47
Port Security

- Prerequisites for Port Security, page 47-1
- Restrictions for Port Security, page 47-1
- Information About Port Security, page 47-2
- Default Port Security Configuration, page 47-4
- How to Configure Port Security, page 47-4
- Verifying the Port Security Configuration, page 47-11

Note

- For complete syntax and usage information for the commands used in this chapter, see these publications:

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.4SY supports only Ethernet interfaces. Cisco IOS Release 15.4SY does not support any WAN features or commands.

Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

Prerequisites for Port Security

None.

Restrictions for Port Security

- With the default port security configuration, to bring all secure ports out of the error-disabled state, enter the **errdisable recovery cause psecure-violation** global configuration command, or manually reenable the port by entering the **shutdown** and **no shut down** interface configuration commands.
- Enter the **clear port-security dynamic** global configuration command to clear all dynamically learned secure addresses.

- Port security learns unauthorized MAC addresses with a bit set that causes traffic to them or from them to be dropped. The **show mac address-table** command displays the unauthorized MAC addresses, but does not display the state of the bit. (CSCeb76844)
- To preserve dynamically learned sticky MAC addresses and configure them on a port following a bootup or a reload and after the dynamically learned sticky MAC addresses have been learned, you must enter a **write memory** or **copy running-config startup-config** command to save them in the startup-config file.
- Port security supports private VLAN (PVLAN) ports.
- Port security supports IEEE 802.1Q tunnel ports.
- Port security does not support Switch Port Analyzer (SPAN) destination ports.
- Port security supports access and trunking EtherChannel port-channel interfaces.
- You can configure port security and 802.1X port-based authentication on the same port.
- Port security supports nonnegotiating trunks.
  - Port security only supports trunks configured with these commands:

    switchport
    switchport trunk encapsulation
    switchport mode trunk
    switchport nonegotiate
  - If you reconfigure a secure access port as a trunk, port security converts all the sticky and static secure addresses on that port that were dynamically learned in the access VLAN to sticky or static secure addresses on the native VLAN of the trunk. Port security removes all secure addresses on the voice VLAN of the access port.
  - If you reconfigure a secure trunk as an access port, port security converts all sticky and static addresses learned on the native VLAN to addresses learned on the access VLAN of the access port. Port security removes all addresses learned on VLANs other than the native VLAN.

Note Port security uses the VLAN ID configured with the **switchport trunk native vlan** command.

- Take care when you enable port security on the ports connected to the adjacent switches when there are redundant links running between the switches because port security might error-disable the ports due to port security violations.
- In Cisco IOS Release 15.1(1)SY2 and later releases, the options starting with the number 6 for the **radius-server attribute** command changed from 6, 61, 69 to 6, 61, 66, 67, and 69.

Information About Port Security

- Port Security with Dynamically Learned and Static MAC Addresses, page 47-3
- Port Security with Sticky MAC Addresses, page 47-3
- Port Security with IP Phones, page 47-4

Port Security with Dynamically Learned and Static MAC Addresses

You can use port security with dynamically learned and static MAC addresses to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. When you assign secure MAC addresses to a secure port, the port does not forward ingress traffic that has source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the device attached to that port has the full bandwidth of the port.

A security violation occurs in these situations:

- When the maximum number of secure MAC addresses is reached on a secure port and the source MAC address of the ingress traffic is different from any of the identified secure MAC addresses, port security applies the configured violation mode.
- If traffic with a secure MAC address that is configured or learned on one secure port attempts to access another secure port in the same VLAN, applies the configured violation mode.

Note After a secure MAC address is configured or learned on one secure port, the sequence of events that occurs when port security detects that secure MAC address on a different port in the same VLAN is known as a MAC move violation.

- Running diagnostic tests with port security enabled.

See the "Configuring the Port Security Violation Mode on a Port" section on page 47-6 for more information about the violation modes.

After you have set the maximum number of secure MAC addresses on a port, port security includes the secure addresses in the address table in one of these ways:

- You can statically configure all secure MAC addresses by using the **switchport port-security mac-address** *mac_address* interface configuration command.
- You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
- You can statically configure a number of addresses and allow the rest to be dynamically configured.

