1 Port Security Commands

Command	Function
switchport port-security	Enable the port security function.
switchport port-security aging	Configure the secure address aging time and its application scope on a port.
switchport port-security binding	Configure the secure addresses bound to a port.
switchport port-security binding-filter logging	Enable address binding log filtering and configure the log printing rate.
switchport port-security interface binding	Configure security binding for a port.
switchport port-security mac-address	Configure static secure addresses.
switchport port-security interface mac-address	Configure static secure addresses.
switchport port-security maximum	Configure the maximum number of secure addresses for a port.
switchport port-security mac-address sticky	Enable sticky MAC address learning and configure sticky MAC addresses.
switchport port-security violation	Configure the method for handling packets that violate the port security requirements.
show port-security	Display port security configurations and secure addresses.

1.1 switchport port-security

Function

Run the **switchport port-security** command to enable the port security function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The port security function is disabled by default.

Syntax

switchport port-security

no switchport port-security

default switchport port-security

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The port security function strictly controls Media Access Control (MAC) addresses and IP addresses (optional) that can access a port.

The port security function can be configured only on switching ports and layer 2 (L2) aggregation ports (APs). Ports configured with port security are called secure ports. If a secure address is configured for a secure port, the secure port allows only packets whose source address is the configured secure address to pass through. Other packets are discarded.

Examples

The following example enables port security on Gigabitethernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 switchport port-security aging

Function

Run the **switchport port-security aging** command to configure the secure address aging time and its application scope on a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

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

Syntax

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

no switchport port-security aging { **static** | **time** }

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

Parameter Description

static: Applies the configured aging time to manually configured and dynamically learned addresses.

time *aging-time*: Configures the aging time of all secure addresses on a port, in minutes. The value range is from 0 to 1440. When the aging time is set to **0**, secure addresses on a port will not be aged.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command together with the **switchport port-security maximum** command for configuring the maximum number of secure addresses allow the device to automatically add and delete secure addresses on a port.

When the **no switchport port-security aging time** command is run to restore the secure address aging time on a port to **0**, secure address aging is disabled on the port. The **no switchport port-security aging static** command allows the aging time to be applied only to dynamically learned secure addresses.

When port security and 802.1x authentication are both enabled but the secure address has aged, 802.1x users must re-initiate authentication requests to continue the communication.

Examples

The following example sets the aging time of secure addresses on GigabitEthernet 0/1 to 8 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# switchport port-security aging time 8
Hostname(config-if)# switchport port-security aging static
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **switchport port-security maximum**

1.3 switchport port-security binding

Function

Run the **switchport port-security binding** command to configure the secure addresses bound to a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No secure address is bound to a port by default.

Syntax

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

no switchport port-security binding [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

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

Parameter Description

mac-address: Source MAC address to be bound to a port, VLAN ID, and IP address.

vlan *vlan-id*: Specifies the virtual local area network (VLAN) ID to be bound to a port, source MAC address, and IP address. The value range is from 1 to 4094.

ipv4-address: IPv4 address to be bound to a port.

ipv6-address: IPv6 address to be bound to a port.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You must first enter the interface configuration mode of the port to be bound and then run this command to bind the port with the source MAC address (optional), VLAN ID (optional), and IP address. Only packets match the security binding can enter the device, and other packets will be discarded.

Packets that comply with IP-MAC address binding or IP address binding for port security can be forwarded only when their source MAC address is the secure address bound to the port.

Before dynamically learned secure addresses are added to the secure address table, packets that comply with IP-MAC address binding or IP address binding for port security cannot be forwarded.

Static secure addresses can access the Internet without authentication. If authorization exists, only static secure addresses that comply with the authorization binding can access the Internet.

Examples

The following example binds IPv4 address 192.168.1.100 to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security binding
192.168.1.100
```

The following example binds IPv4 address 192.168.1.100, MAC address 00d0.f800.5555, and VLAN 1 to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security binding
00d0.f800.5555 vlan 1 192.168.1.100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 switchport port-security binding-filter logging

Function

Run the **switchport port-security binding-filter logging** command to enable address binding log filtering and configure the log printing rate.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Address binding log filtering is disabled by default.

Syntax

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

no switchport port-security binding-filter logging

default switchport port-security binding-filter logging

Parameter Description

rate-limit *rate*: Configures the rate for printing security binding logs, in pieces per second. The value range is from 1 to 120. The default value is **10**. If this parameter is not specified, address binding log filtering is enabled.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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.

Examples

The following example enables the binding log filtering function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switchport port-security binding-filter logging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 switchport port-security interface binding

Function

Run the **switchport port-security interface binding** command to configure security binding for a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No security binding is configured by default.

Syntax

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

no switchport port-security interface *interface-type interface-number* **binding** [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

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

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number of the bound port.

mac-address: Bound source MAC address.

vlan *vlan-id*: Specifies the VLAN bound to the source MAC address.

ipv4-address: Bound IPv4 address.

ipv6-address: Bound IPv6 address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to bind a port with a source MAC address (optional), VLAN ID (optional), and IP address as the security binding of the port. Only packets match the security binding can enter the device, and other packets will be discarded.

Unlike the **switchport port-security binding** [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* } command, this command can be directly configured in global configuration mode without needing to enter the interface configuration mode of the bound port.

Packets that comply with IP-MAC address binding or IP address binding for port security can be forwarded only when their source MAC address is the secure address bound to the port.

Before dynamically learned secure addresses are added to the secure address table, packets that comply with IP-MAC address binding or IP address binding for port security cannot be forwarded.

Examples

The following example binds GigabitEthernet 0/1 to IPv4 secure address 192.168.1.100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switchport port-security interface gigabitethernet 0/1 binding
192.168.1.100
```

