

Configure MAC

- Feature History for MAC, on page 1
- MAC Address and MAC Address Table Management, on page 2
- Configuration steps for MAC address table management, on page 6
- Troubleshoot MAC Address Table Management, on page 11
- Information about port security, on page 12
- How to configure port security, on page 20
- Configuration examples for port security, on page 28

Feature History for MAC

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 26.2.1	MAC Address Table Management: MAC Address Table Management feature for static MAC and static MAC drop support has been introduced.	Cisco C9350 Smart Series Switches
Cisco IOS XE 26.2.1	The Port Security feature restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port.	Cisco C9350 Series Smart Switches
Cisco IOS XE 26.2.1ea	MAC: MAC feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	A MAC address is a Layer 2 address used to identify individual devices on a local area network (LAN). It is a globally unique identifier hardcoded into the network adapter by the manufacturer.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

MAC Address and MAC Address Table Management

MAC Address Table Management (MATM) refers to the processes by which a Layer 2 switch builds, maintains, and uses its MAC address table to efficiently forward Ethernet frames. A Layer 2 switch's primary function is to forward frames based on MAC addresses. To do this efficiently, the switch maintains a MAC address table that maps MAC addresses to specific switch ports and VLANs. MATM encompasses the mechanisms of how entries are added, updated, and removed from this table.

MAC Address Table Management supports manually configured static Media Access Control (MAC) address-table entries, including static MAC drop entries, on supported Cisco C9000 Smart Series Switches.

Unlike dynamically learned MAC entries, static entries are configured by an administrator and associate a MAC address with a specific Virtual Local Area Network (VLAN) and interface. Static MAC drop entries discard matching traffic instead of forwarding it. You can configure and monitor the feature through the command-line interface (CLI), Simple Network Management Protocol (SNMP), Yet Another Next Generation (YANG) data models, Cisco DNA Center, and Meraki Cloud.

Key MATM processes:

- **MAC address learning:**
  - When a switch receives a frame on a port, it inspects the **source MAC address** of the frame.
  - If the source MAC address is not already in the MAC address table, or if it is in the table but associated with a different port, the switch adds or updates the entry, associating the MAC address with the incoming port and VLAN.
  - This allows the switch to know which port to use when sending frames *to* that MAC address in the future.
- **Frame forwarding:**
  - When a switch receives a frame, it inspects the **destination MAC address**.
  - The switch then looks up this destination MAC address in its MAC address table.
  - **Known destination:** If the destination MAC address is found and associated with a specific port (different from the incoming port), the switch forwards the frame only out of that specific port. This is called **unicast forwarding**.
  - **Unknown destination (flooding):** If the destination MAC address is not found in the table, the switch floods the frame out of all ports within the same VLAN, except the port on which it was received. This ensures the frame reaches its intended destination, and the destination's response will allow the switch to learn its MAC address.
  - **Same port (filtering):** If the destination MAC address is found and associated with the same port on which the frame was received, the switch drops (filters) the frame. This prevents unnecessary traffic from being sent back out the same segment.
  - **Broadcast/multicast:** Broadcast frames (destination MAC FF:FF:FF:FF:FF:FF) and unknown multicast frames are always flooded out of all ports within the same VLAN, except the incoming port.
- **MAC address aging:**
  - MAC address entries in the table are not permanent. Each entry has an associated aging timer.

- If the switch does not receive any frames from a particular source MAC address on a specific port within the aging time, that entry is removed from the MAC address table.
- Aging ensures that the table remains current and does not become cluttered with stale entries from devices that are no longer connected or have moved to a different port. The default aging time is typically 300 seconds (5 minutes).

Benefits of MATM:

- **Efficient frame delivery:** Switches forward frames only to the intended destination port, reducing unnecessary traffic on other network segments.
- **Reduced collisions:** Switches segment collision domains to improve network performance in half-duplex environments.
- **Dynamic adaptation:** The table updates automatically as devices connect, disconnect, or move within the network.
- **Unauthorized device prevention:** Prevents unauthorized or malicious devices from participating in the Layer 2 network.
- **MAC address blocking:** Blocks traffic associated with known unauthorized or malicious MAC addresses.
- **Fixed endpoint association:** Maintains a fixed association between a critical endpoint and its designated interface.
- **Threat mitigation:** Helps mitigate MAC spoofing and protocol interference.
- **Enhanced traffic control and isolation:** Switches limit traffic exposure to relevant devices, although this behavior is not a security feature by itself.
- **Centralized administration:** Supports centralized management, monitoring, automation, and auditing.

Best practices for MAC Address Table Management

Follow these best practices to configure and maintain static MAC entries and static MAC drop entries.

