FSOS

Port Security Configuration

Contents

1. Port Security Configuration

1.1 Port Security Overview

Port security is generally applied at the access layer. It can restrict host to access to the network through the device, and allow certain hosts to access the network, while other hosts cannot access the network.

The port security function binds the user's MAC address, IP address, VLAN ID, and PORT number flexibly, and prevents illegal users from accessing the network. This ensures the security of network data and the legal users can obtain sufficient bandwidth.

Users can restrict the hosts that can access the network through three rules: MAC rule, IP rule, and MAX rule. MAC rules are divided into three binding methods: MAC binding, MAC + IP binding, MAC + VID binding; the MAX rule defines the maximum number of MAC addresses that can be learned on a port. This address does not include the number of MAC rules and IP rules generated by the legitimate MAC address. In the MAX rule, there are sticky rules. If the deny rule is only configured on the port and the MAX rule is not configured, the other messages cannot be forwarded (Exception by allowing rule checking).

The MAC address of the Sticky rule can be learned automatically, and configured manually and saved in the running configuration file. If the configuration file is saved before the device reboots, the device does not need to be configured again after the device reboots, and these MAC addresses take effect automatically. When the sticky function is enabled on the port, the dynamic MAC address learned by the MAX rule is added to the sticky rule and saved to the running configuration file. In the case of the MAX rule is not full, it is allowed to continue learning the new MAC address and form the sticky rule until the number of sticky rules reaches the maximum configured by MAX.

MAC rules and IP rules can specify whether messages matching the corresponding rules are allowed to communicate. The user's MAC address and VLAN, MAC address and IP address can be bound flexibly by the MAC rule. Because port security is software-based, the number of rules is not limited by hardware resources, make the configuration more flexible.

The rules of port security are triggered by the ARP messages of the terminal device. When the device receives an ARP message, port security extracts various messages information, and match with the three rules of the configuration. The order of match is MAC address, IP address and MAC rule. The Layer 2 forwarding table of the port is controlled by the matching result, in order to control the forwarding behavior of the port.

When the port security judgment message is illegal, messages are processed accordingly. There are three modes: protect, restrict and shutdown. Protect mode discards messages. The restrict mode discards messages and trap alarms (Receive an illegal message in two minutes of the alarm). Shutdown mode will shut down port in addition to restrict mode of action.

1.2 Port Security Configuration

Configure port security

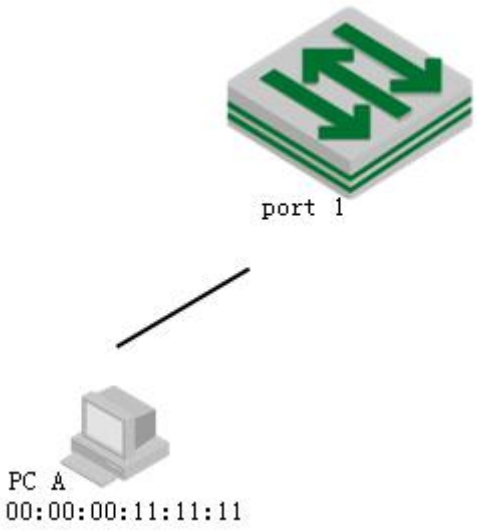
operation	command	remark
Enter the port configuration mode	interface ethernet *port-number*	required
Enable/disable port security	port-security { enable | disable }	required
Configure MAC binding rule	[no] port-security { permit | deny } mac-address ***mac-address*** **{** **[** vlan-id ***vlan-id***] | ip-address ***ip-address*** }	optional
Configure IP rules	[no] port-security { permit | deny } ip-address ***start-ip*** [to ***end-ip***]	optional
Configure MAX rules	[no] port-security maximum ***value***	optional
Enable STICKY	[no] port-security permit mac-address sticky	optional
Configure MAC STICKY rules	[no] port-security permit mac-address sticky ***mac-address*** **[** vlan-id ***vlan-id***]	optional
Configure the address aging time	[no] port-security aging time ***value***	optional
Enable static address aging function	[no] port-security aging static	optional
Configure the policy for receiving invalid message	port-security violation { protect | restrict | shutdown	optional
Enable shutdown automatic recovery	[no] port-security recovery	optional
Configure the automatic recovery time after shutdown	[no] port-security recovery time ***value***	optional
Delete the currently active MAC address	no port-security active-address {all | configured | learned }	optional
Delete all the port security related configurations	no port-security all	optional
Display the security configuration	show port-security [interface list]	optional
Display the MAC rule configuration	show port-security mac-address [interface ethernet *port-number*]	optional
Display the IP rule configuration	show port-security ip-address [interface ethernet *port-number*]	optional
Display the currently active MAC address	show port-security active-address [configured | learned | interface ethernet *port-number*]	optional
Display the configuration of automatic recovery after shutdown	show port-security recovery [interface ethernet ***port-number***]	optional

Note:

1. After the port-security function is enabled, deny all messages by default. Therefore, user must configure one of the mac\ip\max rules.
2. If the sticky function is effective, it is necessary that the port security is enabled, and the number of MAX rule isn't configured for 0. When this function is turned on, the dynamic addresses learned in the previous MAX rule are converted to STICKY rules and stored in the run file. When the function is disabled, the learned STICKY rules are deleted. The number of STICKY rule entries of a port cannot exceed the configured number of MAX rules. If the configuration file is saved before the device reboots, the STICKY rule saved before the port reboots will take effect.
When the port is shutdown, there are two ways to recovery: (1) configure the port for shutdown and no shutdown. (2) Automatic recovery after configuring shutdown.
4. When illegal message is received, trap alarms do not take effect immediately. Traps are generated within two minutes.
5. If a MAC address or ip address is denied, through the upper limit of MAX doesn't reach, the host can't communication.
6. Port security cannot be enabled together with 802.1X or mac authentication.
7. Port security cannot be enabled together with anti-ARP flooding.

1.3 Port Security Configuration Example

I. Network requirements
Configure port 1 to allow only pc A communication;



Port security diagram

2. Configuration procedure
Configure port security
DUT(config)#interface ethernet 0/0/1
DUT(config-if-ethernet-0/0/1)#port-security enable
DUT(config-if-ethernet-0/0/1)#port-security permit mac-address 00:00:00:11:11:11

3. Verify results

(1) Using ixia emulation PC A, configure two network cards, all through DHCP to obtain IP, configure dhcp-snooping (configuration slightly) on the DUT, access to IP as follows:

```
DUT(config)#show dhcp-snooping clients
DHCP client information:
d - days, h - hours, m - minutes, s - seconds
IPAddress          mac                  vlan   port      LeaseTime       ExceedTime
192.168.1.100      00:00:00:11:11:11    1      e0/0/1    1d0h0m0s        23h51m21s
192.168.1.101      00:00:00:54:20:71    1      e0/0/1    1d0h0m0s        23h55m37s
Total entries: 2. Printed entries: 2.
```

2) Use the DUT to ping the two clients separately, obtain the ARP entry, and enable the DUT to establish the port security activation table.

```
DUT(config)#show dhcp-snooping clients
DHCP client information:
d - days, h - hours, m - minutes, s - seconds
IPAddress          mac                  vlan   port      LeaseTime       ExceedTime
192.168.1.100      00:00:00:11:11:11    1      e0/0/1    1d0h0m0s        23h51m21s
192.168.1.101      00:00:00:54:20:71    1      e0/0/1    1d0h0m0s        23h55m37s
Total entries: 2. Printed entries: 2.
```

Display the currently active MAC addresses. Only the permit mac rule entries are displayed

```
DUT(config)#show port-security active-address
   Acitve mac-address:
      Port          MAC address              VID        IP Addr              Derivation     Action
Age(min)
      E1/0/1    00:00:00:11:11:11     1      192.168.1.100          MAC            permit    1
   Total entries:    1
DUT(config)#debug port-security
DUT(config)#logging monitor 0
```

(3) Try to communicate with the DUT using two PCs, respectively: The results are as follows

Use the ip = 192.168.1.100 (mac = 00: 00: 00: 11: 11: 11 match port-security rule) to ping the DUT. It can communicate, log is as follows:

```
00:29:48: DUT: %PORT-SECURITY-7-debug: port e0/0/1 recv packet mac[00:00:00:11:11:11]
vlan [1] type[0x0806]
00:29:48: DUT: %PORT-SECURITY-7-debug: match with MAC RULE
00:29:48: DUT: %PORT-SECURITY-7-debug: action: PERMIT
```

Use the ip = 192.168.1.101 (mac = 00: 00: 00: 54: 20: 71 match port-security rule) to ping the DUT. It can communicate, log is as follows:

```
00:30:07: DUT: %PORT-SECURITY-7-debug: port e0/0/1 recv packet mac[00:00:00:54:20:71]
vlan [1] type[0x0806]
00:30:07: DUT: %PORT-SECURITY-7-debug: match with MAX RULE
00:30:07: DUT: %PORT-SECURITY-7-debug: port e0/0/1 maxnum exceed
```

Maxnum rule by default is 0, so exceed, the message is discarded;