The following example binds GigabitEthernet 0/1 to MAC address 00d0.f800.5555, VLAN ID 1, and IPv4 secure address 192.168.1.100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switchport port-security interface gigabitethernet 0/1 binding
00d0.f800.5555 vlan 1 192.168.1.100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 switchport port-security mac-address

Function

Run the **switchport port-security mac-address** command to configure static secure addresses.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static secure address is configured by default.

Syntax

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

no switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]

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

Parameter Description

mac-address *mac-address*: Specifies the static secure address to be configured.

vlan *vlan-id*: Specifies the VLAN to which a MAC address belongs. The value range is from 1 to 4094. This parameter takes effect only for trunk ports.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the static secure address to 00d0.f800.5555 and VLAN ID to 2 for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security mac-address
00d0.f800.5555 vlan 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 switchport port-security interface mac-address

Function

Run the **switchport port-security interface mac-address** command to configure static secure addresses.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static secure address is configured by default.

Syntax

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

no switchport port-security interface *interface-type interface-number* **mac-address** *mac-address* [**vlan** *vlan-id*]

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

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

mac-address *mac-address*: Specifies the static secure address to be configured.

vlan vlan-*id*: Specifies the VLAN to which a MAC address belongs. The value range is from 1 to 4094. This parameter takes effect only for trunk ports.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the static secure address to 00d0.f800.5555 and VLAN ID to 2 for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switchport port-security interface gigabitethernet 0/1 mac-address 00d0.f800.5555 vlan 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 switchport port-security maximum

Function

Run the **switchport port-security maximum** command to configure the maximum number of secure addresses for a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

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

Syntax

switchport port-security maximum *number*

no switchport port-security maximum

default switchport port-security maximum

Parameter Description

maximum *number*: Specifies the maximum number of secure addresses. The value range is from 1 to 128.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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 number of secure addresses is the sum of statically configured secure addresses and dynamically learned secure addresses. The default value is **128**. If the configured maximum number of secure addresses is smaller than the current number of secure addresses, the configuration fails.

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

Caution

If 802.1x is enabled on a port but the number of authenticated users exceeds the maximum number of users configured for port security, port security cannot be enabled.

Examples

The following example sets the maximum number of secure addresses to 2 for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security maximum 2
```

Notifications

When the configured maximum number of secure addresses is smaller than the current number of secure addresses, the following notification will be displayed:

```
Setting value is less than the current maximum.
```

Common Errors

The configured maximum number of addresses is smaller than the current number of addresses.

Platform Description

N/A

Related Commands

N/A

1.9 switchport port-security mac-address sticky

Function

Run the **switchport port-security mac-address sticky** command to enable sticky MAC address learning and configure sticky MAC addresses.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Sticky MAC address learning is disabled by default.

Syntax

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

no switchport port-security mac-address sticky [*mac-address* [**vlan** *vlan-id*]]

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

Parameter Description

mac-address: MAC address.

vlan *vlan-id*: Specifies the VLAN to which a MAC address belongs. This parameter takes effect only for trunk ports.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Sticky MAC address learning is used to save MAC addresses dynamically learned by the device to sticky MAC addresses. 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.

Examples

The following example configures sticky MAC address 00d0.f800.5555 and VLAN ID 1 for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security mac-address
sticky 00d0.f800.5555 vlan 1
```

The following example enables sticky MAC address learning for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security mac-address
sticky
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 switchport port-security violation

Function

Run the **switchport port-security violation** command to configure the method for handling packets that violate the port security requirements.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

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

Syntax

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

no switchport port-security violation

default switchport port-security violation

Parameter Description

protect: Discards packets that do not match the security address.

restrict: Discards packets that do not match the security address and sends a trap notification.

shutdown: Discards packets that do not match the security address and disables the port.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the number of MAC addresses learned by a port exceeds the maximum number of secure addresses, a security violation event is triggered. If the violation handling mode of the port is changed after a violation, the new violation handling mode takes effect only after the secure port is restored to the non-violation state and violates the security again.