- Configure drop entries only for MAC addresses known to be malicious, unauthorized, or otherwise undesirable.
- Avoid broad drop configurations that could interrupt legitimate traffic.
- Specify the correct VLAN and interface when creating a static forwarding entry.
- Test drop entries in a staging environment before deploying them in production.
- Document static forwarding and drop entries for change control and auditing.
- Review the static MAC address table regularly and remove obsolete entries.
- Ensure that management systems have the required connectivity and credentials before using automation.

Restrictions and limitations of MAC and MATM

Both MAC addresses and MATM processes have inherent restrictions and limitations:

MAC address limitations:

- Flat address space: MAC addresses provide no hierarchical information for routing beyond the local segment. They do not indicate network location or subnet, making them unsuitable for large-scale routing.
- Burned-in nature: MAC addresses are generally hardcoded into the network interface controller (NIC) and are not easily changed by end-users. While they can be spoofed (changed programmatically), this is typically a violation of network policy.
- Security vulnerabilities: MAC addresses are not inherently secure. They are susceptible to spoofing, where a malicious actor impersonates another device by using its MAC address, and to MAC flooding attacks, which can overwhelm a switch's MAC address table.
- Scalability in broadcast domains: While unique, managing an extremely large number of MAC addresses within a single broadcast domain (VLAN) can lead to very large CAM tables, consuming significant switch memory and potentially impacting lookup performance.

MATM limitations:

- The feature is supported only on Cisco C9350 Smart Series Switches running Cisco IOS XE 26.2.1 or later.
- An incorrect VLAN or interface association can misdirect or drop traffic.
- Configuring the wrong MAC address in a static drop entry can interrupt legitimate traffic.
- Static entries apply only to the VLAN specified in the configuration.
- The specified VLAN and Layer 2 interface must exist and be configured correctly.
- CAM table capacity: Content-addressable memory (CAM) tables have a finite capacity. If the number of learned MAC addresses exceeds this capacity, the switch may flood unknown unicast frames through eligible ports in the VLAN. This behavior can reduce performance and increase security risks.
- MAC flooding attacks: Attackers can send frames with numerous unique source MAC addresses to fill the CAM table and force the switch to flood unknown unicast traffic.
- MAC address flapping: A MAC address that moves rapidly between ports can indicate a network loop or configuration error. Frequent flapping can destabilize the CAM table, increase CPU utilization, and disrupt services.
- Aging-time impact: A short aging time can cause frequent MAC address relearning and increase switch overhead. A long aging time can retain stale entries and misdirect frames until the entries age out or the switch relearns them.
- No Layer 3 awareness: MATM operates only at Layer 2 and does not interpret IP addresses, higher-layer protocols, or network topology beyond direct connectivity.

Types of MAC addresses

This section describes different classifications of MAC addresses and various methods for managing MAC address entries within the switch's table.

Types of MAC addresses:

- Unicast MAC addresses: These are unique identifiers assigned to a single network interface. They are the most common type and are used for one-to-one communication. The least significant bit of the first octet is 0.
- Multicast MAC addresses: These addresses are used for one-to-many communication within a local network segment. Frames sent to a multicast MAC address are received by all devices configured to listen for that specific multicast group. The least significant bit of the first octet is 1. IPv4 multicast addresses typically map to MAC addresses in the 01:00:5E:XX:XX:XX range.
- Broadcast MAC addresses: The broadcast MAC address is FF:FF:FF:FF:FF:FF. Frames sent to this address are delivered to all devices within the same broadcast domain (VLAN).
- Universally administered addresses (UAAs): These are the most common type of MAC address. They are burned into the NIC by the manufacturer and are globally unique. The OUI identifies the manufacturer.
- Locally administered addresses (LAAs): These are MAC addresses that can be manually configured or assigned by a network administrator, overriding the burned-in address. LAAs are not globally unique and must be managed carefully to avoid conflicts within a network.

Types of MAC address table entries (MATM methods):

- Dynamic MAC addresses: These are the most common type of entry. The switch learns them automatically when it receives a frame from a source MAC address on a specific port. Dynamic entries have an aging timer and are removed if no traffic is seen from that MAC address within the aging period.
- Static MAC addresses: These entries are manually configured by an administrator to permanently associate a MAC address with a specific port and VLAN. Static entries do not age out and remain in the CAM table until they are manually removed. They are useful for critical devices that should always be accessible on a specific port.
- Sticky MAC addresses: These combine aspects of dynamic and static learning. When enabled on a port, the switch dynamically learns MAC addresses and converts them into sticky entries. These sticky entries are then stored in the running configuration. If the running configuration is saved to the startup configuration, these entries persist across reboots. If a device associated with a sticky MAC address moves to another port, it triggers a security violation.
- Secure MAC addresses (Port Security): These are MAC addresses that are learned or configured under the port security feature. Port security allows you to limit the number of MAC addresses that can be learned on a port and define actions to take if a violation occurs (e.g., shutdown the port, restrict traffic). Secure MAC addresses can be dynamic, static, or sticky.
- Static MAC entry: Associates a MAC address with a particular VLAN and Layer 2 interface. It is commonly used when an endpoint must remain mapped to a fixed interface.
- Static MAC drop entry: Discards frames associated with a particular MAC address in the specified VLAN. It is commonly used to block unauthorized, malicious, misbehaving, or protocol-specific addresses.

