



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 *Catalyst 5000 Family Command Reference*.

This chapter consists of these sections:

- [Understanding How Port Security Works, page 18-1](#)
- [Port Security Configuration Guidelines, page 18-3](#)
- [Configuring Port Security, page 18-3](#)

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 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.

This section describes the following traffic filtering methods:

- [Allowing Traffic Based on the Host MAC Address, page 18-1](#)
- [Restricting Traffic Based on the Host MAC Address, page 18-2](#)

Allowing Traffic Based on the Host MAC Address

The global resource for the system is 1024 MAC addresses. Space also exists for one default MAC address per port to be secured. The total number of MAC addresses that can be specified per port is limited to the global resource of 1024 plus one default MAC address. The total number of MAC addresses on any port cannot exceed 1025.

Allocation of the maximum number of MAC addresses for each port depends on your network configuration. The following combinations are examples of valid allocations:

- 1025 (1+1024) addresses on one 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 specify that the port dynamically configure the MAC address of the connected devices. From 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. After addresses are manually configured or autoconfigured, they are stored in non-volatile RAM (NVRAM) and maintained after a reset.

After you allocate a maximum number of MAC addresses on a port, you can specify an age time during which addresses on the specified 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.

In the event of a security violation, you can configure the port to go into shutdown mode or restrictive mode. You can configure the shutdown mode to specify whether the port will be permanently disabled or disabled for only a specified time. The default behavior during a security violation 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 will shut 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 will shut 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 the port depends on how you configure the port to respond to a security violation.

When a security violation occurs, the Link LED for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol (SNMP) manager. An SNMP trap will not be sent if you have configured 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 that 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.

**Note**

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

Port Security Configuration Guidelines

Follow these guidelines when configuring port security:

- You cannot configure port security on the three-port Gigabit Ethernet module (WS-X5403).
- You cannot configure port security on a SPAN destination port and vice versa.
- You cannot configure dynamic, static, or permanent CAM entries on a secure port.
- 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.

Configuring Port Security

These sections describe how to configure port security:

- [Enabling Port Security, page 18-3](#)
- [Specifying the Maximum Number of Secure MAC Addresses, page 18-4](#)
- [Specifying the Port Security Age Time, page 18-5](#)
- [Clearing MAC Addresses, page 18-5](#)
- [Specifying Security Violation Action, page 18-6](#)
- [Specifying Shutdown Time, page 18-6](#)
- [Disabling Port Security, page 18-7](#)
- [Restricting Traffic Based on Host MAC Address, page 18-7](#)
- [Monitoring Port Security, page 18-8](#)

Enabling Port Security

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
Console> (enable)

```

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/port maximum 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)
```

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 10 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 mod/port age time

```
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

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



Note

If the **clear** command is executed on a MAC address that is in use, that MAC address may be learned and made secure again. For this reason 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 mod/port {mac_addr all}

This example removes 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 removes 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)
```

Specifying Security Violation Action

The port can be set 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.
- 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 violation action on a port.	set port security mod/port 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 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 blocks 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 Shutdown Time

You can specify how long a port remains disabled in case of a security violation. By default, the port is shut down permanently. The valid range is 10 to 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 configurations are 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 sets the shutdown time 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 security on a port:

```
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 Host MAC Address

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

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

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
```

Monitoring Port Security

You can view the following information about a port:

- List of secure MAC addresses for a port
- Maximum number of secure addresses allowed on a port
- Total number of secure MAC addresses
- Age
- Age left and shutdown timeout left
- 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/port
Step 2	Display the port security statistics.	show port security statistics [system] [mod/port]

This example shows 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 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 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)

```