If the port has a link-down condition, all dynamically learned addresses are removed.

Following bootup, a reload, or a link-down condition, port security does not populate the address table with dynamically learned MAC addresses until the port receives ingress traffic.

A security violation occurs if the maximum number of secure MAC addresses have been added to the address table and the port receives traffic from a MAC address that is not in the address table.

You can configure the port for one of three violation modes: protect, restrict, or shutdown. See the "How to Configure Port Security" section on page 47-4.

To ensure that an attached device has the full bandwidth of the port, set the maximum number of addresses to one and configure the MAC address of the attached device.

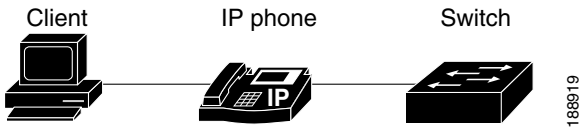
Port Security with Sticky MAC Addresses

Port security with sticky MAC addresses provides many of the same benefits as port security with static MAC addresses, but sticky MAC addresses can be learned dynamically. Port security with sticky MAC addresses retains dynamically learned MAC addresses during a link-down condition.

If you enter a **write memory** or **copy running-config startup-config** command, then port security with sticky MAC addresses saves dynamically learned MAC addresses in the startup-config file and the port does not have to learn addresses from ingress traffic after bootup or a restart.

Port Security with IP Phones

Figure 47-1 Device Connected Through IP Phone



Because the device is not directly connected to the switch, the switch cannot physically detect a loss of port link if the device is disconnected. Later Cisco IP phones send a Cisco Discovery Protocol (CDP) host presence type length value (TLV) to notify the switch of changes in the attached device's port link state. The switch recognizes the host presence TLV. Upon receiving a host presence TLV notification of a link down on the IP phone's data port, port security removes from the address table all static, sticky, and dynamically learned MAC addresses. The removed addresses are added again only when the addresses are learned dynamically or configured.

Default Port Security Configuration

Feature	Default Setting
Port security	Disabled.
Maximum number of secure MAC addresses	1.
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.

How to Configure Port Security

- Enabling Port Security, page 47-5
- Configuring the Port Security Violation Mode on a Port, page 47-6
- Configuring the Maximum Number of Secure MAC Addresses on a Port, page 47-7
- Enabling Port Security with Sticky MAC Addresses on a Port, page 47-8
- Configuring a Static Secure MAC Address on a Port, page 47-9
- Configuring Secure MAC Address Aging on a Port, page 47-10

Enabling Port Security

- Enabling Port Security on a Trunk, page 47-5
- Enabling Port Security on an Access Port, page 47-6

Enabling Port Security on a Trunk

Port security supports nonnegotiating trunks.

Caution Because the default number of secure addresses is one and the default violation action is to shut down the port, configure the maximum number of secure MAC addresses on the port before you enable port security on a trunk (see "Configuring the Maximum Number of Secure MAC Addresses on a Port" section on page 47-7).

To enable port security on a trunk, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	Selects the interface to configure.
Step 2	`Router(config-if)# switchport`	Configures the port as a Layer 2 port.
Step 3	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	Configures the encapsulation as 802.1Q.
Step 4	`Router(config-if)# switchport mode trunk`	Configures the port to trunk unconditionally.
Step 5	`Router(config-if)# switchport nonegotiate`	Configures the trunk not to use DTP.
Step 6	`Router(config-if)# switchport port-security`	Enables port security on the trunk.
Step 7	`Router(config-if)# do show port-security interface type slot/port | include Port Security`	Verifies the configuration.

This example shows how to configure Gigabit Ethernet port 5/36 as a nonnegotiating trunk and enable port security:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/36
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface gigabitethernet 5/36 | include Port
Security
Port Security              : Enabled
```

Enabling Port Security on an Access Port

To enable port security on an access port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	Selects the interface to configure. **Note** The port can be a tunnel port or a PVLAN port.
Step 2	`Router(config-if)# switchport`	Configures the port as a Layer 2 port.
Step 3	`Router(config-if)# switchport mode access`	Configures the port as a Layer 2 access port. **Note** A port in the default mode (dynamic desirable) cannot be configured as a secure port.
Step 4	`Router(config-if)# switchport port-security`	Enables port security on the port.
Step 5	`Router(config-if)# do show port-security interface type slot/port | include Port Security`	Verifies the configuration.

This example shows how to enable port security on Gigabit Ethernet port 5/12:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Port Security
Port Security              : Enabled
```

