



Configuring Port Security

This chapter describes how to configure port security on the Catalyst 6500 series switches.



Note

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



Note

See [Chapter 36, “Configuring 802.1x Authentication”](#) for information on configuring 802.1x authentication to restrict unauthorized devices from connecting to a LAN through publicly accessible ports.



Note

See [Chapter 21, “Configuring the Switch Access Using AAA”](#) for information on configuring authentication, authorization, and accounting (AAA) to monitor and control access to the command-line interface (CLI) on the Catalyst 6500 series switches.

This chapter consists of these major sections:

- [Understanding How Port Security Works, page 35-1](#)
- [Port Security Configuration Guidelines, page 35-3](#)
- [Configuring Port Security on the Switch, page 35-3](#)

Understanding How Port Security Works

You can use port security to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses that are specified for that port. Alternatively, you can use port security to filter traffic destined to or received from a specific host based on the host MAC address.

These sections describe the traffic filtering methods:

- [Allowing Traffic Based on the Host MAC Address, page 35-2](#)
- [Restricting Traffic Based on the Host MAC Address, page 35-3](#)
- [Blocking Unicast Flood Packets on Secure Ports, page 35-3](#)

Allowing Traffic Based on the Host MAC Address

The total number of MAC addresses that you can specify per port is limited to the global resource of 1024 plus 1 default MAC address. The total number of MAC addresses on any port cannot exceed 1025.

Whether you allocate the maximum number of MAC addresses for each port depends on your network configuration. These combinations are examples of valid allocations:

- 1025 (1 + 1024) addresses on 1 port and 1 address each on the rest of the ports.
- 513 (1 + 512) each on 2 ports in a system and 1 address each on the rest of the ports.
- 901 (1 + 900) on one port, 101 (1 + 100) on another port, 25 (1 + 24) on the third port, and 1 address each on the rest of the ports.

After you allocate the maximum number of MAC addresses on a port, you can either specify the secure MAC address for the port manually or you can have the port dynamically configure the MAC address of the connected devices. Out of an allocated number of maximum MAC addresses on a port, you can manually configure all, allow all to be autoconfigured, or configure some manually and allow the rest to be autoconfigured. Once you manually configure or autoconfigure the addresses, the addresses are stored in nonvolatile RAM (NVRAM) and maintained after a reset.

After you allocate a maximum number of MAC addresses on a port, you can specify how long the addresses on the port will remain secure. After the age time expires, the MAC addresses on the port become insecure. By default, all addresses on a port are secured permanently.

If a security violation occurs, you can configure the port to go into shutdown mode or restrictive mode. The shutdown mode option allows you to specify whether the port is to be permanently disabled or disabled for only a specified time. The default is for the port to shut down permanently. The restrictive mode allows you to configure the port to remain enabled during a security violation and drop only the packets that are coming in from insecure hosts.

**Note**

If you configure a secure port in restrictive mode, and a station is connected to the port whose MAC address is already configured as a secure MAC address on another port on the switch, the port in restrictive mode shuts down instead of restricting traffic from that station. For example, if you configure MAC-1 as the secure MAC address on port 2/1 and MAC-2 as the secure MAC address on port 2/2 and then connect the station with MAC-1 to port 2/2 when port 2/2 is configured for restrictive mode, port 2/2 shuts down instead of restricting traffic from MAC-1.

When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device that is attached to the port differs from the list of secure addresses, the port either shuts down permanently (default mode), shuts down for the time that you have specified, or drops incoming packets from the insecure host. The port's behavior depends on how you configure it to respond to a security violation.

If a security violation occurs, the LED labeled "Link" for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol (SNMP) manager. An SNMP trap is not sent if you configure the port for restrictive violation mode. A trap is sent only if you configure the port to shut down during a security violation.

Restricting Traffic Based on the Host MAC Address

You can filter traffic based on a host MAC address so that packets that are tagged with a specific source MAC address are discarded. When you specify a MAC address filter with the **set cam filter** command, incoming traffic from that host MAC address is dropped and the packets that are addressed to that host are not forwarded.