Parameters for MAC Address Table Management

Table 1: Static MAC address-table entry parameters

Parameter	Description
mac-address	The 48-bit MAC address to forward or drop.

Parameter	Description
vlan-id	The VLAN in which the entry applies.
interface	The Layer 2 interface associated with a forwarding entry.
drop	Discards frames matching the MAC address.

Configuration steps for MAC address table management

How MAC Address Table Management works

This process describes the switch behavior that occurs when an administrator configures a static MAC entry or a static MAC drop entry.

Summary

This component takes part in static MAC entry processing:

- Switch: Uses the manually configured MAC address-to-interface association instead of dynamically learning the address from observed traffic, or discards frames that match a configured static MAC drop entry.

The switch applies the configured association or drop action until an administrator explicitly removes the entry.

Workflow

These stages describe how the switch processes a static MAC entry or a static MAC drop entry.

1. An administrator manually configures a MAC address, VLAN, and interface as a static MAC entry, or a MAC address, VLAN, and drop action as a static MAC drop entry.
2. For a static MAC entry, the switch uses the fixed MAC address, VLAN, and interface association instead of dynamically learning the address from observed traffic.
3. For a static MAC drop entry, the switch discards Ethernet frames that match the configured MAC address as a source or destination in the specified VLAN, instead of switching them through the device.
4. The static entry remains in the MAC address table until an administrator explicitly removes it.

Configure MAC Address Table Management

Before you begin

- Ensure that the device is running Cisco IOS XE 26.2.1 or later.
- Obtain administrative access.
- Ensure that the required VLAN and interface exist.

- For centralized or model-driven management, confirm that the management platform has network and credential access.

Procedure

Step 1 Enter global configuration mode.

Example:

```
configure terminal
```

Step 2 Configure a static MAC address entry.

Example:

```
mac address-table static <mac-address> vlan <vlan-id> interface <interface-type>
<interface-number>
```

Example: Configure MAC address 0022.3344.5566 as a static entry on VLAN 10 and interface GigabitEthernet1/0/1.

```
mac address-table static 0022.3344.5566 vlan 10 interface GigabitEthernet1/0/1
```

Step 3 Configure a static MAC drop entry.

Example:

```
mac address-table static <mac-address> vlan <vlan-id> drop
```

Example: Configure MAC address aabb.ccdd.eeff to be dropped on VLAN 20.

```
mac address-table static aabb.ccdd.eeff vlan 20 drop
```

Step 4 Exit configuration mode.

Example:

```
end
```

Step 5 Verify the static MAC address entry or static MAC drop entry.

Example:

```
mac address-table static 0000.1111.2222 vlan 201 drop
Device-config# show mac address-table static vlan 201
Device-config# show platform software fed switch active matm macTable vlan 201 mac
0000.1111.2222
```

Table 2: Example abbreviated output

VLAN	MAC address	Type	Port
201	0000.1111.2222	Static	Drop

Example abbreviated output: Total Mac Addresses for this criterion: 1.

Table 3: Example abbreviated output

VLAN	MAC address	Type	Seq#	EC	Bi	Flags	*a time	*e time ports	Con
201	0000.1111.2222	Static	0x802	0	0	0	0	0	No

The static MAC address entry or static MAC drop entry is added to the MAC address table and takes effect immediately.

Configure global MAC address table aging time

This procedure changes the global aging time for dynamically learned MAC addresses.

Procedure

Step 1 enable

Example:

```
Switch> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 configure terminal

Example:

```
Switch# configure terminal
```

Enters global configuration mode.

Step 3 mac address-table aging-time seconds [vlan vlan-id]

Example:

```
Switch(config)# mac address-table aging-time 600
Switch(config)# mac address-table aging-time 120 vlan 10
```

Configures the aging time for MAC address table entries.

For seconds, the range is 0 to 1000000. A value of 0 disables aging.

(Optional) Use vlan vlan-id to configure the aging time for a specific VLAN.

Step 4 end

Example:

```
Switch(config)# end
```

Returns to privileged EXEC mode.

Step 5 copy running-config startup-config

Example:

```
Switch# copy running-config startup-config
```

Saves the running configuration to the startup configuration.

Configure a static MAC address entry

This procedure manually binds a MAC address to a specific port and VLAN.

Procedure

Step 1 enable

Example:

```
Switch> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 configure terminal

Example:

```
Switch# configure terminal
```

Enters global configuration mode.

