



CHAPTER 32

Configuring Port Security

This chapter describes how to configure port security on Catalyst 4500 series switches. It provides guidelines, procedures, and configuration examples.



Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>.

This chapter consists of these sections:

- [Overview of Port Security, page 32-1](#)
- [Default Port Security Configuration, page 32-3](#)
- [Port Security Guidelines and Restrictions, page 32-3](#)
- [Configuring Port Security, page 32-3](#)
- [Displaying Port Security Settings, page 32-7](#)

Overview of Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with 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 workstation attached to that port is assured the full bandwidth of the port.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a workstation attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs.

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

- You can 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 configure a number of addresses and allow the rest to be dynamically configured.

**Note**

If the port shuts down, all dynamically learned addresses are removed.

- You can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts. Although sticky secure addresses can be manually configured, it is not recommended.

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling *sticky learning*. To enable sticky learning, enter the **switchport port-security mac-address sticky** command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the configuration, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

After the maximum number of secure MAC addresses is configured, they are stored in an address table. To ensure that an attached device has the full bandwidth of the port, configure the MAC address of the attached device and set the maximum number of addresses to one, which is the default.

**Note**

When a Catalyst 4500 series switch port is configured to support voice as well as port security, the maximum number of allowable MAC addresses on this port should be changed to three.

A security violation occurs if the maximum number of secure MAC addresses has been added to the address table and a workstation whose MAC address is not in the address table attempts to access the interface.

You can configure the interface for one of these violation modes, based on the action to be taken if a violation occurs:

- Restrict—A port security violation restricts data, causes the SecurityViolation counter to increment, and causes an SNMP Notification to be generated. The rate at which SNMP traps are generated can be controlled by the **snmp-server enable traps port-security trap-rate** command. The default value (“0”) causes an SNMP trap to be generated for every security violation.
- Shutdown—A port security violation causes the interface to shut down immediately. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command or you can manually reenabling it by entering the **shutdown** and **no shut down** interface configuration commands. This is the default mode.

You can also customize the time to recover from the specified error disable cause (default is 300 seconds) by entering the **errdisable recovery interval interval** command.

Default Port Security Configuration

Table 32-1 shows the default port security configuration for an interface.

Table 32-1 Default Port Security Configuration

Feature	Default Setting
Port security	Disabled on a port
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.
Aging	Disabled
Aging type	Absolute
Static Aging	Disabled
Sticky	Disabled

Port Security Guidelines and Restrictions

Follow these guidelines when configuring port security:

- A secure port cannot be a trunk port.
- A secure port cannot be a destination port for Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel port-channel interface.
- A secure port and static MAC address configuration are mutually exclusive.

Configuring Port Security

These sections describe how to configure port security:

- [Configuring Port Security on an Interface, page 32-4](#)
- [Configuring Port Security Aging, page 32-6](#)

Configuring Port Security on an Interface

To restrict traffic through a port by limiting and identifying MAC addresses of the stations allowed to access the port, perform this task:

	Command	Purpose
Step 1	Switch(config)# interface <i>interface_id</i>	Enters interface configuration mode and enters the physical interface to configure, for example gigabitethernet 3/1 .
Step 2	Switch(config-if)# switchport mode access	Sets the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.
Step 3	Switch(config-if)# switchport port-security	Enables port security on the interface.
Step 4	Switch(config-if)# switchport port-security maximum <i>value</i>	(Optional) Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 3072; the default is 1.
Step 5	Switch(config-if)# switchport port-security violation { restrict shutdown }	(Optional) Sets the violation mode, the action to be taken when a security violation is detected, as one of these: • restrict—A port security violation restricts data and causes the SecurityViolation counter to increment and send an SNMP trap notification. • shutdown—The interface is error-disabled when a security violation occurs. Note When a secure port is in the error-disabled state, you can bring it out of this state by entering the errdisable recovery cause psecure-violation global configuration command or you can manually reenale it by entering the shutdown and no shut down interface configuration commands.
Step 6	Switch(config-if)# switchport port-security limit rate invalid-source-mac	Sets the rate limit for bad packets.
Step 7	Switch(config-if)# switchport port-security mac-address <i>mac_address</i>	(Optional) Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.
Step 8	Switch(config-if)# switchport port-security mac-address sticky	(Optional) Enable sticky learning on the interface.
Step 9	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 10	Switch# show port-security address Switch# show port-security address	Verifies your entries.

- To return the interface to the default condition as not a secure port, use the **no switchport port-security** interface configuration command.
- To return the interface to the default number of secure MAC addresses, use the **no switchport port-security maximum** *value*.
- To delete a MAC address from the address table, use the **no switchport port-security mac-address** *mac_address* command.
- To return the violation mode to the default condition (shutdown mode), use the **no switchport port-security violation {restrict | shutdown}** command.
- To disable sticky learning on an interface, use the **no switchport port-security mac-address sticky** command. The interface converts the sticky secure MAC addresses to dynamic secure addresses.
- To delete a sticky secure MAC addresses from the address table, use the **no switchport port-security sticky mac-address** *mac_address* command. To delete all the sticky addresses on an interface or a VLAN, use the **no switchport port-security sticky interface** *interface-id* command.
- To clear dynamically learned port security MAC in the CAM table, use the **clear port-security dynamic** command. The **address** keyword enables you to clear a secure MAC addresses. The **interface** keyword enables you to clear all secure addresses on an interface.

This example shows how to enable port security on Fast Ethernet port 12 and how to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
Switch# show port-security interface fastethernet 3/12
Port Security           :Enabled
Port Status             :Secure-up
Violation Mode          :Shutdown
Aging Time              :0
Aging Type               :Absolute
SecureStatic Address Aging :Enabled
Maximum MAC Addresses    :5
Total MAC Addresses      :0
Configured MAC Addresses :0
Sticky MAC Addresses     :11
Last Source Address      :0000.0000.0401
Security Violation Count :0
```

This example shows how to configure a secure MAC address on Fast Ethernet port 5/1 and verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 10
Switch(config-if)# switchport port-security mac-address 0000.0000.0003 (Static secure MAC)
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)#
switchport port-security mac-address sticky 0000.0000.0001 (Sticky static MAC)
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# end
```

```
Switch#show port address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
  1      0000.0000.0001    SecureSticky        Fa5/1    -
  1      0000.0000.0002    SecureSticky        Fa5/1    -
  1      0000.0000.0003    SecureConfigured    Fa5/1    -
-----
Total Addresses in System (excluding one mac per port)    : 2
Max Addresses limit in System (excluding one mac per port) : 1024
```

Configuring Port Security Aging

You can use port security aging to set the aging time and aging type for all secure addresses on a port.

Use this feature to remove and add PCs on a secure port without manually deleting the existing secure MAC addresses while still limiting the number of secure addresses on a port.

To configure port security aging, perform this task:

	Command	Purpose
Step 1	Switch(config)# interface <i>interface_id</i>	Enters interface configuration mode for the port on which you want to enable port security aging.
Step 2	Switch(config-if)# switchport port-security [aging { static time <i>aging_time</i> type { absolute inactivity }]	Sets the aging time for the secure port. The static keyword enables aging for statically configured secure addresses on this port. The time <i>aging_time</i> keyword specifies the aging time for this port. Valid range for <i>aging_time</i> is from 0 to 1440 minutes. If the time is equal to 0, aging is disabled for this port. The type keyword sets the aging type as absolute or inactive . For absolute aging, all the secure addresses on this port ago out exactly after the time (minutes) specified and are removed from the secure address list. For inactive aging, the secure addresses on this port ago out only if there is no data traffic from the secure source address for the specified time period.
Step 3	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 4	Switch# show port security [interface <i>interface_id</i>] [address]	Verifies your entries.

To disable port security aging for all secure addresses on a port, use the **no switchport port-security aging time** interface configuration command.

This example shows how to set the aging time as 2 hours for the secure addresses on the Fast Ethernet interface 5/1:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes:

```
Switch(config-if)# switchport port-security aging time 2
```

You can verify the previous commands by entering the **show port-security interface *interface_id*** command.

Displaying Port Security Settings

Use the **show port-security** command to display port-security settings for an interface or for the switch.

To display traffic control information, perform one or more of these tasks:

Command	Purpose
Switch# show port-security [interface <i>interface_id</i>]	Displays port security settings for the switch or for the specified interface, including 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, and the violation mode.
Switch# show port-security [interface <i>interface_id</i>] address	Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.

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

```
Switch# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
      (Count)      (Count)      (Count)
-----
Fa3/1          2           2             0          Restrict
Fa3/2          2           2             0          Restrict
Fa3/3          2           2             0          Shutdown
Fa3/4          2           2             0          Shutdown
Fa3/5          2           2             0          Shutdown
Fa3/6          2           2             0          Shutdown
Fa3/7          2           2             0          Shutdown
Fa3/8          2           2             0          Shutdown
Fa3/10         1           0             0          Shutdown
Fa3/11         1           0             0          Shutdown
Fa3/12         1           0             0          Restrict
Fa3/13         1           0             0          Shutdown
Fa3/14         1           0             0          Shutdown
Fa3/15         1           0             0          Shutdown
Fa3/16         1           0             0          Shutdown
-----
Total Addresses in System (excluding one mac per port)    :8
Max Addresses limit in System (excluding one mac per port) :1024
Global SNMP trap control for port-security                :20 (traps per second)
```

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

```
Switch# show port-security interface fastethernet 5/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address     : 0000.0001.001a
Security Violation Count : 0
```

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

```
Switch#sh port-security address
Secure Mac Address Table
-----
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0000.0001.0000	SecureConfigured	Fa3/1	15 (I)
1	0000.0001.0001	SecureConfigured	Fa3/1	14 (I)
1	0000.0001.0100	SecureConfigured	Fa3/2	-
1	0000.0001.0101	SecureConfigured	Fa3/2	-
1	0000.0001.0200	SecureConfigured	Fa3/3	-
1	0000.0001.0201	SecureConfigured	Fa3/3	-
1	0000.0001.0300	SecureConfigured	Fa3/4	-
1	0000.0001.0301	SecureConfigured	Fa3/4	-
1	0000.0001.1000	SecureDynamic	Fa3/5	-
1	0000.0001.1001	SecureDynamic	Fa3/5	-
1	0000.0001.1100	SecureDynamic	Fa3/6	-
1	0000.0001.1101	SecureDynamic	Fa3/6	-
1	0000.0001.1200	SecureSticky	Fa3/7	-
1	0000.0001.1201	SecureSticky	Fa3/7	-
1	0000.0001.1300	SecureSticky	Fa3/8	-
1	0000.0001.1301	SecureSticky	Fa3/8	-

```
-----
Total Addresses in System (excluding one mac per port) :8
Max Addresses limit in System (excluding one mac per port) :1024
```