CHAPTER 30

Configuring Port Security and Trunk Port Security

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

Note For complete syntax and usage information for the switch commands used in this chapter, see the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

If the command is not found in the *Cisco Catalyst 4500 Command Reference*, you can locate it in the larger Cisco IOS library. Refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

This chapter consists of these sections:

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 for access, private VLAN host, and private VLAN promiscuous ports.
- You can configure all secure MAC addresses by using the **port-security mac-address** vlan range configuration command for trunk and private VLAN trunk ports.
- 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's link goes down, all dynamically secured addresses are no longer secure.

- 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* port security. To enable sticky port security, 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 running config file to the configuration file, the interface does not need to relearn these addresses when the switch restarts. If you do not save the configuration, they are lost.

If sticky port security 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.

Note The address on a voice VLAN, such as a Cisco IP Phone, cannot be made sticky.

A security violation occurs if the maximum number of secure MAC addresses to a port 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 (that is, packets are dropped in software), 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 reenable 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.

Port mode changes

Generally, when a port mode changes, all dynamic addresses associated with that port are removed. All static or sticky addresses and other port security parameters configured on the native VLAN are moved to the native VLAN of the port in the new mode. All the addresses on the non-native VLANs are removed.

The behavior for port mode changes is as follows:

- When the mode changes from trunk or access to private VLAN trunk, all the static or sticky addresses configured on the access VLAN of the access port and the native VLAN of the trunk port are moved to the private VLAN native vlan of the private VLAN trunk port. All other addresses are removed.
- When the mode changes from private VLAN trunk to trunk or access mode, all the static or sticky addresses configured on the private VLAN native VLAN are moved to the native VLAN of the trunk port and the access VLAN of the access port. All other addresses are removed.

  For a regular or private VLAN trunk port, if the VLAN is removed from the allowed VLAN list, all the addresses associated with that VLAN are removed.

Default Port Security Configuration

Table 30-1 shows the default port security configuration for an interface.

Table 30-1 Default Port Security Configuration

Feature	Default Setting
Aging	Disabled
Aging type	Absolute
invalid-source-mac	10 packets per second
Maximum number of secure MAC addresses	1
Port security	Disabled on a port
Static Aging	Disabled

Table 30-1 Default Port Security Configuration

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

Port Security Guidelines and Restrictions

Follow these guidelines when configuring port security:

- 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 for an interface are mutually exclusive.
- Port security cannot be enabled on dynamic access ports.
- Port security cannot be enabled on Ether Channels.
- When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP phone, the IP phone requires up to two MAC addresses. The IP phone address is learned on the voice VLAN and might also be learned on the access VLAN. Connecting a PC to the IP phone requires additional MAC addresses.
- When you enter a maximum secure address value for an interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

Configuring Port Security

These sections describe how to configure port security:

- Configuring Port Security on an Interface, page 30-5
- Configuring Trunk Port Security, page 30-7
- Configuring Port Security Aging, page 30-10

Configuring Port Security on an Interface

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

	Command	Purpose
Step 1	`Switch(config)# interface interface_id`	Enters interface configuration mode and specifies the physical interface to configure.
Step 2	`Switch(config-if)# switchport mode {access | private vlan host | private vlan promiscuous}`	Sets the interface mode. **Note** 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 value`	(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 reenable 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 packets_per_sec`	Sets the rate limit for bad packets.
Step 7	`Switch(config-if)# switchport port-security mac-address mac_address`	(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. **Note** This command only applies is valid to access, PVLAN host, and PVLAN promiscuous mode. For more details on PVLAN or trunk or regular trunk mode, refer to the "Configuring Trunk Port Security" section on page 30-7.
Step 8	`Switch(config-if)# switchport port-security mac-address sticky`	(Optional) Enable sticky learning on the interface.

	Command	Purpose (continued)
Step 9	`Switch(config-if)# switchport port-security mac-address mac_address sticky`	Specifies the sticky mac-address for the interface. **Note** This command only applies is valid to access, PVLAN host, and PVLAN promiscuous mode. For more details on PVLAN or trunk or regular trunk mode, refer to the "Configuring Trunk Port Security" section on page 30-7.
Step 10	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 11	`Switch# show port-security address interface interface_id` `Switch# show port-security address`	Verifies your entries.

- To return the interface to the default condition as nonsecure port, use the **no switchport port-security** 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 mac-address** *mac_address* **sticky** command. To delete all the sticky addresses on an interface, use the **no switchport port-security mac-address sticky** 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. The VLAN keyword allows you to clear port security MACs on a per-VLAN per-port basis.