Step 3 mac address-table static mac-address vlan vlan-id interface type number

Example:

```
Switch(config)# mac address-table static 0011.2233.4455 vlan 10 interface GigabitEthernet0/1
```

Creates a static MAC address entry.

Replace mac-address with the actual MAC address, vlan-id with the VLAN ID, and type number with the interface.

Step 4 end

Example:

```
Switch(config)# end
```

Returns to privileged EXEC mode.

Step 5 copy running-config startup-config

Example:

```
Switch# copy running-config startup-config
```

Saves the running configuration to the startup configuration.

Configure MAC address move notification

This procedure enables the switch to send notifications (SNMP traps) when a MAC address moves from one port to another.

Procedure

Step 1 enable

Example:

```
Switch> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 configure terminal

Example:

```
Switch# configure terminal
```

Enters global configuration mode.

Step 3 mac address-table notification mac-move

Example:

```
Switch(config)# mac address-table notification mac-move
```

Enables MAC address move notifications globally.

Step 4 snmp-server enable traps mac-notification change

Example:

```
Switch(config)# snmp-server enable traps mac-notification change
```

Enables SNMP traps for MAC address table change notifications.

Step 5 end

Example:

```
Switch(config)# end
```

Returns to privileged EXEC mode.

Step 6 copy running-config startup-config

Example:

