Port Security Configuration

Port security function limits the number of MAC addresses that can access the switch port, preventing illegal users from communicating with the network through the switch interface, thus enhancing the security of network resources.

The dynamic MAC address learned by the secure interface is converted into secure MAC address, and the maximum number of secure MAC addresses is allowed to be configured. When the number of learned MAC addresses exceeds the MAC limit, a violation action is triggered to protect the system, which can be configured by the user to shut down the port or discard packets with new source MAC addresses.

NOTE:

When configuring port security, follow the guidelines and restrictions described below:

- By enabling the port security function, the dynamic MAC address table entries learned previously on the secure interface will be deleted automatically and the static MAC address table entry configured previously will be prompted to manually delete.
- Port security and static MAC configurations on the same interface are mutually exclusive.
- Port security does not support to configure on a LAG interface.
- Make sure MAC learning is enabled before enabling port security on the same interface. (By default, MAC learning is enabled.)
- Executing the command "**run clear MAC address table all**" will clear only the dynamic secure MAC addresses, but not clear static secure MAC and sticky secure MAC.
- When the secure port goes Down and Up, the system clears only dynamic secure MAC, but not clear static secure MAC and sticky secure MAC.
- A secure interface can learn only one secure MAC address by default. Set the maximum number of secure MAC addresses according to the actual networking requirement.
- For dynamic security MACs, you can move them to any other port; however, for sticky security MACs, learning on any other port is not supported unless statically configured.
- The new learned MAC addresses will temporarily occupy the system MAC address table resources when it reaches the MAC limit. In this case, if the interface still learns a large number of MAC addresses, it may cause the device to temporarily fail to learn the new MAC address.

Enabling Port Security

When port security is enabled, the dynamic MAC address table entries learned previously on the secure interface will be deleted automatically and the static MAC address table entry configured previously will be prompted to manually delete.

After port security is enabled, the dynamic MAC addresses learned on the secure interface will be changed to a dynamic secure MAC address.

When port security is disabled, all the secure MAC addresses on the interface will be deleted, and the port will need to re-learn the MAC address on the port.

The following example enables port security on interface ge-1/1/1.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security
admin@XorPlus# commit
Commit OK.
Save done.
```

Three Types of Secure MAC

There are three types of secure MAC address on a secure port: Dynamic Secure MAC, Static Secure MAC and Sticky Secure MAC.

1. Dynamic Secure MAC

Dynamic secure MAC is the MAC address dynamically learned on the secure port.

When the secure port goes Down and Up, or device reboots/restarts, the dynamic secure MAC addresses are lost and needs to be re-learned.

Dynamic secure MAC addresses will be aged out by the following MAC aging time CLI command.

```
admin@XorPlus# set interface ethernet-switching-options mac-table-aging-time 100
admin@XorPlus# commit
Commit OK.
Save done.
```

2. Static Secure MAC

Static secure MAC addresses are configured by the user with the following CLI command.

The configuration will not be lost when the switch is rebooted/restarted, or port goes down and up.

Static secure MAC addresses do not age.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:23 vlan 1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:24 vlan 1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:25 vlan 1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:26 vlan 1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:27 vlan 1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ----------------- ------- ----------
1 00:00:23:23:23:23 static ge-1/1/1
1 00:00:23:23:23:24 static ge-1/1/1
1 00:00:23:23:23:25 static ge-1/1/1
1 00:00:23:23:23:26 static ge-1/1/1
1 00:00:23:23:23:27 static ge-1/1/1
-----------------------------------------------------
MAC age time :300s
```

3. Sticky Secure MAC

When sticky function is enabled on the secure port, the system changes the dynamic secure MAC to sticky secure MAC.

Port security with sticky MAC addresses retains dynamically learned MAC addresses when the port goes down and restores the MAC addresses when the link is up.

Sticky secure MAC addresses also do not age.

NOTE:

- After a device reboots/restarts, sticky secure MAC addresses are lost and need to be re-learned.
- Disabling the sticky function converts the sticky secure MAC addresses on the current interface to dynamic secure MAC addresses.

For example, enable sticky function on secure port ge-1/1/1.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security sticky true
admin@XorPlus# commit
Merging the configuration.
Commit OK.
Save done.
admin@XorPlus#
```

In **run show port-security address**, the MAC type of the sticky secure MAC is displayed as sticky; however, in **run show MAC address table**, the MAC type of the sticky secure MAC is displayed as static.

For example,

```
admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ----------------- ------- ----------
1 00:00:11:11:11:11 sticky ge-1/1/1
1 00:00:23:23:23:25 static ge-1/1/1
-----------------------------------------------------
MAC age time :300s

admin@Xorplus# run show mac-address table
Total entries in switching table:   2
Static entries in switching table:  2
Dynamic entries in switching table: 0

VLAN   MAC address    Type      Age    Interfaces      User
----      -----------------    ---------    ----    ----------------   ----------
1        00:00:11:11:11:11 static      300    ge-1/1/1       xorp
1        00:00:23:23:23:25 static      300    ge-1/1/1       xorp
```

Configuring the Maximum Number of Secure MACs

The MAC limit number is used to limit the number of secure MACs on the interface, including the number of dynamic secure MAC and manually configured secure static MAC. If sticky is enabled, MAC limit includes sticky secure MAC and secure static MAC.

A secure interface can learn only one secure MAC address by default. Set the maximum number of secure MAC addresses according to the actual networking requirement.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-limit 5
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ----------------- ------- ----------
1 00:00:11:11:11:11 dynamic ge-1/1/1
1 00:00:11:11:11:12 dynamic ge-1/1/1
1 00:00:11:11:11:13 dynamic ge-1/1/1
1 00:00:11:11:11:14 dynamic ge-1/1/1
1 00:00:11:11:11:15 dynamic ge-1/1/1
-----------------------------------------------------
MAC age time :300s
```

Configuring Port Security Violation Mode on a Port

Violation mode can be configured for the system to take a protective action when the number of learned MAC addresses exceeds the MAC limit on the secure port, as one of the following four:

- **protect**: Discards packets with new source MAC addresses when the number of learned MAC addresses exceeds the limit. This is the default value.
- **restrict**: Discards packets with new source MAC addresses and generates a warning syslog message when the number of learned MAC addresses exceeds the limit.
- **shutdown**: Shuts the interface down, sets the interface status toerror-discard and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. User can recover the port with the **run clear port-security port-error** command.

- **shutdown-temp**: Shuts the interface down temporarily, sets the interface status to error-discard and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. After 20 seconds (default), the interface comes up. The **set interface ethernet-switching-options port-error-discard timeout** command configures the port recovery interval when the port security violation mode is configured to **shutdown-temp**.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/33 port-security violation ?
Possible completions:
  protect                     Drop packets with unknown source addresses
  restrict                     Drop packets with unknown source addresses and log violation
  shutdown                   Disable interface
  shutdown-temp              Disable interface temporarily (20 seconds by default)

admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security violation restrict
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring Port Security Auto-recovery Time

When the port security violation mode is configured to shutdown-temp, user can configure the recovery interval with the command below.

```
admin@XorPlus# set interface ethernet-switching-options port-error-discard timeout 30
admin@XorPlus# commit
Commit OK.
Save done.
```

Recovering the Port in Error-discard

When the port security violation mode is configured to **shutdown**, the port will be set to error-discard state after detecting a violation. User can recover the port with the following command.

```
admin@Xorplus# run show interface gigabit-ethernet ge-1/1/23
Physical interface: ge-1/1/23, Enabled, error-discard True(Port Security), Physical link is Down
Interface index: 23, Mac Learning Enabled
Description:
Link-level type: Ethernet, MTU: 1518, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled
Auto-negotiation: Enabled, Advertised speed modes: 10M,100M,1G
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Interface burst limit ingress:unlimited, egress:unlimited
Precision Time Protocol mode:none
Current address: 20:04:0f:01:63:4a, Hardware address: 20:04:0f:01:63:4a
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 0 bits/sec, 0 packets/sec
  Input Packets.............................42
  Output Packets............................31
  Input Octets..............................4781
  Output Octets.............................4545

admin@XorPlus# run clear port-security port-error interface gigabit-ethernet ge-1/1/33
Clear done.
```

Configuring Port Security Block Mode

Port security can be configured to take one of five block actions:

- **all**: Discards all the packets in egress direction of the port.
- **broadcast**: Discards only the broadcast packets in egress direction of the port.
- **multicast**: Discards only the multicast packets in egress direction of the port.
- **uni-multi-cast**: Discards both the unknown unicast packets and multicast packets in egress direction of the port.
- **unicast**: Discards only the unknown unicast packets in egress direction of the port.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/33 port-security block ?
Possible completions:
  all                           Block broadcast and unknown addresses
  broadcast                     Block broadcast address
  multicast                     Block unknown multicast addresses
  uni-multi-cast                Block unknown uni/multi cast addresses
  unicast                       Block unknown unicast addresses

admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security block broadcast
admin@XorPlus# commit
Commit OK.
Save done.
```

Displaying Port Security Settings

To display port security settings, enter this command:

```
admin@Xorplus# run show port-security brief
Secure Port    MaxMacLimit    CurrentAddr    ViolationCount    Action
-------------------------------------------------------------------------------------------------------------------
ge-1/1/22      2              0              0                 restrict
ge-1/1/23      1              0              0                 shutdown-temp
ge-1/1/34      1              0              0                 protect

admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ----------------- ------- ----------
1 00:00:11:11:11:11 dynamic ge-1/1/1
1 00:00:23:23:23:26 static ge-1/1/1
1 00:00:23:23:23:27 static ge-1/1/1
-----------------------------------------------------
MAC age time :100s

admin@Xorplus# run show port-security interface
Interface ge-1/1/22
---------------------------------------
Port Security               : enabled
Violation action            : restrict
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 2
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0

Interface ge-1/1/23
---------------------------------------
Port Security               : enabled
Violation action            : shutdown-temp
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 1
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0
```

Disabling Port Security

To disable port security, enter this command:

```
admin@XorPlus# delete interface gigabit-ethernet ge-1/1/1 port-security
Deleting:
port-security {
mac-limit: 5
violation: "restrict"
mac-address 00:00:23:23:23:23 {
vlan 1 {
}
}
mac-address 00:00:23:23:23:24 {
vlan 1 {
}
}
mac-address 00:00:23:23:23:25 {
vlan 1 {
}
}
mac-address 00:00:23:23:23:26 {
vlan 1 {
}
}
mac-address 00:00:23:23:23:27 {
vlan 1 {
}
}
sticky: true
block: "broadcast"
}
OK
admin@XorPlus# commit
Commit OK.
Save done.
```