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 interface 5/1 and verify the configuration:

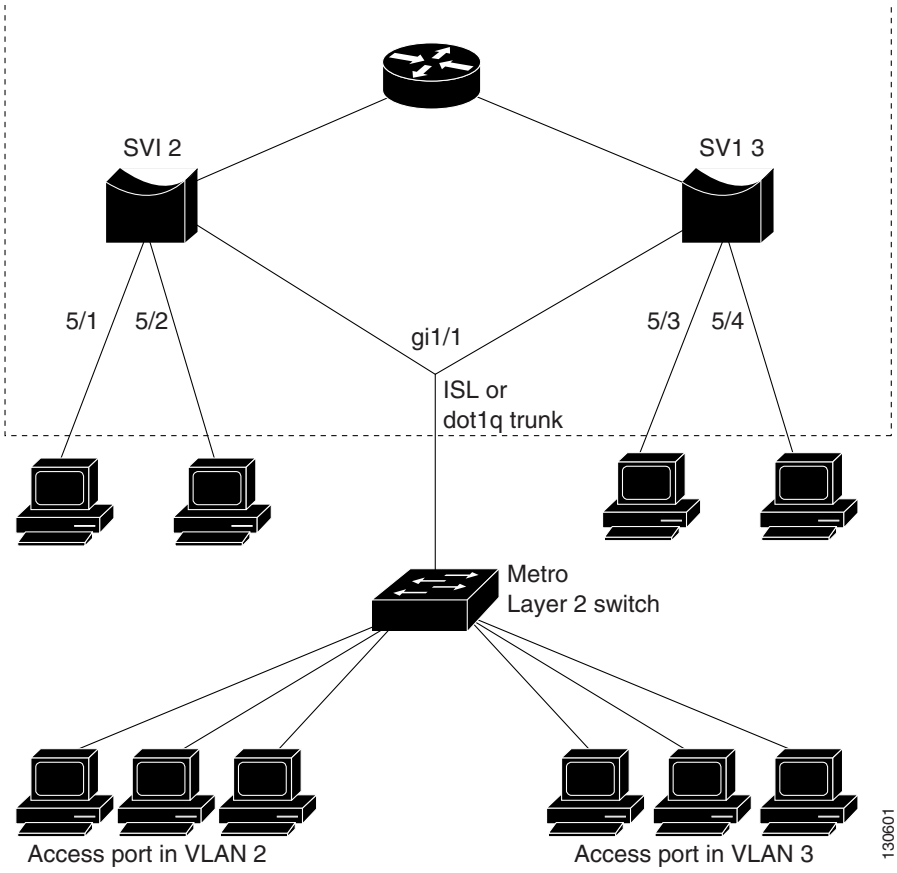
```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 10
Switch(config-if)# switchport 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 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 Trunk Port Security

Trunk port security extends port security to trunk ports. It restricts the allowed MAC addresses or the maximum number of MAC addresses to individual VLANs on a trunk port. Trunk port security enables service providers to block the access from a station with a different MAC address than the ones specified for that VLAN on that trunk port. When a trunk port security violation occurs, the trunk port is shut down and an SNMP trap may be generated. Trunk port security is also supported on private VLAN trunk ports.

Trunk port security is used when a Catalyst 4500 series switch has a dot1q or isl trunk attached to a neighborhood Layer 2 switch. This may be used, for example, in metro aggregation networks (Figure 30-1).

Figure 30-1 Trunk Port Security



You can configure various port security related parameters on a per-port per-VLAN basis.

To configure port security related parameters on a per-VLAN per-port basis, perform this task:

	Command	Purpose
Step 1	`Switch(config)# interface interface_id`	Enters interface configuration mode and specifies the physical interface to configure.
Step 2	`Switch(config-if)# switchport port-security maximum value vlan`	Configures a maximum number of secure mac-addresses for all the VLANs that are not explicitly configured for a maximum mac-address limit.
Step 3	`Switch(config-if)# vlan-range range`	Enters VLAN range sub-mode. **Note** You can specify single or multiple VLANs.
Step 4	`Switch(config-if-vlan-range)# port-security maximum value`	Configures a maximum number of secure MAC addresses for all the VLANs that have not been configured explicitly with a maximum value. If a maximum value is configured for a specific VLAN, it will overwrite the value specified by this CLI.

	Command	Purpose (continued)
Step 5	`Switch(config-if-vlan-range)#` **`no port-security maximum`**	Removes a maximum number of secure MAC addresses configuration for all the VLANs. Subsequently, the maximum value configured on the port will be used for all the VLANs.
Step 6	`Switch(config-if-vlan-range)#` [**no**] **port-security mac-address** *mac_address*	Configures a secure MAC-address on a specific VLAN range of VLANs.
Step 7	`Switch(config-if-vlan-range)#` [**no**] **port-security mac-address sticky** *mac_address*	Configures a sticky MAC-address on a specific VLAN range of VLANs.
Step 8	`Switch(config-if-vlan-range)#` **end**	Returns to interface configuration mode.
Step 9	`Switch(config-if)#` **end**	Returns to privileged EXEC mode.

This example shows how to configure a secure MAC-address and a maximum limit of secure MAC addresses on interface g1/1:

```
Switch(config)# interface g1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# sw mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 33
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# vlan 2-6
Switch(config-if-vlan-range)# port-security maximum 3
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.2
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.3
Switch(config-if-vlan-range)#

