



Configuring Port Security

This chapter describes how to configure port security and how to limit the number of MAC addresses that are learned on the Catalyst 6500 series switches.



Note

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



[Authentication Bypass.](#) [Chapter 41, “Configuring MAC](#)



For information on configuring 802.1X authentication to restrict the unauthorized devices from connecting to a LAN through the publicly accessible ports, see [Chapter 40, “Configuring 802.1X Authentication.”](#)



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, see [Chapter 39, “Configuring the Switch Access Using AAA.”](#)



For information on configuring network admission control, see [Chapter 44, “Configuring Network Admission Control.”](#)

This chapter consists of these sections:

- [Understanding How Port Security Works, page 38-2](#)
[Understanding How MAC-Address Monitoring Works, page 38-3](#)
[Port Security Configuration Guidelines, page 38-4](#)
[Configuring Port Security on the Switch, page 38-4](#)
[Configuring MAC-Address Monitoring, page 38-14](#)

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 the traffic that is destined to or received from a specific host that is based on the host MAC address.

These sections describe the traffic filtering methods:

[Allowing the Traffic Based on the Host MAC Address, page 38-2](#)

[Restricting the Traffic Based on the Host MAC Address, page 38-3](#)

[Blocking the Unicast Flood Packets on the Secure Ports, page 38-3](#)

Allowing the Traffic Based on the Host MAC Address

-
-

MAC addresses on any port cannot exceed 4097.

Whether you allocate the maximum number of MAC addresses for each port depends on your network configuration. These combinations are examples of the valid allocations for the software releases prior to 8.1(1); the logic is the same for software release 8.1(1) and later releases:

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 1 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 learned dynamically, or configure some manually and allow the rest to be learned dynamically. Once you manually configure or autoconfigure the addresses, the addresses are stored in nonvolatile RAM (NVRAM) and maintained after a reset. The addresses that have been learned dynamically are not saved, so after a reset of the switch, all dynamically learned addresses are cleared.

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 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 the insecure hosts.

**Note**

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 the 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 learned dynamically 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 the 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 the Traffic Based on the Host MAC Address

You can filter the traffic that is based on a host MAC address so that the packets that are tagged with a specific source MAC address are discarded. When you specify a MAC address filter with the **set cam filter**



set cam filter

Blocking the Unicast Flood Packets on the Secure Ports

Understanding How MAC-Address Monitoring Works

```

Console> (enable) set port security 2/1 enable
Port 2/1 security enabled.
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) set port security 2/1 enable 00-90-2b-03-34-08

```

```

Trunking disabled for Port 2/1 due to Security Mode
Console> (enable)

```

```

Console> (enable) set port security 2/2 00-90-2b-03-34-09 1,20,30

```

Setting the Maximum Number of Secure MAC Addresses

-
-

and secured on multiple ports that are in different VLANs. For example, a MAC address "00-00-aa-00-00-aa" can be configured or secured on port 2/1 in VLAN 10 and 2/2 in VLAN 20. If both these ports were in VLAN 10, this MAC address could be configured or secured on only one of these ports. A MAC address can be configured or secured on only one of the ports belonging to a VLAN.

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

Task	Command
	maximum <i>num_of_mac</i>

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

```
set port security 7/7 maximum 20
```

```
set port security 7/7 maximum 18
```

```
00-11-22-33-44-66 cleared from secure address list for port 7/7
Console> (enable)
```

Automatically Configuring Dynamically Learned MAC Addresses



Note

	set port security auto-configure enable disable
--	--

```
set port security auto-configure 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)
```

range is from 1–1440 minutes. Setting the age time to zero disables the aging of the secure addresses.

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

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

```
set port security 7/7 age 600
```

Setting the Port Security Aging Type



Note

{ **inactivity** } command is supported on the Supervisor Engine 720 and Supervisor Engine 32 only.

In software release 8.2(1) and later releases, you can set the type of aging to be applied to the addresses that were learned dynamically on a per-port basis. The two types of aging are as follows:

Absolute aging—Times out the MAC address after the *age_time* has been exceeded, regardless of the traffic pattern. This is the default for any secured port, and the *age_time* is set to 0.

Inactivity aging—Times out the MAC address only after the *age_time* of inactivity from the corresponding host has been exceeded.

To set the port-security aging type for the dynamically learned addresses on a per-port basis, perform this task in privileged mode:

This example shows how to set the different port-security aging types on port 5/1:

```
set port security 5/1 timer-type absolute
set port security 5/1 timer-type inactivity
```



clear port security 3/37 00-00-aa-00-00-aa 20,30

clear port security 3/37 00-00-aa-00-00-aa all

clear port security 2/2 00-90-2b-03-34-09 1



```
set port security 4/1 unicast-flood disable
show port security 4/1
```

```
show port unicast-flood 4/1
```



Specifying the Security Violation Action

-
-

Specify the violation action on a port.	{
	}



Note

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.

You can set the time that 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.



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:

Set the shutdown timeout on a port.	

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

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

Disable port security on the desired ports.	
Verify the configuration.	[]

This example shows how to disable port security:

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

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

This example shows how to clear the filter:

This example shows how to display the static CAM entries:

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


Console> (enable)

* = Configured MAC Address

Port	Security Violation	Shutdown-Time	Age-Time	Maximum-Adrs	Trap	IfIndex
4/1	enabled shutdown	120	1440	25	disabled	3

Port	Secure-Src-Adrs	Age-Left	Last-Src-Addr	Shutdown	Shutdown-Time-Left
4/1	00-11-22-33-44-55 00-10-14-da-77-f1	4 100	00-11-22-33-44-55	No	-

Port Flooding on Address Limit

4/1 Enabled

Console> (enable)

Port	Total-Adrs	Maximum-Adrs
4/1	4	10

Console> (enable)

Console> (enable)

Port	Total-Adrs	Maximum-Adrs
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 secure ports: 0

Total MAC address(es): 223

Total global address space used (out of 4096): 199

Status: installed

Console> (enable)

```
Console> (enable)

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)
```

Configuring Global MAC-Address Monitoring

Task	Command
Note	

Monitoring the MAC Addresses in the CAM Table

Task	Command
Note	

Specifying the Polling Interval for Monitoring

Task	Command
Note	

Specifying the Lower Threshold for MAC-Address Monitoring

Task	Command
Note	

Specifying the Upper Threshold for MAC-Address Monitoring

Task	Command
<p data-bbox="386 562 435 590">Note</p>	

Clearing the Configuration for MAC-Address Monitoring

Task	Command
	<p data-bbox="1175 1436 1533 1463"><i>mod/port mod/port vlan vlan</i></p> <p data-bbox="1357 1528 1474 1556"><i>mod/port </i></p> <p data-bbox="954 1560 1182 1587"><i>mod/port vlan vlan</i></p> <p data-bbox="1338 1604 1455 1631"><i>mod/port </i></p> <p data-bbox="954 1635 1182 1663"><i>mod/port vlan vlan</i></p>

Displaying the Configuration for the CAM Monitor


```

Port Status Low Low High High No. of
Threshold Action Threshold Action mac addr
-----
3/1 enabled 500 warning 32000 warning 0
4/2 enabled 500 warning* 32000 warning 0

Total port entries = 2

Console> (enable)

```


```

Console> (enable)
Cam monitor global configuration:
status : enabled
interval : 5 seconds
Console> (enable)

```