Contents

1 Configuring Port Security

1.1 Introduction

1.1.1 Overview

Port security is used to control packets entering a device port based on the source Media Access Control (MAC) address in the packets.

You can configure static MAC addresses or the maximum number of dynamically learned MAC addresses on a port to control packets entering the port.

Ports configured with port security are called secure ports.

1.1.2 Principles

1. Basic Concepts

- Secure port

  Ports configured with port security are called secure ports.

- Secure address and maximum number of secure addresses

  Addresses bound to secure ports are called secure addresses. Secure addresses can be layer 2 (L2) addresses, namely, MAC addresses, or layer 3 (L3) addresses, namely, IP addresses or IP addresses and MAC addresses.

  The maximum number of secure addresses is the sum of statically configured secure addresses and dynamically learned secure addresses. When the number of secure addresses for a secure port does not reach the maximum number, the secure port can dynamically learn new secure addresses. When the number of secure addresses for the secure port reaches the maximum number, the secure port will not learn dynamic secure addresses any longer. If a new user host accesses the secure port after the number of secure addresses reaches the maximum number, a security violation event occurs.

- Dynamic binding

  The device automatically learns addresses and converts learned addresses into secure addresses.

- Static binding

  You can manually configure secure addresses.

2. Port Security and Security Violation

After port security is enabled on a port, user packets that access the network through the port will be controlled.

The security module of the device will check the source MAC addresses of received packets. Only packets from addresses in the secure address list will be forwarded, and other packets will be discarded.

When the number of MAC addresses learned by a port exceeds the maximum number of secure addresses, a security violation event is triggered. You can configure the following modes for handling security violation events:

- **protect**: When security violation occurs, the corresponding secure port stops learning MAC addresses and discards all packets of newly accessed users. This is the default violation handling mode.
- **restrict**: When security violation occurs, a port violation trap notification will be sent in addition to the behavior in **protect** mode.
- **shutdown**: When security violation occurs, the port will be disabled in addition to the behavior in **protect** mode.

If the number of user hosts connected to a port is less than the maximum number of secure addresses after a security violation event occurs, the port is restored to the non-violation state.

1.2 Restrictions and Guidelines

When port security is configured together with other access control functions, such as 802.1x and IP source guard, packets can enter a port only after the packets pass through all security check rules. If a security channel or global IP-MAC address binding is configured on a port, packets that meet the security channel or global IP-MAC address binding conditions will be exempted from port security check.

1.3 Configuration Task Summary

Port security configuration includes the following tasks:

(1) Configuring Secure Ports

(2) (Optional) Configuring Secure Address Management

(3) (Optional) Configuring Static Secure Addresses

(4) (Optional) Configuring Secure Address Binding

(5) (Optional) Enabling Binding Log Filtering

1.4 Configuring Secure Ports

1.4.1 Overview

After port security is enabled on a port, you can configure the method for handling packets that violate port security requirements.

1.4.2 Restrictions and Guidelines

- The port security function can be configured only on switching ports and L2 aggregation ports (APs).
- Switch Port Analyzer (SPAN) destination ports cannot be configured as secure ports.
- The port security function cannot be configured for Dynamic Host Configuration Protocol (DHCP) Snooping trusted ports.
- The port security function cannot be configured for excluded ports of global IP-MAC address binding.
- **protect** indicates that the device discards packets that do not match the security address. **restrict** indicates that the device discards packets that do not match the security address and sends a trap notification. **shutdown** indicates that the device discards packets that do not match the security address and disables the port.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable port security.

switchport port-security

The port security function is disabled by default.

(5) (Optional) Configure the method for handling packets that violate port security requirements.

switchport port-security violation { **protect** | **restrict** | **shutdown** }

Packets that do not match the security address are discarded by default.

1.5 Configuring Secure Address Management

1.5.1 Overview

1. Maximum Number of Secure Addresses

The number of secure addresses is the sum of statically configured secure addresses and dynamically learned secure addresses. When the number of MAC addresses learned by a port exceeds the maximum number of secure addresses, a security violation event is triggered.

If you set the maximum number of secure addresses for a port to **1** and configure a secure address for this port, the workstation (whose address is the configured secure address) connected to this port will exclusively use all bandwidth of the port.

The maximum number of secure addresses takes effect only to secure addresses and is invalid to security bindings.

By configuring the maximum number of secure addresses and secure address aging time, the device can automatically add and delete secure addresses on a port.

2. Secure Address Aging

After the secure address aging time is configured, an aging timer is triggered to regularly query and delete secure addresses whose aging time expires. By configuring the maximum number of secure addresses and secure address aging time, the device can automatically add and delete secure addresses on a port.

