresses in every 10 seconds and send to the management host.

Switch#configure

Switch(config)#mac address-table notification global-status enable

Switch(config)#mac address-table notification interval 10

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

Switch(config-if)#mac address-table notification new-mac-learned enable

Switch(config-if)#show mac address-table notification interface gigabitEthernet 1/0/1

Mac Notification Global Config

Notification Global Status : enable

Table Full Notification Status: disable

Notification Interval : 10

Port LrnMode Change New Mac Learned

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

Gi1/0/1 disable enable

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.2 Limiting the Number of MAC Addresses in VLANs

Follow these steps to limit the number of MAC addresses in VLANs:

Step 1	**configure** Enter global configuration mode.
Step 2	**mac address-table security vid** *vid* **max-learn** *num* **{**drop | forward**}** Configure the maximum number of MAC addresses in the specified VLAN and select a mode for the switch to adopt when the maximum number is exceeded. *vid*: Specify an existing VLAN in which you want to limit the number of MAC addresses. *num*: Set the maximum number of MAC addresses in the specific VLAN. It ranges from 0 to 16383. drop | forward: The mode that the switch adopts when the maximum number of MAC addresses in the specified VLAN is exceeded. drop: Packets of new source MAC addresses in the VLAN will be dropped when the maximum number of MAC addresses in the specified VLAN is exceeded. forward: Packets of new source MAC addresses will be forwarded but the addresses not learned when the maximum number of MAC addresses in the specified VLAN is exceeded.
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 limit the number of MAC addresses to 100 in VLAN 10, and configure the switch to drop packets of new source MAC addresses when the limit is exceeded.

Switch#configure

Switch(config)#mac address-table security vid 10 **max-learn** 100 drop

Switch(config)#show mac address-table security vid 10

VlanId	Max-learn	Current-learn	Status
10	100	0	Drop

Switch(config)#end

Switch#copy running-config startup-config

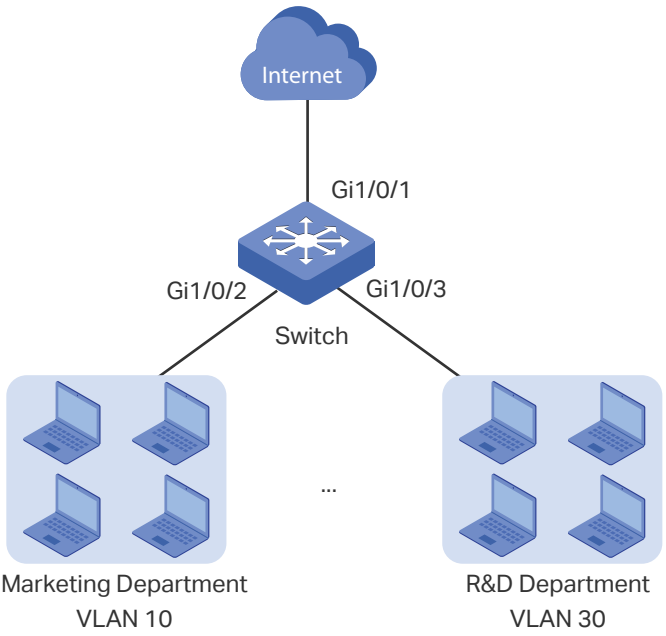
4 Example for Security Configurations

4.1 Network Requirements

Several departments are connected to the company network as shown in Figure 4-1. Now the Marketing Department that is in VLAN 10 has network requirements as follows:

- Free the network system from illegal accesses and MAC address attacks by limiting the number of access users in this department to 100.
- Assist the network manager supervising the network with notifications of any new access users.

Figure 4-1 The Network Topology



4.2 Configuration Scheme

VLAN Security can be configured to limit the number of access users and in this way to prevent illegal accesses and MAC address attacks.

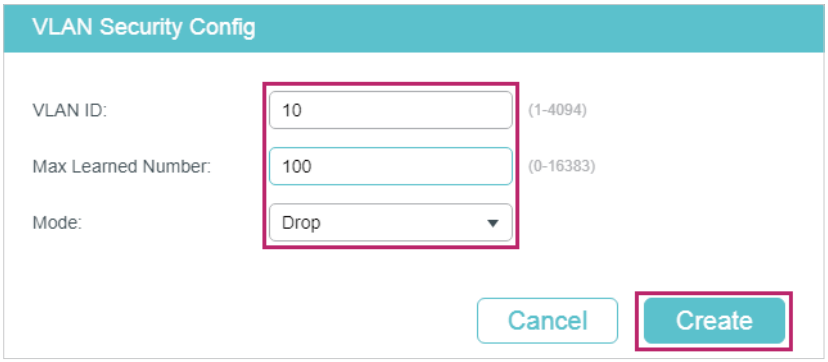
MAC Notification and SNMP can be configured to monitor the interface which is used by the Marketing Department. Enable the new-MAC-learned notification and the SNMP, then the network manager can get notifications when new users access the network.

Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

4.3 Using the GUI

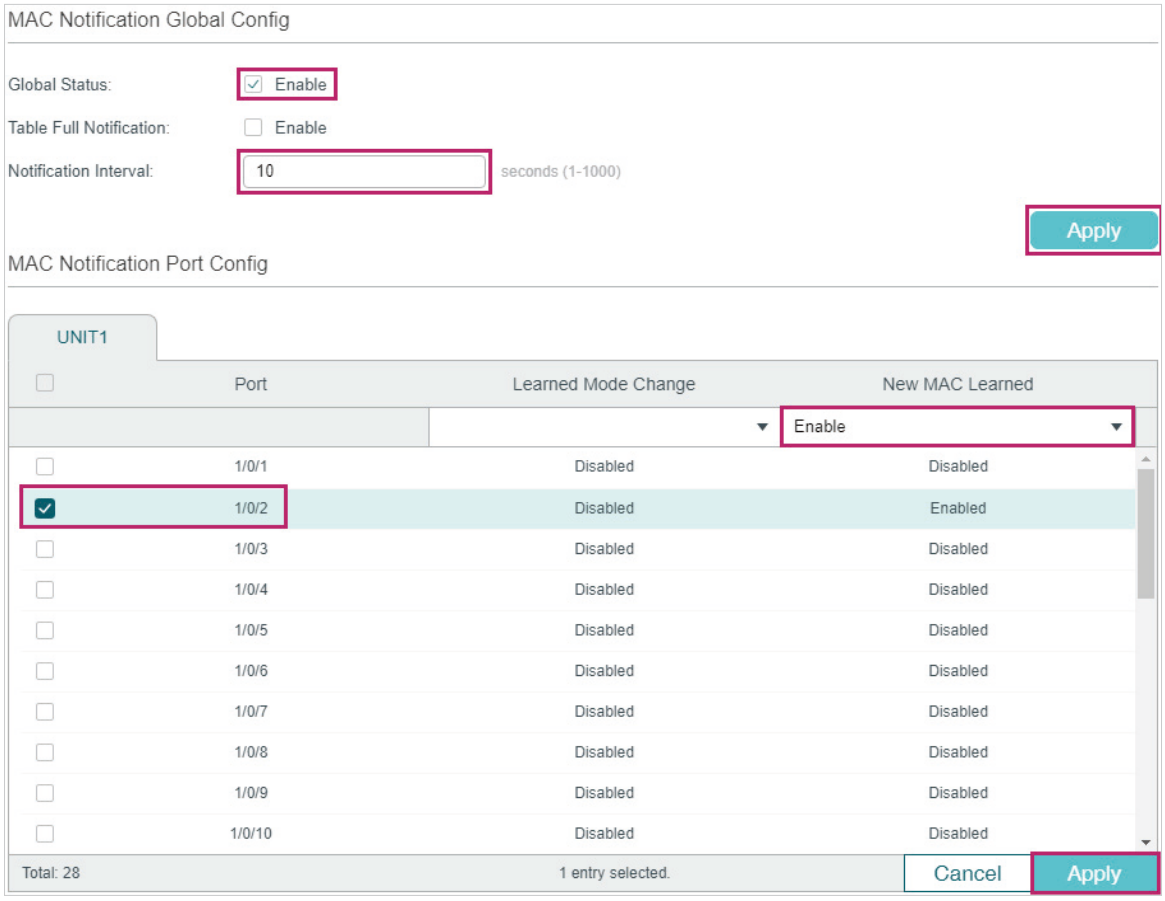
1) Choose the menu **L2 FEATURES > Switching > MAC Address > MAC VLAN Security** and click **Add** to load the following page. Set the maximum number of MAC address in VLAN 10 as 100, choose drop mode and click **Create**.

Figure 4-2 Configuring VLAN Security



2) Choose the menu **L2 FEATURES > Switching > MAC Address > MAC Notification** to load the following page. Enable Global Status, set notification interval as 10 seconds, and click **Apply**. Then, enable new-mac-learned trap on port 1/0/2 and click **Apply**.

Figure 4-3 Configuring New-MAC-learned Traps



3) Click Save to save the settings.

4) Enable SNMP and set a management host. For detailed SNMP configurations, please refer to *Configuring SNMP & RMON.*

4.4 Using the CLI

1) Set the maximum number of MAC address in VLAN 10 as 100, and choose drop mode.

   Switch#configure

   Switch(config)#mac address-table security vid 10 max-learn 100 drop

2) Configure the new-MAC-learned trap on port 1/0/2 and set notification interval as 10 seconds.

   Switch(config)#mac address-table notification global-status enable

   Switch(config)#mac address-table notification interval 10

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

   Switch(config-if)#mac address-table notification new-mac-learned enable

   Switch(config-if)#end

   Switch#copy running-config startup-config

3) Configure SNMP and set a management host. For detailed SNMP configurations, please refer to *Configuring SNMP & RMON.*

Verify the Configurations

Verify the configuration of VLAN Security.

Switch#show mac address-table security vid 10

VlanId	Max-learn	Current-learn	Status
10	100	0	Drop

Verify the configuration of MAC Notification on port 1/0/2.

Switch#show mac address-table notification interface gigabitEthernet 1/0/2

Port	LrnMode Change	New Mac Learned
Gi1/0/2	disable	enable

5 Appendix: Default Parameters

Default settings of the MAC Address Table are listed in the following tables.

Table 5-1 Entries in the MAC Address Table

Parameter	Default Setting
Static Address Entries	None
Dynamic Address Entries	Auto-learning
Filtering Address Entries	None

Table 5-2 Default Settings of Dynamic Address Table

Parameter	Default Setting
Auto Aging	Enable
Aging Time	300 seconds

Table 5-3 Default Settings of MAC Notification

Parameter	Default Setting
Global Status	Disable
Table Full Notification	Disable
Notification Interval	1 Second
Learned Mode Change Notification	Disable
Exceed Max Learned Notification	Disable
New MAC Learned Notification	Disable

Table 5-4 Default Settings of MAC VLAN Security

Parameter	Default Setting
MAC VLAN Security	Disable