**Note**

The **set cam filter** command allows filtering for unicast addresses only. You cannot filter traffic for multicast addresses with this command.

Blocking Unicast Flood Packets on Secure Ports

You can block unicast flood packets on a secure Ethernet port by disabling the unicast flood feature. If you disable unicast flood on a port, the port will drop unicast flood packets when it reaches the allowed maximum number of MAC addresses.

The port automatically restarts unicast flood packet learning when the number of MAC addresses drops below the maximum number that is allowed. The learned MAC address count decreases when a configured MAC address is removed or a time to live counter (TTL) is reached.

Port Security Configuration Guidelines

This section describes the guidelines for configuring port security:

- Do not configure port security on a trunk port.
- Do not enable port security on a SPAN destination port and vice versa.
- Do not configure dynamic, static, or permanent CAM entries on a secure port.

Configuring Port Security on the Switch

These sections describe how to configure port security:

- [Enabling Port Security, page 35-4](#)
- [Setting the Maximum Number of Secure MAC Addresses, page 35-5](#)
- [Automatically Configuring Dynamically Learned MAC Addresses, page 35-5](#)
- [Setting the Port Security Age Time, page 35-6](#)
- [Clearing MAC Addresses, page 35-7](#)
- [Configuring Unicast Flood Blocking on Secure Ports, page 35-7](#)
- [Specifying the Security Violation Action, page 35-8](#)
- [Setting the Shutdown Timeout, page 35-9](#)
- [Disabling Port Security, page 35-9](#)
- [Restricting Traffic Based on a Host MAC Address, page 35-10](#)
- [Displaying Port Security, page 35-10](#)

Enabling Port Security

Port security is either autoconfigured or enabled manually by specifying a MAC address. If a MAC address is not specified, the source address from the incoming traffic is autoconfigured and secured, up to the maximum number of MAC addresses allowed. These autoconfigured MAC Addresses remain secured for a time, depending upon the aging timer set. The autoconfigured MAC Addresses are cleared from the port in case of a link-down event.

When you enable port security on a port, any static or dynamic CAM entries that are associated with the port are cleared; any currently configured permanent CAM entries are treated as secure.

To enable port security, perform this task in privileged mode:

	Task	Command
Step 1	Enable port security on the desired ports. If desired, specify the secure MAC address.	set port security <i>mod/port</i> enable [<i>mac_addr</i>]
Step 2	You can add MAC addresses to the list of secure addresses.	set port security <i>mod/port</i> <i>mac_addr</i>
Step 3	Verify the configuration.	show port [<i>mod[/port]</i>]

This example shows how to enable port security using the learned MAC address on a port and verify the configuration:

```

Console> (enable) set port security 2/1 enable
Port 2/1 port security enabled with the learned mac address.
Trunking disabled for Port 2/1 due to Security Mode
Console> (enable) show port 2/1
Port Name                Status      Vlan      Level Duplex Speed Type
-----
2/1                      connected  522      normal half   100 100BaseTX

Port Security Secure-Src-Addr Last-Src-Addr Shutdown Trap IfIndex
-----
2/1 enabled  00-90-2b-03-34-08 00-90-2b-03-34-08 No disabled 1081

Port Broadcast-Limit Broadcast-Drop
-----
2/1 - 0

Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize
-----
2/1 0 0 0 0 0

Port Single-Col Multi-Coll Late-Coll Excess-Col Carri-Sen Runts Giants
-----
2/1 0 0 0 0 0 0 0

Last-Time-Cleared
-----
Fri Jul 10 1998, 17:53:38

```

This example shows how to enable port security on a port and manually specify the secure MAC address:

```

Console> (enable) set port security 2/1 enable 00-90-2b-03-34-08
Port 2/1 port security enabled with 00-90-2b-03-34-08 as the secure mac address
Trunking disabled for Port 2/1 due to Security Mode
Console> (enable)

```

Setting the Maximum Number of Secure MAC Addresses

You can set the number of MAC addresses to secure on a port. By default, at least one MAC address per port can be secured. In addition to this default, a global resource of up to 1024 MAC addresses is available to be shared by the ports. If the entire global resource of 1024 MAC addresses is used on some ports, you can still enable port security on the rest of the ports with a maximum of one MAC per port.