The **switchport port-security aging time** *aging-time* command is used to configure the secure address aging time, in minutes. The value range is from 0 to 1440. The default secure address aging time is **0**, which indicates that secure addresses never age. If a non-zero value is configured, the device regularly queries and deletes secure addresses based on the configured time. When a non-zero aging time is configured, only dynamically learned addresses are aged by default. If the **switchport port-security aging static** command is configured, statically configured and dynamically learned secure addresses are aged.

3. Sticky MAC Address

Sticky MAC addresses are special MAC addresses not affected by the aging mechanism. No matter whether dynamic or static aging is configured, sticky MAC addresses will not be aged.

If dynamically learned secure addresses are saved as static sticky MAC addresses, these addresses will not age. After the configurations are saved, these addresses do not need to be learned again upon a restart. If this function is not enabled, these addresses must be learned again after a device restart.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum number of secure addresses for a port.

switchport port-security maximum *number*

The default maximum number of secure addresses for a port is **128**.

(5) Configure the secure address aging time and its application scope on a port.

switchport port-security aging { **static** | **time** *aging-time* }

The secure address aging time is **0** (that is, not aged), and the aging time applies only to dynamically learned addresses by default.

(6) Enable sticky MAC address learning and configure sticky MAC addresses.

switchport port-security mac-address sticky [*mac-address* [**vlan** *vlan-id*]]

Sticky MAC address learning is disabled by default.

1.6 Configuring Static Secure Addresses

1.6.1 Overview

After static secure addresses are configured on a secure port, only specified users can use this port. The secure addresses are periodically updated to ensure network security.

1.6.2 Restrictions and Guidelines

- The maximum number of secure addresses configured by running the **switchport port-security maximum** *number* command takes effect only to secure addresses, and the number of security bindings is not limited.
- If security binding and a static secure MAC address are configured, the static secure MAC address must be the same as the MAC address in the IP-MAC address binding. Otherwise, communication may fail due to inconsistency with the binding. Similarly, if only IP address binding is configured, only packets whose secure MAC addresses are statically configured or dynamically learned and whose source IP address is the bound IP address can enter the device.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure static secure addresses for a port. Please configure only one task.

- Configure static secure addresses for a port in global configuration mode.

  switchport port-security interface *interface-type interface-number* **mac-address** *mac-address* [**vlan** *vlan-id*]

  No static secure address is configured for a port by default.

- Enter the interface configuration mode of the port and configure static secure addresses.

  interface *interface-type interface-number*

  switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]

  No static secure address is configured for a port by default.

1.7 Configuring Secure Address Binding

1.7.1 Overview

When security binding (IP address binding or IP-MAC address binding) is configured, IP packets are first checked for secure addresses (including statically configured and dynamically learned secure addresses). If secure address check fails, the IP packets are discarded. If secure address check is successful, the bound IP address is checked. If IP address check is successful, the data packets are forwarded. Otherwise, the packets are discarded.

1.7.2 Restrictions and Guidelines

- The maximum number of secure addresses configured by running the **switchport port-security maximum** *number* command takes effect only to secure addresses, and the number of security bindings is not limited.
- If security binding and a static secure MAC address are configured, the static secure MAC address must be the same as the MAC address in IP-MAC address binding. Otherwise, communication may fail due to inconsistency with the binding. Similarly, if only IP address binding is configured, only packets whose secure MAC addresses are statically configured or dynamically learned and whose source IP address is the bound IP address can enter the device.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure security bindings. Please configure only one task.

- Configure security bindings for a port in global configuration mode.

switchport port-security interface *interface-type interface-number* **binding** [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

No security binding is configured by default.

- Enter the interface configuration mode of the port to be bound and configure security binding.

  interface *interface-type interface-number*

  switchport port-security binding [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

  No secure address is bound to a port by default.

1.8 Enabling Binding Log Filtering

1.8.1 Overview

After the binding log filtering function is enabled, the device prints alert logs if received IP packets do not match the bound IP and MAC addresses or the bound IP address for port security.

When the binding log printing rate exceeds the configured rate, the number of suppressed logs will be displayed.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enable binding log filtering.

switchport port-security binding-filter logging [**rate-limit** *rate*]

Address binding log filtering is disabled by default.

1.9 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show port-security	Displays all port security configurations.
show port-security all	Displays all effective secure addresses and secure address bindings on a port.
show port-security address [**interface** *interface-type interface-number*]	Displays secure addresses of all ports or a specified port.
show port-security binding [**interface** *interface-type interface-number*]	Displays secure address bindings of all ports or a specified port.
show port-security interface *interface-*	Displays port security configurations of a specified port.

Command	Purpose
type interface-number	

1.10 Common Errors

- Port security is enabled on a SPAN port.
- Port security is enabled on a DHCP trusted port.
- The configured maximum number of secure addresses is smaller than the current number of secure addresses.