Basic Port Configuration

Contents

Chapter 1 Port Security

1.1 Port Security Description

Port security is usually applied to the access layer to restrict access from hosts. With port security, network access is available only to specified hosts.

The port security function binds the MAC address, IP address, VLAN ID, and port number to deny access of illegitimate users so as to ensure network data security and sufficient bandwidth for authorized users.

Users can restrict the access to a network by applying three kinds of rules: MAC rules, IP rules, MAX rules. The MAC rules are further divided into three binding modes: MAC binding, MAC+IP binding, and MAC+VID binding. The IP rules may apply to a certain IP address or a series of IP addresses. The MAX rules limit the number of MAC addresses that can be sequentially learned by a port, excluding the valid MAC addresses generated by the MAC rules and IP rules. Sticky rules are maintained under a MAX rule. If a port is configured with only a deny rule, the packets except those authorized by the permit rule cannot be forwarded through this port.

The MAC addresses specified by a sticky rule can be learned automatically or configured manually and are saved in a configuration file being executed. If the configuration file is saved before restart of a device, it does not need to be configured after the restart because these MAC address may take effect automatically. When the sticky function is enabled on a port, the MAC addresses dynamically learned by the MAX rules will be added as sticky rules and saved in a configuration file being executed. New MAC addresses can be learned to generate sticky rules until the number of sticky rules reaches the upper limit of a MAX rule.

The MAC and IP rules can determine whether the packets matching a rule are forwarded. The MAC rules allow MAC addresses to be bound with VLANs and IP addresses as required. Port security is based on software and therefore the number of allowed rules is beyond the hardware restraint, which contributes to more flexible configuration.

Port security rules are triggered by ARP packets of terminal devices. When a device receives an ARP packet, port security uses the three kinds of rules (matching sequence: MAC rules, IP rules, and MAX rules) to match the packet and controls the L2 forwarding table of the port based on the matching result, so that packet forwarding at the port is under control.

Invalid packets will be processed in protect, restrict, or shutdown mode. In protect mode, an invalid packet is discarded; in restrict mode, an invalid packet is discarded and a trap alarm is generated two minutes after reception of the packet; in shutdown mode, the port that has received an invalid packet is shut down in addition to the actions taken in restrict mode.

🕮 **Notes:**

If the MAC address or IP address of a host is denied, the host is restricted from accessing the network even if the number of MAC addresses or IP addresses has not reached the upper limit of the MAX rule.

Port security must not be deployed together with 802.1X or MAC authentication.

Port security and anti-ARP flooding are mutually exclusive.

1.1 Port Security Configuration

Table 1- 1 Configuring port security

Operation	Command	Remarks
Enters the global configuration mode.	**configure terminal**	-
Enters the port configuration mode.	**interface ethernet** *device/slot/port*	-
Enables/Disables port security.	**port-security {enable|disable}** Port security is disabled by default.	Mandatory
Configures MAC binding rules for a port.	**port-security {permit|deny mac-address** *mac-address***}** MAC binding is not configured by default.	Optional
Configures MAC+VLAN binding rules for a port.	**port-security {permit|deny mac-address** *mac-address* **vlan-id** *vlanId***}** MAC+VLAN binding is not configured by default.	Optional
Configures MAC+IP binding rules for a port.	**port-security {permit|deny mac-address** *mac-address* **ip-address** *ip-address***}** MAC+IP binding is not configured by default.	Optional
Configures IP rules for a port.	**port-security {permint|deny ip-address** *start-ip-address* **[to** *end-ip-address***]}** IP rules are not configured by default.	Optional
Configures MAX rules for a port.	**port-security maximum {***0-4000***}** The maximum number of rules is 0 by default.	Optional
Enables the sticky function on a port.	**port-security permit mac-address sticky** The sticky function is disabled by default.	Optional
Configures MAC sticky rules for a port.	**port-security permit mac-address sticky {***mac-address***}** MAC sticky rules are not configured by default.	Optional
Configures MAC+VLAN sticky rules for a port.	**port-security permit mac-address sticky {***mac-address***} vlan-id {***vlanId***}** MAC+VLAN sticky rules are not configured by default.	Optional
Configures the address aging time for a port (in the unit of minute).	**port-security aging time {0-1440}** The address aging time is 1 minute by default.	Optional
Enables static address aging on a port.	**port-security aging static** Static address aging is disabled by default.	Optional
Configures the method of handling the invalid packets (the packets matching a deny rule or the packets received after the upper limit of a MAX rule is reached) received by a port.	**port-security violation {protect|restrict|shutdown}** Invalid packets are handled in protect mode by default.	Optional
Configures the function of automatically recovering a port that is	**port-security recovery** This function is disabled by default.	Optional

Operation	Command	Remarks
shut down.		
Configures the time to wait before a port that is shut down recovers.	**port-security recovery time <***value***>** The wait time is 5 minutes by default.	Optional
Deletes the MAC address specified by a port.	**no port-security active-address {all| configured| learned}** **all**: All the MAC addresses are deleted. **configured**: The MAC addresses that are learned after the upper limit of the MAX rule is exceeded are deleted. **learned**: The MAC addresses learned by the MAX rule are deleted.	Optional
Deletes all the port security-related configurations on a port.	**no port-security all**	Optional
Displays port configurations.	**show port-security [interface list]**	Optional
Displays the MAC rule configuration of a port.	**show port-security mac-address [interface list]**	Optional
Displays the IP rule configuration of a port.	**show port-security ip-address [interface list]**	Optional
Displays the currently activated MAC addresses of a port.	**show port-security active-address [configured | learned][interface list]**	Optional
Displays the configuration for automatically recovering a port that has been shut down.	**show port-security recovery [interface list]**	Optional

🕮 **Notes:**

To make the sticky function effective, enable port security and set the upper limit of the MAX rule to a value larger than 0. When the sticky function is enabled, the dynamically learned addresses in the MAX rule will be converted into sticky rules and saved in a configuration file being executed. When the sticky function is disabled, all the learned sticky rules will be deleted.