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

Examples

The following example enables port security on Gigabitethernet 0/1 and sets the port security violation handling mode to **shutdown**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security violation
shutdown
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show port-security

Function

Run the **show port-security** command to display port security configurations and secure addresses.

Syntax

show port-security [**all** | [**address** | **binding**] [**interface** *interface-type interface-number*]]

Parameter Description

address: Specifies the secure address to be displayed.

binding: Specifies the security binding to be displayed.

interface *interface-type interface-number*: Specifies the interface whose port security configurations are displayed.

all: Displays all effective secure addresses and security bindings.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified when this command is run (**show port-security**), port security configurations, violation handling, and other information of all interfaces are displayed.

Examples

The following example displays all port security configurations.

```
Hostname> enable
Hostname# show port-security
NO.  SecurePort MaxSecureAddr CurrentAddr CurrentIpBind CurrentIpMacBind
SecurityAction AgingTime
                  (Count)      (Count)      (Count)          (Count)
(min)
1    Gi0/1      128           2           2             1                protect
Total secure addresses in System : 2
Total secure bindings  in System : 3
```

Table 1-1Output Fields of the show port-security Command

Field	Description
NO.	Record number
Secure Port	Device port name
MaxSecureAddr(count)	Maximum number of secure addresses allowed on a port
CurrentAddr(count)	Current number of secure addresses on a port
CurrentIpBind (count)	Number of secure IP address bindings on a port
CurrentIpMacBind (count)	Number of secure IP-MAC address bindings on a port
Security Action	Violation handling mode on a port
Total secure addresses in System	Total number of secure addresses configured on a device
Total secure bindings in System	Number of security bindings configured on a device

The following example displays all secure addresses.

```
Hostname> enable
Hostname# show port-security address
NO.  VLAN  MacAddress      PORT                      TYPE
RemainingAge(mins)  STATUS
1    1     00d0.f800.073c  GigabitEthernet 0/1       Configured         --
active
```

```
2    1     00d0.f800.073d  GigabitEthernet 0/1       Configured         --
active
```

Table 1-2Output Fields of the show port-security address Command

Field	Description
NO.	Record number
Vlan	VLAN ID
Mac Address	MAC address
Port	Port name
Type	Method for generating the secure address
Remaining Age(mins)	Address aging time
STATUS	Secure address effective status

The following example displays all security bindings.

```
Hostname> enable
Hostname# show port-security binding
NO.  VLAN MacAddress     PORT       IpAddress
FilterType FilterStatus
1    1    00d0.f800.073c Gi0/1      192.168.12.202
ipv4-mac   active
2     --        --       Gi0/1      192.168.0.1
ipv4-only  active
3     --        --       Gi0/1      ffaa:ddcc::1
ipv6-only  active
```

Table 1-3Output Fields of the show port-security binding Command

Field	Description
NO.	Record number
Vlan	VLAN ID
Mac Address	MAC address
Port	Port name
IpAddress	IP address
FilterType	Security binding filtering type
FilterStatus	Security binding effective status

The following example displays port security configurations of Gigabitethernet 0/1.

```
Hostname> enable
Hostname# show port-security interface gigabitethernet 0/1
Interface                    : GigabitEthernet 0/1
Port status                  : down
Port Security                : enabled
SecureStatic address aging   : disabled
Sticky dynamic address       : disabled
Violation mode               : protect
Maximum MAC Addresses        : 128
Total MAC Addresses          : 2
Configured MAC Addresses     : 2
Dynamic MAC Addresses        : 0
Sticky MAC Addresses         : 0
Total security binding       : 3
IPv4-ONLY Binding Addresses  : 1
IPv6-ONLY Binding Addresses  : 1
IPv4-MAC Binding Addresses   : 1
IPv6-MAC Binding Addresses   : 0
Aging time(min)              : 0
```

Table 1-4Output Fields of the show port-security interface Command

Field	Description
Interface	Device port name
Port status	Device port status
Port Security	Port security enabling status on the port
SecureStatic address aging	Whether secure addresses statically configured on the port will be aged
Sticky dynamic address	Whether secure addresses dynamically learned on the port will be converted to sticky addresses
Violation mode	Violation handling mode on the port
Maximum MAC Addresses	Maximum number of secure addresses allowed on a port
Total MAC Addresses	Number of effective secure addresses
Configured MAC Addresses	Number of statically configured secure addresses
Dynamic MAC Addresses	Number of dynamically configured secure addresses
Sticky MAC Addresses	Number of sticky secure addresses
Total security binding	Number of effective security bindings

Field	Description
IPv4-ONLY Binding Addresses	Number of security bindings with only IPv4 addresses
IPv6-ONLY Binding Addresses	Number of security bindings with only IPv6 addresses
IPv4-MAC Binding Addresses	Number of security bindings with IPv4 and MAC addresses
IPv6-MAC Binding Addresses	Number of security bindings with IPv6 and MAC addresses
Aging time(min)	Secure address aging time

Notifications

N/A

Platform Description

N/A