Configuring the Port Security Violation Mode on a Port

To configure the port security violation mode on a port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport port-security violation {protect | restrict | shutdown}`	(Optional) Sets the violation mode and the action to be taken when a security violation is detected.
Step 3	`Router(config-if)# do show port-security interface type slot/port | include violation_mode`	Verifies the configuration. The values for *violation_mode* are **protect**, **restrict**, or **shutdown**.

- **protect**—The PFC drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- **restrict**—The PFC drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the security violation counter to increment.
- **shutdown**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

Note To bring a secure port out of the error-disabled state, enter the **errdisable recovery cause** *violation_mode* global configuration command, or you can manually reenable it by entering the **shutdown** and **no shut down** interface configuration commands.

This example shows how to configure the protect security violation mode on Gigabit Ethernet port 5/12:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security violation protect
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Protect
Violation Mode             : Protect
```

This example shows how to configure the restrict security violation mode on Gigabit Ethernet port 5/12:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security violation restrict
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Restrict
Violation Mode             : Restrict
```

Configuring the Maximum Number of Secure MAC Addresses on a Port

To configure the maximum number of secure MAC addresses on a port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	Selects the interface to configure.
Step 2	`Router(config-if)# switchport port-security maximum number_of_addresses vlan {vlan_ID | vlan_range}`	Sets the maximum number of secure MAC addresses for the port (default is 1). **Note** Per-VLAN configuration is supported only on trunks.

- The range for *number_of_addresses* is 1 to 4,097.
- Port security supports trunks.
  - On a trunk, you can configure the maximum number of secure MAC addresses both on the trunk and for all the VLANs on the trunk.
  - You can configure the maximum number of secure MAC addresses on a single VLAN or a range of VLANs.
  - For a range of VLANs, enter a dash-separated pair of VLAN numbers.

  - You can enter a comma-separated list of VLAN numbers and dash-separated pairs of VLAN numbers.

This example shows how to configure a maximum of 64 secure MAC addresses on Gigabit Ethernet port 5/12:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security maximum 64
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Maximum
Maximum MAC Addresses      : 64
```

Enabling Port Security with Sticky MAC Addresses on a Port

To enable port security with sticky MAC addresses on a port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	Selects the interface to configure.
Step 2	`Router(config-if)# switchport port-security mac-address sticky`	Enables port security with sticky MAC addresses on a port.

- When you enter the **switchport port-security mac-address sticky** command:
  - All dynamically learned secure MAC addresses on the port are converted to sticky secure MAC addresses.
  - Static secure MAC addresses are not converted to sticky MAC addresses.
  - Secure MAC addresses dynamically learned in a voice VLAN are not converted to sticky MAC addresses.
  - New dynamically learned secure MAC addresses are sticky.
- When you enter the **no switchport port-security mac-address sticky** command, all sticky secure MAC addresses on the port are converted to dynamic secure MAC addresses.
- To preserve dynamically learned sticky MAC addresses and configure them on a port following a bootup or a reload, after the dynamically learned sticky MAC addresses have been learned, you must enter a **write memory** or **copy running-config startup-config** command to save them in the startup-config file.

This example shows how to enable port security with sticky MAC addresses on Gigabit Ethernet port 5/12:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security mac-address sticky
```

Configuring a Static Secure MAC Address on a Port

To configure a static secure MAC address on a port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport port-security mac-address sticky mac_address [vlan vlan_ID]`	Configures a static MAC address as secure on the port. **Note** Per-VLAN configuration is supported only on trunks.
Step 3	`Router(config-if)# end`	Exits configuration mode.

- You can configure sticky secure MAC addresses if port security with sticky MAC addresses is enabled (see the "Enabling Port Security with Sticky MAC Addresses on a Port" section on page 47-8).
- The maximum number of secure MAC addresses on the port, configured with the **switchport port-security maximum** command, defines how many secure MAC addresses you can configure.
- If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are learned dynamically.
- Port security is supported on trunks.
  - On a trunk, you can configure a static secure MAC address in a VLAN.
  - On a trunk, if you do not configure a VLAN for a static secure MAC address, it is secure in the VLAN configured with the **switchport trunk native vlan** command.