```
Switch# copy running-config startup-config
```

Saves the running configuration to the startup configuration.

Verify MAC address table management features configuration

To ensure that the MAC address table management features are properly configured on the switch, enabling accurate learning, aging, and control of MAC addresses for optimal network performance and security.

After configuring MAC address table management features, use these commands in privileged EXEC mode to verify their operation:

Table 4: Commands for displaying MAC address table status

Command	Purpose	Example Output

show mac address-table	Displays all MAC addresses learned by the switch, including dynamic, static, and sticky entries, along with their associated VLANs and ports.	`Vlan Mac Address Type Ports`
		`---`
		`10 0011.2233.4455 STATIC GigabitEthernet0/1`
		`20 00A0.B0C0.D0E0 DYNAMIC GigabitEthernet0/3`
		`30 00F1.F2F3.F4F5 STATIC GigabitEthernet0/2`

show mac address-table aging-time	Shows the configured global and VLAN-specific MAC address aging times.	`Global aging time: 300`
		`Vlan Aging Time`
		`---`
		`10 120`

show mac address-table static	Displays only the static MAC address entries.	`Vlan Mac Address Type Ports`
		`---`
		`10 0011.2233.4455 STATIC GigabitEthernet0/1`
		`30 00F1.F2F3.F4F5 STATIC GigabitEthernet0/2`

show running-config | include mac address-table notification mac-move	Verifies that MAC address move notification is enabled globally.	`mac address-table notification mac-move`
show running-config | include snmp-server enable traps mac-notification change	Verifies that SNMP traps for MAC address table change notifications are enabled.	`snmp-server enable traps mac-notification change`

Troubleshoot MAC Address Table Management

Procedure

Step 1 Confirm the configuration when a static entry is missing.

- Ensure that the correct MAC address and VLAN were configured.
- Use **`show mac address-table`** to check whether the entry is installed.

Step 2 Verify the VLAN and interface association when traffic is forwarded incorrectly.

- Verify the VLAN and interface associated with the static entry.
- Ensure that the target interface is operating as a valid Layer 2 interface.
- Check for an incorrect static association that could be causing traffic to be dropped or forwarded to the wrong interface.

Step 3 Review the static MAC drop entries when legitimate traffic is being dropped.

- Review the configured static MAC drop entries.
- Ensure that the affected source or destination MAC address was not added accidentally.
- Remove obsolete or incorrect drop entries.
- Verify that the drop applies to the intended VLAN.
- After you configure a drop entry, confirm that traffic to and from the specified MAC address is handled as expected on the specified VLAN.

Information about port security

Port security

Port security is a network security feature that

- restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port
- prevents the port from forwarding packets with source addresses outside the group of defined addresses, and
- ensures full bandwidth allocation when configured with a single secure MAC address per port.

Security violation conditions

A security violation occurs when:

- A port is configured as a secure port and the maximum number of secure MAC addresses is reached, and the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses.
- A station with a secure MAC address configured or learned on one secure port attempts to access another secure port.

The switch cannot physically detect the link state for devices connected through a Cisco IP phone. When a port disconnects from the switch, the system immediately removes the dynamic secure MAC addresses, even if the port-security aging inactivity is configured to retain those addresses.

Requirement: prerequisites for port security

If you try to set the maximum value to a number less than the number of secure addresses already configured on an interface, the command is rejected.

Restrictions for port security

The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system. This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

Port Security is not supported on EtherChanel interfaces.

Port Security is not supported on private VLAN ports.

We recommend that you do not enable port security on an 802.1X authenticator interface.

When port-security is disabled on a port, the 802.1X sessions on the port get removed, because the aging timer and inactivity type is still configured. To ensure that the 802.1X sessions are not removed, when disabling port-security, disable the aging timer and inactivity type by removing the following commands:

- **switchport port-security aging time 1**
- **switchport port-security aging type inactivity**

If the inactivity timer is required, see the section "Enabling and Configuring Port Security Aging".

Types of secure MAC addresses

The switch supports these types of secure MAC addresses:

The switch supports secure MAC addresses with these characteristics:

- Static secure MAC addresses—These are manually configured by using the **switchport port-security MAC-address** *MAC-address* interface configuration command, stored in the address table, and added to the switch running configuration.
- Dynamic secure MAC addresses—These are dynamically configured, stored only in the address table, and removed when the switch restarts.
- Sticky secure MAC addresses—These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.

Default MAC address table settings

This reference provides the default configuration settings for MAC address table features.

The table shows the default settings for the MAC address table.

Table 5: Default settings for the MAC address

Feature	Default Setting
Aging time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	None configured

MAC address table creation

MAC address table creation is a dynamic addressing process that

- learns the source address of packets received on each port and adds the address and its associated port number to the address table
- updates the address table by adding new dynamic addresses and aging out those that are not in use as devices are added or removed from the network, and
- enables packet forwarding between any combination of ports based on the destination address of the received packet.

MAC address table characteristics

The aging interval is globally configured. However, the device maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The device sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the device forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The device always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

Sticky secure MAC addresses

A sticky secure MAC address is a network security feature that

- converts dynamic MAC addresses to secure MAC addresses through sticky learning
- adds converted addresses to the running configuration automatically, and
- maintains address security without requiring manual configuration of each MAC address.

Sticky learning behavior

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky learning. The interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All sticky secure MAC addresses are added to the running configuration.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

Security violations

Security violations occur in specific situations and can be configured with different violation modes, each with corresponding actions. It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.
- Running diagnostic tests with port security enabled.

You can configure the interface for one of three violation modes, based on the action to be taken if a violation occurs:

- protect—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

Note We do not recommend configuring the protect violation mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

- restrict—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
- shutdown—a port security violation causes the interface to become error-disabled and to shut down immediately, and the port LED turns off. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause** *psecure-violation* global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands. This is the default mode.
- shutdown VLAN—Use to set the security violation mode per-VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs

This table shows the violation mode and the actions taken when you configure an interface for port security.

Table 6: Security violation mode actions

Violation Mode	Traffic is forwarded [1]	Sends SNMP trap	Sends syslog message	Displays error message [2]	Violation counter increments	Shu
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No
shutdown	No	No	No	No	Yes	Yes
shutdown VLAN	No	No	Yes	No	Yes	No [3]

[1] Packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.
[2] The switch returns an error message if you manually configure an address that would cause a security violation.
[3] Shuts down only the VLAN on which the violation occurred.

Port security aging

Port security aging is a security feature that

- sets the aging time for all secure addresses on a port
- supports two types of aging per port: absolute and inactivity, and
- automatically deletes secure addresses based on configured time parameters.

Aging types

Two types of aging are supported per port:

- Absolute—The secure addresses on the port are deleted after the specified aging time.
- Inactivity—The secure addresses on the port are deleted only if the secure addresses are inactive for the specified aging time.

Port security and switch stacks

A port security and switch stack is a security mechanism that

- manages secure MAC addresses when switches dynamically join or leave a stack configuration,
- distributes and cleans up secure MAC addresses automatically among stack members, and
- ensures that the MAC address table remains consistent and up-to-date as the stack's membership changes.

Stack membership behavior

When switches join or leave a stack, the port security feature handles secure MAC address distribution and cleanup:

- When a switch joins a stack, the new switch will get the configured secure addresses. All dynamic secure addresses are downloaded by the new stack member from the other stack members.
- When a switch (either the active switch or a stack member) leaves the stack, the remaining stack members are notified, and the secure MAC addresses configured or learned by that switch are deleted from the secure MAC address table.

Default port security configuration

This table provides the default configuration settings for port security features on network ports.

Table 7: Default port security configuration

Feature	Default Setting
Port security	Disabled on a port.
Sticky address learning	Disabled.
Maximum number of secure MAC addresses per port	One address
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Port security aging	Disabled. Aging time is 0. Static aging is disabled. Type is absolute.

Guidelines for port security configuration

Port type restrictions

Configure port security only on static access ports or trunk ports. A secure port cannot be a dynamic access port.

- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- Voice VLAN is only supported on access ports and not on trunk ports, even though the configuration is allowed.

Voice VLAN configuration

When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the phone.

Trunk port voice commands

When a trunk port configured with port security and assigned to an access VLAN for data traffic and to a voice VLAN for voice traffic, entering the **switchport voice** and **switchport priority extend** interface configuration commands has no effect.

- When a connected device uses the same MAC address to request an IP address for the access VLAN and then an IP address for the voice VLAN, only the access VLAN is assigned an IP address.

Maximum address configuration

When you enter a maximum secure address value for an interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the

previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

Sticky MAC address aging

The switch does not support port security aging of sticky secure MAC addresses.

Management traffic control

Management traffic control is a network security feature that

- allows traffic to enter through a user-defined physical interface and restricts traffic to any other interfaces that is not defined by the user
- assigns a single IP address on the device to receive traffic when the feature is enabled, and
- allows traffic flow only through the defined interface when the network protocol and the IP address is set according to the user's preference.

Supported interfaces and protocols

The feature is supported on these interfaces:

- Layer 2 physical interface.
- Layer 3 physical interface.
- Layer 2 port channel.
- Layer 3 port channel.
- App-hosting interface.

This table shows the supported protocols and their respective port numbers:

Table 8: Supported protocols and the respective port numbers

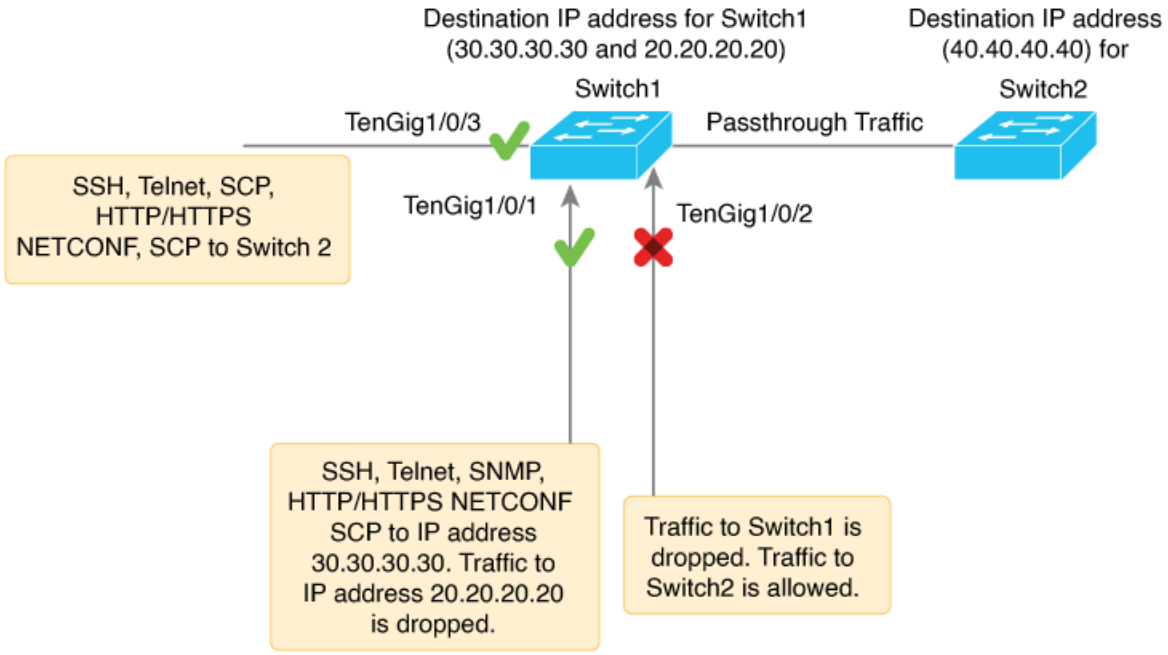
Protocol	Keyword	Port Number
HTTPS	TCP	443
TELNET	TCP	23
SSH	TCP	22
NETCONF-SSH	TCP	830
SNMP	UDP	161
HTTP	TCP	80

Note

- You cannot configure IPv6 address configurations in the management traffic control feature.
- VRF based IP configuration is not supported on the managament traffic control feature.
- The management traffic control feature is not supported on interfaces like port-channel member, SVI, stack-port and management port.

Traffic control example

Switch1 and Switch2 are devices that are in a network. Management traffic control feature is enabled on Switch1 with the interface Tengig 1/0/1 and destination IP address 30.30.30.30. Traffic is allowed through the interface with the enabled protocols SSH, TELNET, SNMP, HTTP, HTTPS, NETCONF, SCP to destination IP address 30.30.30.30. Traffic passing through interface Tengig 1/0/1 to IP address 20.20.20.20 is dropped. Management traffic control feature enables only one destination IP address to be configured. If interface TenGig 1/0/2 is not defined by the management traffic control feature for any of the devices, traffic will not be allowed to Switch1 but can still pass through to its configured destination in the network.



How to configure port security

Enable and configure port security

This task restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port.

Port security helps secure your network by controlling which devices can connect to a specific port based on their MAC addresses. This feature is particularly useful in environments where you need to restrict access to network resources.

Before you begin

Follow these steps to enable and configure port security:

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** *interface-ID*

Example:

