Configuring Port Security

This chapter describes how to configure the port security feature. Release 12.1(13)E and later releases support the port security feature.

Note
For complete syntax and usage information for the commands used in this chapter, refer to the Catalyst 6500 Series Switch Cisco IOS Command Reference publication.

This chapter consists of these sections:
- Understanding Port Security, page 26-1
- Default Port Security Configuration, page 26-2
- Port Security Guidelines and Restrictions, page 26-2
- Configuring Port Security, page 26-2
- Displaying Port Security Settings, page 26-5

Understanding 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. If a workstation with a secure MAC that is address configured or learned on one secure port attempts to access another secure port, a violation is flagged.

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.
Default Port Security Configuration

Table 26-1 shows the default port security configuration for an interface.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port security</td>
<td>Disabled on a port</td>
</tr>
<tr>
<td>Maximum number of secure MAC addresses</td>
<td>1</td>
</tr>
<tr>
<td>Violation mode</td>
<td>Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.</td>
</tr>
</tbody>
</table>

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 cannot be an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

Configuring Port Security

These sections describe how to configure port security:

- Configuring Port Security on an Interface, page 26-3
- Configuring Port Security Aging, page 26-4
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router(config)# interface interface_id</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config-if)# switchport mode access</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-if)# switchport port-security</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config-if)# switchport port-security maximum value</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Router(config-if)# switchport port-security violation {protect</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Router(config-if)# switchport port-security mac-address mac_address</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Router(config-if)# end</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Router# show port-security interface interface_id</td>
</tr>
</tbody>
</table>

When configuring port security, note the following syntax information about port security violation modes:

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

**Note**

When port security is enabled, if an address learned or configured on one secure interface is seen on another secure interface in the same VLAN, port security puts the interface into the error-disabled state immediately.

To bring a secure port out of the error-disabled state, enter the **errdisable recovery cause psecure_violation** global configuration command or you can manually reenable it by entering the **shutdown** and **no shutdown** interface configuration commands.
To return the interface to the default condition (not a secure port), enter the `no switchport port-security` interface configuration command.

To return the interface to the default number of secure MAC addresses, enter the `no switchport port-security maximum value` command.

To delete a MAC address from the address table, enter the `no switchport port-security mac-address mac_address` command.

To return the violation mode to the default condition (shutdown mode), enter the `no switchport port-security violation {protocol | restrict}` command.

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

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# switchport port-security maximum 5
Router(config-if)# end
```

```
Router# show port-security interface fastethernet 3/12
Security Enabled:Yes, Port Status:SecureUp
Violation Mode:Shutdown
Max. Addrs:5, Current Addrs:0, Configure Addrs:0
```

This example shows how to configure a secure MAC address on Fast Ethernet port 12 and verify the configuration:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
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     Fa5/12
```

**Configuring Port Security Aging**

You can use port security aging to set the aging time 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router(config)# interface interface_id</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config-if)# switchport port-security aging time aging_time</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# no switchport port-security aging time</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-if)# end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router# show port security [interface interface_id] [address]</td>
</tr>
</tbody>
</table>

When configuring port security aging, note the following:

- With all releases, you can enter the no keyword to disable aging.
- For Release 12.1(19)E and later releases, the valid aging-time range is from 1 to 1440 minutes.
- For releases earlier than Release 12.1(19)E, the valid aging-time range is from 0 to 1440 minutes. You can enter zero to disable aging.

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

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

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

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

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

### Displaying Port Security Settings

The `show interfaces interface_id switchport` privileged EXEC command displays the interface traffic suppression and control configuration. The `show interfaces counters` privileged EXEC commands display the count of discarded packets. The `show storm control` and `show port-security` privileged EXEC commands display those features.
Chapter 26  Configuring Port Security

To display traffic control information, enter one or more of these commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# <code>show port-security [interface interface_id]</code></td>
<td>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.</td>
</tr>
<tr>
<td>Router# <code>show port-security [interface interface_id] address</code></td>
<td>Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.</td>
</tr>
</tbody>
</table>

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)        ------------------------------------------
Fa5/1           11            11            0            Shutdown
Fa5/5           15            5             0            Restrict
Fa5/11          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 fastethernet 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 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 Fa5/1      15 (I)
1  0001.0001.0002 SecureDynamic Fa5/1      15 (I)
1  0001.0001.1111 SecureConfigured Fa5/1     16 (I)
1  0001.0001.1112 SecureConfigured Fa5/1   -
1  0001.0001.1113 SecureConfigured Fa5/1   -
1  0005.0005.0001 SecureConfigured Fa5/5     23
1  0005.0005.0002 SecureConfigured Fa5/5     23
1  0005.0005.0003 SecureConfigured Fa5/5     23
1  0011.0011.0001 SecureConfigured Fa5/11    25 (I)
1  0011.0011.0002 SecureConfigured Fa5/11    25 (I)

Total Addresses in System: 10
Max Addresses limit in System: 128
```