This example shows how to configure a MAC address 1000.2000.3000 as secure on Gigabit Ethernet port 5/12 and verify the configuration:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security mac-address 1000.2000.3000
Router(config-if)# end
Router# show port-security address
          Secure Mac Address Table
------------------------------------------------------------

Vlan    Mac Address       Type                Ports
----    -----------       ----                -----
   1    1000.2000.3000    SecureConfigured     Gi5/12
```

Configuring Secure MAC Address Aging on a Port

- Configuring the Secure MAC Address Aging Type on a Port, page 47-10
- Configuring Secure MAC Address Aging Time on a Port, page 47-10

Note

- Static secure MAC addresses and sticky secure MAC addresses do not age out.
- When the aging type is configured with the **absolute** keyword, all the dynamically learned secure addresses age out when the aging time expires. When the aging type is configured with the **inactivity** keyword, the aging time defines the period of inactivity after which all the dynamically learned secure addresses age out.

Configuring the Secure MAC Address Aging Type on a Port

You can configure the secure MAC address aging type on a port. To configure the secure MAC address aging type on a port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport port-security aging type {absolute | inactivity}`	Configures the secure MAC address aging type on the port (default is absolute).

This example shows how to set the aging type to inactivity on Gigabit Ethernet port 5/12:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security aging type inactivity
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Type
Aging Type                 : Inactivity
```

Configuring Secure MAC Address Aging Time on a Port

To configure the secure MAC address aging time on a port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	Selects the interface to configure.
Step 2	`Router(config-if)# switchport port-security aging time aging_time`	Configures the secure MAC address aging time on the port. The *aging_time* range is 1 to 1440 minutes (default is 0).

This example shows how to configure 2 hours (120 minutes) as the secure MAC address aging time on Gigabit Ethernet port 5/1:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/1
Router(config-if)# switchport port-security aging time 120
```

```
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Time
Aging Time                : 120 mins
```

Verifying the Port Security Configuration

To display port security settings, enter this command:

Command	Purpose
`Router# show port-security [interface {{vlan vlan_ID} | {type slot/port}}] [address]`	Displays port security settings for the switch or for the specified interface.

- Port security supports the **vlan** keyword only on trunks.
- Enter the **address** keyword to display secure MAC addresses, with aging information for each address, globally for the switch or per interface.
- The display includes these values:
  - The maximum allowed number of secure MAC addresses for each interface
  - The number of secure MAC addresses on the interface
  - The number of security violations that have occurred
  - The violation mode

This example displays output from the **show port-security** command when you do not enter an interface:

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
---------------------------------------------------------------------------

     Gi5/1           11            11            0            Shutdown
     Gi5/5           15            5             0            Restrict
     Gi5/11          5             4             0            Protect
---------------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
```

This example displays output from the **show port-security** command for a specified interface:

```
Router# show port-security interface gigabitethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

This example displays the output from the **show port-security address** privileged EXEC command:

```
Router# show port-security address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                        (mins)
```

```
----    -----------       ----                -----   -------------
   1    0001.0001.0001    SecureDynamic       Gi5/1      15 (I)
   1    0001.0001.0002    SecureDynamic       Gi5/1      15 (I)
   1    0001.0001.1111    SecureConfigured    Gi5/1      16 (I)
   1    0001.0001.1112    SecureConfigured    Gi5/1      -
   1    0001.0001.1113    SecureConfigured    Gi5/1      -
   1    0005.0005.0001    SecureConfigured    Gi5/5      23
   1    0005.0005.0002    SecureConfigured    Gi5/5      23
   1    0005.0005.0003    SecureConfigured    Gi5/5      23
   1    0011.0011.0001    SecureConfigured    Gi5/11     25 (I)
   1    0011.0011.0002    SecureConfigured    Gi5/11     25 (I)
------------------------------------------------------------------------
Total Addresses in System: 10
Max Addresses limit in System: 128
```

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum