Configuring Port Security

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-28PS v3 or above, T1600G-28TS 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 Overview

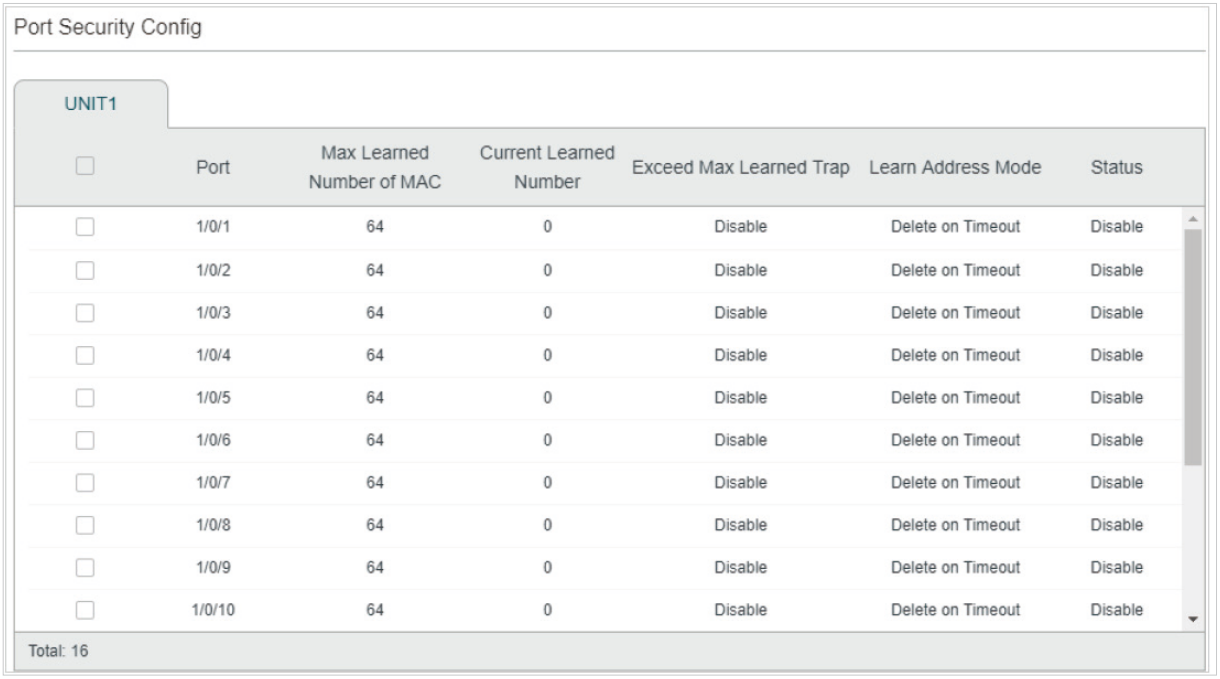
You can use the Port Security feature to limit the number of MAC addresses that can be learned on each port, thus preventing the MAC address table from being exhausted by the attack packets. In addtion, the switch can send a notification if the number of learned MAC addresses on the port exceeds the 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	Disable
Learn Address Mode	Delete on Timeout
Status	Disable