



Configuring Port Security

This chapter describes how to configure port security on the Catalyst enterprise LAN switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*.

This chapter consists of these major sections:

- [Understanding How Port Security Works, page 16-1](#)
- [Port Security Configuration Guidelines, page 16-3](#)
- [Configuring Port Security, page 16-3](#)
- [Monitoring Port Security, page 16-10](#)

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 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.

The next two sections describe the traffic filtering methods.

Allowing Traffic Based on the Host MAC Address

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

The maximum number of MAC addresses you can allocate for each port depends on your network configuration. The following combinations are valid allocations:

- 1025 (1 + 1024) addresses on one port and 1 address each on the rest of the ports
- 513 (1 + 512) each on two 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 a third port, and 1 address on each of 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 have the port dynamically configure the MAC address of the connected devices. Out of a maximum allocated number of 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, they are stored in nonvolatile RAM (NVRAM) and are maintained after a reset.

When you manually change the maximum number of MAC addresses associated to a port greater than the default value and then manually enter the authorized MAC addresses, any remaining MAC addresses automatically configured. For example, if you configure the port security for a port to have a maximum of ten MAC addresses but add only two MAC addresses, the next eight new source MAC addresses received on that port are added to the secured MAC address list for the port.

After you allocate a maximum number of MAC addresses on a port, you can also 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 either 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 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 attached to the port differs from the list of secure addresses, the port either shuts down permanently (default mode), shuts down for the time you have specified, or drops incoming packets from the insecure host.

The behavior of a port 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 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 packets addressed to that host are not forwarded. You cannot filter traffic for multicast addresses with this command.

**Note**

The **set cam filter** command allows filtering for unicast addresses only.

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 the port 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 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 lists guidelines for configuring port security:

- Do not configure port security on a SPAN destination port.
- Do not configure SPAN destination on a secure port.
- Do not configure dynamic, static, or permanent CAM entries on a secure port.

Configuring Port Security

These sections describe how to configure port security:

- [Enabling Port Security, page 16-3](#)
- [Specifying the Maximum Number of Secure MAC Addresses, page 16-4](#)
- [Specifying the Port Security Age Time, page 16-5](#)
- [Clearing MAC Addresses, page 16-5](#)
- [Enabling Unicast Flood Blocking on Secure Ports, page 16-6](#)
- [Enabling MAC Address Notification, page 16-7](#)
- [Specifying Security Violation Action, page 16-8](#)
- [Specifying the Shutdown Time, page 16-9](#)
- [Disabling Port Security, page 16-9](#)
- [Restricting Traffic for a Host MAC Address, page 16-10](#)

Enabling Port Security

When you enable port security on a port, any static or dynamic CAM entries 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_num/port_num</i> enable [<i>mac_addr</i>]
Step 2	You can add MAC addresses to the list of secure addresses.	set port security <i>mod_num/port_num</i> <i>mac_addr</i>
Step 3	Verify the configuration.	show port [<i>mod_num</i> [/ <i>port_num</i>]]

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

```
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
```

This example shows how to verify the port security:

```
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)
```

Specifying the Maximum Number of Secure MAC Addresses

You can specify 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. This means that 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_num/port_num maximum num_of_mac</i>

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

```
Console> (enable) set port security 4/7 maximum 20
Maximum number of secure addresses set to 20 for port 4/7.
Console> (enable)
```

This example shows how to reduce the number of MAC addresses; it also shows how to display the list of cleared MAC addresses:

```
Console> (enable) set port security 4/7 maximum 18
Maximum number of secure addresses set to 18 for port 4/7
00-11-22-33-44-55 cleared from secure address list for port 4/7
00-11-22-33-44-66 cleared from secure address list for port 4/7
Console> (enable)
```

Specifying 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 to 1440 minutes. Setting the age time to zero disables 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 <i>mod_num/port_num age time</i>

```
Console> (enable) set port security 4/7 age 600
Secure address age time set to 600 minutes for port 4/7.
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 use the **clear** command on a MAC address that is in use, the network may relearn that MAC address and make the MAC address secure again. We recommend that you disable port security before you clear MAC addresses.

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

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

This example removes one MAC address from the secure address list on port 4/7:

```
Console> (enable) clear port security 4/7 00-11-22-33-44-55
00-11-22-33-44-55 cleared from secure address list for port 4/7
Console> (enable)
```

This example removes all MAC addresses from ports 4/5–7:

```
Console> (enable) clear port security 4/5-7 all
All addresses cleared from secure address list for ports 4/5-7
Console> (enable)
```

Enabling 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 task 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 blocking.	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 upon if the port has exceeded its address limitation.

Enabling MAC Address Notification

Enabling MAC address notification allows you to monitor MAC addresses at the module and port level that were added by the switch or removed from the CAM table.

A new MAC address is added when either of the following occurs:

- When a packet is received from a new device on one of the ports of the switch with a new source address
- When the MAC address is added to the CAM table by the CLI

A MAC address is removed from the CAM table when one of the following is true:

- When the MAC address receives no packets during the time-out period
- When the switch invalidates a CAM table entry and replaces the entry with a new one
- When the MAC address is removed from the CAM table by the CLI

**Note**

MAC address notification settings are ignored on PAgP and LACP EtherChannel ports.

To enable MAC address notification globally, perform this task in privileged mode:

	Task	Command
Step 1	Enable MAC address notification globally.	set cam notification {enable disable}
Step 2	Set the history log size.	set cam notification historysize <i>log_size</i>
Step 3	Enable notification of added MAC addresses.	set cam notification added {enable disable} <i>mod/port</i>
Step 4	Enable notification of removed MAC addresses.	set cam notification removed {enable disable} <i>mod/port</i>
Step 5	Verify the configuration.	show cam notification all

MAC addresses are stored in memory between notifications. To set the interval time between notifications and verify the configuration, perform this task in privileged mode:

	Task	Command
Step 1	Set the interval time between notifications.	set cam notification interval <i>time</i>
Step 2	Verify the configuration.	show cam notification all

If the **set cam notification interval** is set to 0, the switch will send notification immediately. If the notifications are sent immediately, they will have an impact on the performance of the switch.

You can generate SNMP traps whenever a MAC address change occurs; do so by enabling the commands **set snmp trap enable macnotification**, **set cam notification**, and **set cam notification historysize**.

To set the SNMP trap MAC address notification, perform this task in privileged mode:

Task	Command
Set the SNMP traps on the system.	set snmp trap enable macnotification

This example shows how to enable MAC address notification globally, how to enable notification of added and removed MAC addresses, and how to set interval time between notifications:

```

Console> (enable) set cam notification enable
MAC address change detection globally enabled
Be sure to specify which ports are to detect MAC address changes
with the 'set cam notification [added|removed] enable <m/p>' command.
SNMP traps will be sent if 'set snmp trap enable macnotification' has been set.
Console> (enable) set cam notification historysize 300
MAC address change history log size set to 300 entries
Console> (enable) set cam notification added enable 3/1-4
MAC address change notifications for added addresses are
enabled on port(s) 3/1-4
Console> (enable) set cam notification removed enable 3/3-6
MAC address change notifications for removed addresses are
enabled on port(s) 3/3-6
Console> (enable) set cam notification interval 10
MAC address change notification interval set to 10 seconds
Console> (enable) show cam notification all
MAC address change detection enabled
CAM notification interval = 10 second(s).
MAC address change history log size = 300
MAC addresses added = 3
MAC addresses removed = 5
MAC addresses added overflowed = 0
MAC addresses removed overflowed = 0
MAC address SNMP traps generated = 0
Console> (enable) set snmp trap enable macnotification
SNMP MAC notification trap enabled.
Console> (enable)

```

Specifying Security Violation Action

You can set a port to 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.
- **Restrict**—Drops all packets from insecure hosts, but remains enabled.

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

Task	Command
Set the security violation action on a port.	set port security mod_num/port_num violation {shutdown restrict}

This example sets the port to drop all packets that are coming in on the port from insecure hosts:

```
Console> (enable) set port security 4/7 violation restrict
Port security violation on port 4/7 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 being connected to that port as well as to any other port in the same VLAN for the duration of the VLAN aging time. By default, the VLAN aging time is five 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.

Specifying the Shutdown Time

You can specify how long a port is to remain disabled in the event of a security violation. By default, the port is shut down permanently. The valid range is from 1 to 1440 minutes.

If you set the time 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_num/port_num</i> <i>shutdown time</i>

This example shows how to set the shutdown time to 600 minutes on port 4/7:

```
Console> (enable) set port security 4/7 shutdown 600
Secure address shutdown time set to 600 minutes for port 4/7.
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_num/port_num</i> disable
Step 2	Verify the configuration.	show port security [<i>mod_num/port_num</i>]

This example shows how to disable security on a port:

```
Console> (enable) set port security 2/1 disable
Port 2/1 port security disabled.
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 for a Host MAC Address

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

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

This example shows how to create a filter 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
Console> (enable)

```

Monitoring Port Security

You can view the following port security information:

- List of secure MAC addresses for a port
- Maximum number of secure addresses allowed on a port
- Total number of secure MAC addresses
- Age and shutdown timeout
- Shutdown and security mode

- Statistics data related to port security

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

	Task	Command
Step 1	Display the configuration.	show port security [statistics] mod_num/port_num
Step 2	Display the port security statistics.	show port security [statistics] [system] [mod_num/port_num]

These examples show how to display 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 port security statistics on a module:

```

Console> (enable) show port security statistics 3
Port  Total-Addrs Maximum-Addrs
-----
3/1          0             1
3/2          0             1
3/3          0             1
3/4          0             1
3/5          0             1
3/6          0             1
Module 3:
  Total ports: 6
  Total secure ports: 0
  Total MAC addresses: 6
  Total global address space used (out of 1024): 0
  Status: installed
Console> (enable)

```

This example shows how to display 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
Console> (enable)

```