If you reduce the maximum number of MAC addresses, the system clears the specified number of MAC addresses and displays the list of removed addresses.

To set a number of MAC addresses to be secured for a particular port, perform this task in privileged mode:

Task	Command
Set the number of MAC addresses to be secured on a port.	set port security <i>mod/port</i> maximum <i>num_of_mac</i>

This example shows how to set the number of MAC addresses to be secured:

```
Console> (enable) set port security 7/7 maximum 20
Maximum number of secure addresses set to 20 for port 7/7.
Console> (enable)
```

This example shows how to reduce the number of MAC addresses and the list that displays the cleared MAC addresses:

```
Console> (enable) set port security 7/7 maximum 18
Maximum number of secure addresses set to 18 for port 7/7
00-11-22-33-44-55 cleared from secure address list for port 7/7
00-11-22-33-44-66 cleared from secure address list for port 7/7
Console> (enable)
```

Automatically Configuring Dynamically Learned MAC Addresses

Automatic configuration of dynamically learned MAC addresses enables dynamically learned MAC addresses to be associated with particular ports. This feature applies globally to all secure ports on the system.

The dynamically learned addresses are treated like manually configured addresses and the configuration is stored in NVRAM. The addresses are retained in the event that a secure port is shut down due to a security violation, port security is disabled, or a secure port is administratively disabled.



Note

Dynamically learned addresses that have been configured using the automatic configuration option are not cleared under any circumstances. These addresses must be cleared manually using the **clear port security** command.

To enable automatic configuration of dynamically learned MAC addresses, perform the following task in privileged mode:

Task	Command
Enable automatic configuration of dynamically learned MAC addresses.	set port security auto-configure enable disable

This example shows how to enable automatic configuration of dynamically learned MAC addresses globally on the switch:

```
Console> (enable) set port security auto-configure enable
Automatic configuration of secure learnt addresses enabled.
Console> (enable)
```

To view the automatic configuration, use the **show port security statistics system** command.

```
Console> (enable) show port security statistics system

Auto-Configure Option: Enabled
Module 2:
  Total ports: 24
  Total secure ports: 0
  Total MAC addresses: 24
  Total global address space used (out of 4096): 0
  Status: installed
Module 3:
  Total ports: 48
  Total secure ports: 0
  Total MAC addresses: 48
  Total global address space used (out of 4096): 0
  Status: installed
Module 5:
  Total ports: 2
  Total secure ports: 0
  Total MAC addresses: 2
  Total global address space used (out of 4096): 0
  Status: installed
Total secure ports in the system: 0
Total secure MAC addresses in the system: 74
Total global MAC address resource used in the system (out of 4096): 0
Console> (enable)
```

Setting the Port Security Age Time

The age time on a port specifies how long all addresses on that port will be secured. This age time is activated when a MAC address initiates traffic on the port. After the age time expires for a MAC address, the entry for that MAC address on the port is removed from the secure address list. The valid range is from 1–1440 minutes. Setting the age time to zero disables the aging of secure addresses.

To set the age time on a port, perform this task in privileged mode:

Task	Command
Set the age time for which addresses on a port will be secured.	set port security mod/port age time

This example shows how to set the age time on port 7/7:

```
Console> (enable) set port security 7/7 age 600
Secure address age time set to 600 minutes for port 7/7.
Console> (enable)
```

Clearing MAC Addresses

Enter the **clear port security** command to clear MAC addresses from a list of secure addresses on a port.



Note

If you execute the **clear** command on a MAC address that is in use, that MAC address may be learned and made secure again. We recommend that you disable port security before you clear MAC addresses.