```
Device(config)# interface gigabitethernet 1/0/1
```

Specifies the interface to be configured, and enter interface configuration mode.

Step 4 **switchport mode** {**access** | **trunk**}

Example:

```
Device(config-if)# switchport mode access
```

Sets the interface switchport mode as access or trunk; an interface in the default mode (dynamic auto) cannot be configured as a secure port.

Step 5 **switchport voice vlan** *vlan-id*

Example:

```
Device(config-if)# switchport voice vlan 22
```

Enables voice VLAN on a port.

VLAN-ID—Specifies the VLAN to be used for voice traffic.

Step 6 **switchport port-security**

Example:

```
Device(config-if)# switchport port-security
```

Enables port security on the interface.

Note
Under certain conditions, when port security is enabled on the member ports in a switch stack, the DHCP and ARP packets would be dropped. As a workaround, shutdown the interface and then configure the **no shutdown** command.

Step 7 **switchport port-security [maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]

Example:

```
Device(config-if)# switchport port-security maximum 20
```

(Optional) Sets the maximum number of secure MAC addresses for the interface. The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

(Optional) **vlan**—sets a per-VLAN maximum value

Enter one of these options after you enter the **vlan** keyword:

- *vlan-list*—On a trunk port, you can set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.
- **access**—On an access port, specifies the VLAN as an access VLAN.
- **voice**—On an access port, specifies the VLAN as a voice VLAN.

Note
The **voice** keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN. If an interface is configured for voice VLAN, configure a maximum of two secure MAC addresses.

Step 8 **switchport port-security violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}

Example:

```
Device(config-if)# switchport port-security violation restrict
```

(Optional) Sets the violation mode, the action to be taken when a security violation is detected, as one of these:

- **protect**—When the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

  Note
  We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

- **restrict**—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
- **shutdown**—The interface is error-disabled when a violation occurs, and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
- **shutdown vlan**—Use to set the security violation mode per VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs.

Note
When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command. You can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands or by using the **clear errdisable interface vlan** privileged EXEC command.

Step 9 **switchport port-security [mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}]

Example:

```
Device(config-if)# switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice
```

(Optional) Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.

Note
If you enable sticky learning after you enter this command, the secure addresses that were dynamically learned are converted to sticky secure MAC addresses and are added to the running configuration.

(Optional) **vlan**—sets a per-VLAN maximum value.

Enter one of these options after you enter the **vlan** keyword:

- *vlan-id*—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used.
- **access**—On an access port, specifies the VLAN as an access VLAN.
- **voice**—On an access port, specifies the VLAN as a voice VLAN.

Note
The **voice** keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN. If an interface is configured for voice VLAN, configure a maximum of two secure MAC addresses.

Step 10 **switchport port-security mac-address sticky**

Example:

```
Device(config-if)# switchport port-security mac-address sticky
```

(Optional) Enables sticky learning on the interface.

Step 11 **switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]

Example:

```
Device(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice
```

(Optional) Enters a sticky secure MAC address, repeating the command as many times as necessary. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned, are converted to sticky secure MAC addresses, and are added to the running configuration.

Note
If you do not enable sticky learning before this command is entered, an error message appears, and you cannot enter a sticky secure MAC address.

(Optional) **vlan**—sets a per-VLAN maximum value.

Enter one of these options after you enter the **vlan** keyword:

- *vlan-id*—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used.
- **access**—On an access port, specifies the VLAN as an access VLAN.
- **voice**—On an access port, specifies the VLAN as a voice VLAN.

Note
The **voice** keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN.

Step 12 **end**

Example:

```
Device(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

Step 13 **show port-security**

Example:

```
Device# show port-security
```

Displays information about the port-security settings.

Port security is now enabled and configured on the interface. The port security settings are displayed, showing the maximum number of secure MAC addresses, violation mode, and any configured secure MAC addresses.

Enable and configure port security aging

Enable and configure port security aging to automatically manage secure MAC addresses on a port by allowing them to age out after a specified time period, which enables adding new devices without manually removing existing secure addresses.

Use this feature to remove and add devices on a secure port without manually deleting the existing secure MAC addresses and to still limit the number of secure addresses on a port. You can enable or disable the aging of secure addresses on a per-port basis.

Before you begin

Follow these steps to enable and configure port security aging:

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** *interface-id*

Example:

```
Device(config)# interface gigabitethernet1/0/1
```

Specifies the interface to be configured, and enter interface configuration mode.

Step 4 **switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}

Example:

```
Device(config-if)# switchport port-security aging time 120
```

Enables or disable static aging for the secure port, or set the aging time or type.

Note
The switch does not support port security aging of sticky secure addresses.

Enter **static** to enable aging for statically configured secure addresses on this port.

For *time*, specifies the aging time for this port. The valid range is from 0 to 1440 minutes.

For **type**, select one of these keywords:

- **absolute**—Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list.
- **inactivity**—Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.

Step 5 **end**

Example:

```
Device(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

Step 6 **show port-security** [**interface** *interface-id*] [**address**]

Example:

```
Device# show port-security interface gigabitethernet1/0/1
```

Displays information about the port-security settings on the specified interface.

Port security aging is configured on the specified interface, allowing secure MAC addresses to age out automatically based on the configured time and type settings.

Change the address aging time

This task configures the dynamic address table aging time to control how long MAC address entries remain active in the address table.

Dynamic address table aging time determines how long a learned MAC address remains in the table before being removed. The range is 10 to 1000000 seconds with a default of 300 seconds. You can also enter 0 to disable aging completely. Static address entries are never aged or removed from the table.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **MAC address-table aging-time** [*0* | *10-1000000*] [**routed-MAC** | **vlan** *vlan-id*]

Example:

```
Device(config)# mac address-table aging-time 500 vlan 2
```

Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.

The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table.

vlan-id—Valid IDs are 1 to 4094.

Step 4 **end**

Example:

```
Device(config)# end
```

Exits global configuration mode and returns to privileged EXEC mode.

The dynamic address table aging time is configured. MAC addresses will now age out according to the specified time interval for the configured VLAN or globally if no VLAN was specified.

Monitor port security

This reference provides commands for monitoring port security settings, including maximum allowed secure MAC addresses, current secure MAC addresses, security violations, and violation modes for device interfaces.

This table displays port security information.

Table 9: Commands for displaying port security status and configuration

Command	Purpose
show port-security [**interface** *interface-id*]	Displays port security settings for the device or for the specified including the maximum allowed number of secure MAC addre each interface, the number of secure MAC addresses on the int number of security violations that have occurred, and the violat
show port-security [**interface** *interface-id*] **address**	Displays all secure MAC addresses configured on all device in on a specified interface with aging information for each addres
show port-security interface *interface-id* **VLAN**	Displays the number of secure MAC addresses configured per the specified interface.

Configure management traffic control

Configure the management traffic control feature to control and define the network protocols and destination addresses for traffic management through specific interfaces.

Management traffic control enables you to specify which interfaces, protocols, and destination addresses are allowed for traffic management on your device. This feature provides granular control over network access and enhances security by restricting traffic to authorized pathways.

Before you begin

Follow these steps to configure management traffic control:

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **mgmt-traffic control ipv4**

Example:

```
Device# mgmt-traffic control ipv4
Device(config-mtc-ipv4)#
```

Enables the management traffic control feature.

Step 4 **interface** *interface-id*

Example:

```
Device(config-mtc-ipv4)# interface gigabitethernet1/0/1
Device(config-mtc-ipv4)#
```

Defines the interface through which traffic is allowed.

Step 5 **protocol** { [**telnet http https netconf scp snmp ssh**] }

Example:

```
Device(config-mtc-ipv4)# protocol telnet http https netconf scp snmp ssh
Device(config-mtc-ipv4)#
```

Enables the specified network protocols in the interface.

Step 6 **address** *ip-address*

Example:

```
Device(config-mtc-ipv4)# address 30.30.30.30
Device(config-mtc-ipv4)#
```

Specifies the destination address of traffic.

Step 7 **end**

Example:

```
Device(config-mtc-ipv4)# end
```

Exits management traffic control configuration mode and returns to privileged EXEC mode.

Management traffic control is now configured with the specified interface, protocols, and destination address. The device will restrict management traffic according to the configured parameters.

Configuration examples for port security

This section provides configuration examples for port security, including enabling port security on ports, setting maximum secure addresses, configuring static secure MAC addresses, and implementing sticky learning.

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 50. The violation mode is the default, no static secure MAC addresses are configured, and sticky learning is enabled.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 50
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# end
```

This example shows how to configure a static secure MAC address on VLAN 3 on a port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
Device(config-if)# end
```

This example shows how to enable sticky port security on a port, to manually configure MAC addresses for data VLAN and voice VLAN, and to set the total maximum number of secure addresses to 20 (10 for data VLAN and 10 for voice VLAN).

```
Device> enable
Device# configure terminal
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# switchport access vlan 21
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan 22
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 20
Device(config-if)# switchport port-security violation restrict
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Device(config-if)# switchport port-security mac-address 0000.0000.0003
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Device(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Device(config-if)# switchport port-security maximum 10 vlan access
Device(config-if)# switchport port-security maximum 10 vlan voice
Device(config-if)# end
```