Switch# show port-security interface g1/1 vlan
Default maximum: not set, using 3072
VLAN  Maximum    Current
   2          3          3
   3          3          3
   4          3          3
   5          3          3
   6          3          3
Switch# show port-security interface g1/1 address vlan 2-4
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age
                                                              (mins)
----    -----------       ----                      -----   -------------
  2    0001.0001.0001    SecureConfigured          Gi1/1        -
  2    0001.0001.0002    SecureSticky              Gi1/1        -
  2    0001.0001.0003    SecureSticky              Gi1/1        -
  3    0001.0001.0001    SecureConfigured          Gi1/1        -
  3    0001.0001.0002    SecureSticky              Gi1/1        -
  3    0001.0001.0003    SecureSticky              Gi1/1        -
  4    0001.0001.0001    SecureConfigured          Gi1/1        -
  4    0001.0001.0002    SecureSticky              Gi1/1        -
  4    0001.0001.0003    SecureSticky              Gi1/1        -
------------------------------------------------------------------------
Total Addresses: 15

Switch#
```

Configuration guidelines

Follow these guidelines when configuring port security related parameters on a per-port per-VLAN basis:

- A secure MAC-address cannot be configured on a VLAN that is not allowed on a regular trunk port.
- For private-VLAN trunk ports, the VLAN on which the configuration is being performed must be in either the allowed VLAN list of the private VLAN trunk or the secondary VLAN list in the association pairs. (The CLI is rejected if this condition is not met.) The allowed VLAN list on a private VLAN trunk is intended to hold the VLAN-IDs of all the regular VLANs that are allowed on the private VLAN trunk.
- The configuration on the primary VLAN on the private VLAN trunk is not allowed. The CLI will be rejected and an error message is displayed.
- If a specific VLAN on a port is not configured with a maximum value, the maximum configured for the port is used for that VLAN. In this situation, the maximum number of addresses that can be secured on this VLAN is limited to the maximum value configured on the port.

  Each VLAN can be configured with a maximum count that is greater than the value configured on the port. Also, the sum of the maximum configured values for all the VLANs can exceed the maximum configured for the port. In either of these situations, the number of MAC addresses secured on each VLAN is limited to the lesser of the VLAN configuration maximum and the port configuration maximum.

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 interface_id`	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 aging_time | 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** *aging_tim*e keyword specifies the aging time for this port. Valid range for *aging_time* 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.

	Command	Purpose
Step 3	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 4	`Switch# show port security [interface interface_id] [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 interface_id]`	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 interface_id] address`	Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.
`Switch# show port-security [interface interface_id] vlan vlan_list`	Displays the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on a specific VLAN-list and a specific interface.
`Switch# show port-security [interface interface_id] [address [vlan vlan_list]]`	Displays all secure MAC addresses configured on a specific VLAN-list and a specific interface.

This example shows how to display port security settings for the entire switch:

```
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 shows how to display port security settings for interface Fast Ethernet 5/1:

```
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 shows how to display all secure MAC addresses configured on all switch interfaces:

```
Switch# show 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
```

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addressees on interface g1/1:

```
Switch# show port-security interface g1/1 vlan
Default maximum: 22
VLAN  Maximum    Current
    2         22          3
    3         22          3
    4         22          3
    5         22          1
    6         22          2
```

This example shows how to display the port security settings on interface g1/1 for VLANs 2 and 3:

```
Switch# show port-security interface g1/1 vlan 2-3
Default maximum: 22
VLAN  Maximum    Current
    2         22          3
    3         22          3
```

This example shows how to display all secure MAC addresses configured on interface g1/1 with aging information for each address.

```
Switch# show port-security interface g1/1 address

          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age(mins)
----    -----------                 ----                      -----   -------------
   2    0001.0001.0001    SecureConfigured         Gi1/1        -
   2    0001.0001.0002    SecureSticky                 Gi1/1        -
   2    0001.0001.0003    SecureSticky                 Gi1/1        -
   3    0001.0001.0001    SecureConfigured         Gi1/1        -
   3    0001.0001.0002    SecureSticky                 Gi1/1        -
   3    0001.0001.0003    SecureSticky                 Gi1/1        -
   4    0001.0001.0001    SecureConfigured         Gi1/1        -
   4    0001.0001.0002    SecureSticky             Gi1/1        -
   4    0001.0001.0003    SecureSticky             Gi1/1        -
   5    0001.0001.0001    SecureConfigured         Gi1/1        -
   6    0001.0001.0001    SecureConfigured         Gi1/1        -
   6    0001.0001.0002    SecureConfigured         Gi1/1        -
------------------------------------------------------------------------
Total Addresses: 12
```

This example shows how to display all secure MAC addresses configured on VLANs 2 and 3 on interface g1/1 with aging information for each address:

```
Switch# show port-security interface g1/1 address vlan 2-3

          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age(mins)
----    -----------       ----                      -----   -------------
   2    0001.0001.0001    SecureConfigured         Gi1/1        -
   2    0001.0001.0002    SecureSticky             Gi1/1        -
   2    0001.0001.0003    SecureSticky             Gi1/1        -
```

```
   3    0001.0001.0001    SecureConfigured         Gi1/1        -
   3    0001.0001.0002    SecureSticky             Gi1/1        -
   3    0001.0001.0003    SecureSticky             Gi1/1        -
------------------------------------------------------------------------
Total Addresses: 12
Switch#
```