To clear all or a particular MAC address from the list of secure MAC addresses, perform this task in privileged mode:

Task	Command
Clear all or a particular MAC address from the list of secure MAC addresses.	clear port security <i>mod/port</i> { <i>mac_addr</i> all }

This example shows how to clear one MAC address from the secure address list on port 7/7:

```
Console> (enable) clear port security 7/7 00-11-22-33-44-55
00-11-22-33-44-55 cleared from secure address list for port 7/7
Console> (enable)
```

This example shows how to clear all MAC addresses from ports 7/5-7:

```
Console> (enable) clear port security 7/5-7 all
All addresses cleared from secure address list for ports 7/5-7
Console> (enable)
```

Configuring Unicast Flood Blocking on Secure Ports

To configure unicast flood blocking, you must disable the unicast flood feature.



Note

The port disables unicast flooding once the MAC address limit is reached.

To configure unicast flood blocking on a secure port, perform this procedure in privileged mode:

	Task	Command
Step 1	Disable unicast flood blocking on the desired secure ports.	set port security <i>mod/port</i> unicast-flood disable
Step 2	Verify the configuration of unicast flood.	show port security <i>mod/port</i>
Step 3	Verify the status of unicast flood blocking.	show port unicast-flood <i>mod/port</i>

This example shows how to configure the switch to disable unicast flood packets on a port and how to verify its configuration:

```

Console> (enable) set port security 4/1 unicast-flood disable
Port 4/1 security flood mode set to disable.
Console> (enable) show port security 4/1
Port Security Violation Shutdown-Time Age-Time Max-Addr Trap IfIndex
-----
4/1 disabled shutdown 0 0 1 disabled 50

Port Num-Addr Secure-Src-Addr Age-Left Last-Src-Addr Shutdown/Time-Left
-----
4/1 0 - - - -

Port Flooding on Address Limit
-----
4/1 Disabled
Console> (enable) show port unicast-flood 4/1
Port Unicast Flooding
----
4/1 Disabled
Console> (enable)

```

**Note**

The **show port unicast-flood** command displays the run-time status of unicast flood blocking. The output can show unicast flooding as either enabled or disabled depending if the port has exceeded its address limitation.

Specifying the Security Violation Action

You can set the port for the following two modes to handle a security violation:

- **Shutdown**—Shuts down the port permanently or for a specified time. Permanent shutdown is the default mode.
- **Restrictive**—Drops all packets from the insecure hosts but remains enabled.

To specify the security violation action to be taken, perform this task in privileged mode:

Task	Command
Specify the violation action on a port.	set port security <i>mod/port</i> violation {shutdown restrict}

This example shows how to specify that port 7/7 drop all packets from insecure hosts:

```

Console> (enable) set port security 7/7 violation restrict
Port security violation on port 7/7 will cause insecure packets to be dropped.
Console> (enable)

```

**Note**

If you restrict the number of secure MAC addresses on a port to one and additional hosts attempt to connect to that port, port security prevents these additional hosts from connecting to that port and to any other port in the same VLAN for the duration of the VLAN aging time. By default, the VLAN aging time is 5 minutes. If a host is blocked from joining a port in the same VLAN as the secured port, allow the VLAN aging time to expire before you attempt to connect the host to the port again.

Setting the Shutdown Timeout

You can set the time a port remains disabled in case of a security violation. By default, the port is shut down permanently. The valid range is from 1–1440 minutes.

If the time is set to zero, the shutdown is disabled for this port.



Note

When the shutdown timeout expires, the port is reenabled and all port security-related configuration is maintained.

To set the shutdown timeout, perform this task in privileged mode:

Task	Command
Set the shutdown timeout on a port.	set port security <i>mod/port</i> shutdown <i>time</i>

This example shows how to set the shutdown timeout to 600 minutes on port 7/7:

```
Console> (enable) set port security 7/7 shutdown 600
Secure address shutdown time set to 600 minutes for port 7/7.
Console> (enable)
```

Disabling Port Security

To disable port security, perform this task in privileged mode:

	Task	Command
Step 1	Disable port security on the desired ports.	set port security <i>mod/port</i> disable
Step 2	Verify the configuration.	show port security [<i>mod/port</i>]

This example shows how to disable port security:

```
Console> (enable) set port security 2/1 disable
Port 2/1 port security disabled.
Console> (enable)
Console> (enable) show port security 2/1
Port Security Violation Shutdown-Time Age-Time Max-Addr Trap IfIndex
-----
3/24 disabled restrict 20 300 10 disabled 921

Port Num-Addr Secure-Src-Addr Age-Left Last-Src-Addr Shutdown/Time-Left
-----
3/24 1 00-e0-4f-ac-b4-00 - - -
Console> (enable)
```

Restricting Traffic Based on a Host MAC Address

To restrict traffic for a specific MAC address, perform this task in privileged mode:

	Task	Command
Step 1	Restrict traffic destined to or originating from a specific MAC address.	set cam {static permanent} filter <i>unicast_mac vlan</i>
Step 2	Remove the filter.	clear cam <i>mac_address vlan</i>
Step 3	Verify the configuration.	show cam {static permanent}

This example shows how to create a filter that restricts traffic for a specific MAC address:

```
Console> (enable) set cam static filter 00-02-03-04-05-06 1
Filter entry added to CAM table.
Console> (enable)
```

This example shows how to clear the filter:

```
Console> (enable) clear cam 00-02-03-04-05-06 1
CAM entry cleared.
Console> (enable)
```

This example shows how to display the static CAM entries:

```
Console> show cam static

VLAN  Dest MAC/Route Des      [CoS]  Destination Ports or VCs / [Protocol Type]
-----
3      04-04-05-06-07-08  *      FILTER
```

Displaying Port Security

The **show port security** command displays the following information:

- List of secure MAC addresses for a port
- Maximum number of secure addresses that are allowed on a port
- Total number of secure MAC addresses
- Age
- Age left and shutdown timeout left
- Shutdown/security mode
- Statistics that are related to port security

To display the port security configuration information and statistics, perform this task in privileged mode:

	Task	Command
Step 1	Display the configuration.	show port security [statistics] <i>mod/port</i>
Step 2	Display the port security statistics.	show port security statistics [system] <i>[mod/port]</i>

This example shows how to display the port security configuration information and statistics:

```

Console> (enable) show port security 3/24
Port Security Violation Shutdown-Time Age-Time Max-Addr Trap IfIndex
-----
3/24 enabled shutdown 300 60 10 disabled 921

Port Num-Addr Secure-Src-Addr Age-Left Last-Src-Addr Shutdown/Time-Left
-----
3/24 4 00-e0-4f-ac-b4-00 60 00-e0-4f-ac-b4-00 no -
      00-11-22-33-44-55 0
      00-11-22-33-44-66 0
      00-11-22-33-44-77 0

Console> (enable) show port security statistics 3/24
Port Total-Addrs Maximum-Addrs
-----
3/24 4 10
Console> (enable)
Port Total-Addrs Maximum-Addrs
-----
3/24 1 10
Console> (enable)

```

This example shows how to display the port security statistics on a module:

```

Console> (enable) show port security statistics 7
Port Total-Addrs Maximum-Addrs
-----
7/1 0 1
7/2 0 1
7/3 0 1
7/4 0 1
7/5 0 1
7/6 0 1
7/7 0 1
7/8 0 1
7/9 0 1
7/10 0 200
7/11 0 1
7/12 0 1
7/13 0 1
7/14 0 1
7/15 0 1
7/16 0 1
7/17 0 1
7/18 0 1
7/19 0 1
7/20 0 1
7/21 0 1
7/22 0 1
7/23 0 1
7/24 0 1

Module 7:
  Total ports: 24
  Total MAC address(es): 223
  Total global address space used (out of 1024): 199
  Status: installed
Console> (enable)

```

This example shows how to display the port security statistics on the system:

```
Console> (enable) show port security statistics system
Module 1:
  Total ports: 2
  Total MAC address(es): 2
  Total global address space used (out of 1024): 0
  Status: installed
Module 3:
  Module does not support port security feature
Module 6:
  Total ports: 48
  Total MAC address(es): 48
  Total global address space used (out of 1024): 0
  Status: installed
Module 7:
  Total ports: 24
  Total MAC address(es): 223
  Total global address space used (out of 1024): 199
  Status: installed
Console> (enable)
```