The number of sticky rules on a port must not exceed the upper limit of the MAX rule.

If a configuration file is saved before restart of a device, the sticky rules that have been saved before the restart will take effect automatically after the restart.

A port that has been shut down can be recovered through either of the following methods:

(1) Run **shutdown** and then **no shutdown** on the port.

(2) Make the port recover automatically after running **shutdown** on the port.

A trap alarm is generated two minutes after the reception of an invalid packet.

1.2 Configuration example

1, open the port security on port 8~10, configure port 8 allows the source MAC address through 00:01:7f:00:22:33 message:

Switch(config)#interface range ethernet 0/0/8 to ethernet 0/0/10

Switch(config-if-range)#port-security enable

Switch(config-if-range)#interface ethernet 0/0/8

Switch(config-if-ethernet-0/0/8)#port-security permit mac-address 00:01:7f:0

0:22:33

2, configure the ports 9 allows the source MAC address is 00:01:7f:44:55:66, VLAN is 3 packets by. Configure port 10 discarded a source MAC address of 00:01:7f:23:56:89, the source IP 192.168.1.88 message:

Switch(config-if-ethernet-0/0/8)#interface ethernet 0/0/9

Switch(config-if-ethernet-0/0/9)#port-security permit mac-address 00:01:7f:4

4:55:66 vlan-id 3

Switch(config-if-ethernet-0/0/9)#interface ethernet 0/0/10

Switch(config-if-ethernet-0/0/10)#port-security deny mac-address 00:01:7f:23

:56:89 ip-address 192.168.1.88

3, on port 8, prohibits communication source IP from all messages between 192.168.1.100 to 192.168.1.200:

Switch(config-if-ethernet-0/0/10)#interface ethernet 0/0/8

Switch(config-if-ethernet-0/0/8)#port-security deny ip-address 192.168.1.100

to 192.168.1.200

4, open the mac+vlan sticky port 9:

Switch(config-if-ethernet-0/0/8)interface ethernet 0/0/9

Switch(config-if-ethernet-0/0/9)#port-security permit mac-address sticky

5,open 10 ports aging function in static address :

Switch(config-if-ethernet-0/0/9)#i e 0/0/10

Switch(config-if-ethernet-0/0/10)#port-security aging static

6, the configuration port 8, 9, 10 Max rules for each 500, aging time is 5 minutes, discard all packet matching configuration rules of deny and send a warning and a shutdown port, shutdown port and 3 minutes after the restart:

Switch(config-if-ethernet-0/0/10)#interface range ethernet 0/0/8 to ethernet

0/0/10

Switch(config-if-range)#port-security maximum 500

Switch(config-if-range)#port-security aging time 5

Switch(config-if-range)#port-security violation shutdown

Switch(config-if-range)#port-security recovery

Switch(config-if-range)#port-security recovery time 3

Switch(config-if-range)#exit

Switch(config)#show port-security interface ethernet 0/0/8 to 0/0/10

tips: ViMode(violation mode) AT(AgingTime) AS(AgingStatic) ST(shutdown)

Port Status MaxNum UserNum ViMode AT(min) AS Sticky ST

e0/0/8	enable	500	0	shutdown	5	disable	disable	FALSE
e0/0/9	enable	500	0	shutdown	5	disable	enable	FALSE
e0/0/10	enable	500	0	shutdown	5	enable	disable	FALSE

Total entries: 3

7, after the completion of configuration display the corresponding configuration information.

Switch(config)#show port-security ip-address

Configuration of rules:

Port	Action	Start ipaddress	End ipaddress
e0/0/8	deny	192.168.1.100	192.168.1.200

Total entries: 1

Switch(config)#show port-security mac-address

Configuration of rules:

Port	Action	Mac address	VID	IP Addr	ConfigType
e0/0/8	permit	00:01:7f:00:22:33	N/A	N/A	MAC
e0/0/9	permit	00:01:7f:44:55:66	3	N/A	MAC+VLAN
e0/0/10	deny	00:01:7f:23:56:89	N/A	192.168.1.88	MAC+IP

Total entries: 3

Switch(config)#show port-security recovery interface ethernet 0/0/8

to 0/0/10

Auto recovery configurations:

Port	Auto recovery	Time(min)
e0/0/8	enable	3
e0/0/9	enable	3
e0/0/10	enable	3

Total entries: 3

Switch(config)#show running-config interface ethernet 0/0/8

Building configuration...

![ethernet 0/0/8]

port-security enable

port-security maximum 500

port-security aging time 5

port-security violation shutdown

port-security recovery

port-security recovery time 3

port-security permit mac-address 00:01:7f:00:22:33

port-security deny ip-address 192.168.1.100 to 192.168.1.200

```
end
Switch(config)#show running-config interface ethernet 0/0/9
Building configuration...
![ethernet 0/0/9]
port-security enable
port-security maximum 500
port-security aging time 5
port-security permit mac-address sticky
port-security violation shutdown
port-security recovery
port-security recovery time 3
port-security permit mac-address 00:01:7f:44:55:66 vlan-id 3
end
Switch(config)#show running-config interface ethernet 0/0/10
Building configuration...
![ethernet 0/0/10]
port-security enable
port-security maximum 500
port-security aging static
port-security aging time 5
port-security violation shutdown
port-security recovery
port-security recovery time 3
port-security deny mac-address 00:01:7f:23:56:89 ip-address 192.168.1.88
end
```