



# CHAPTER 41

## Configuring MAC Authentication Bypass

---

This chapter describes how to configure MAC authentication bypass 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* publication.

---

**Note**

For information on configuring IEEE 802.1X authentication, see [Chapter 40, “Configuring 802.1X Authentication.”](#)

---

**Note**

For information on using 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, see [Chapter 38, “Configuring Port Security.”](#) That chapter also provides information on using port security to filter the traffic that is destined to or received from a specific host that is based on the host MAC address.

---

**Note**

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.”](#)

---

**Note**

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

---

This chapter consists of these sections:

- [Understanding How MAC Authentication Bypass Works](#), page 41-2
- [MAC Authentication Bypass Configuration Guidelines and Restrictions](#), page 41-4
- [Configuring MAC Authentication Bypass](#), page 41-6
- [Configuring MAC Authentication Bypass with ACL Assignments](#), page 41-13
- [Configuring Agentless Hosts for NAC Auditing with MAB](#), page 41-14

# Understanding How MAC Authentication Bypass Works

These sections describe how MAC authentication bypass works on the Catalyst 6500 series switches:

- [Overview, page 41-2](#)
- [Understanding Reauthentication of MAC Addresses, page 41-2](#)
- [Understanding MAC Authentication Bypass States, page 41-3](#)
- [Understanding MAC Authentication Bypass Events, page 41-4](#)

## Overview

MAC authentication bypass is an alternative to 802.1X that allows network access to devices (such as printers and IP phones) that do not have the 802.1X supplicant capability. MAC authentication bypass uses the MAC address of the connecting device to grant or deny network access.

To support MAC authentication bypass, the RADIUS authentication server maintains a database of MAC addresses for devices that require access to the network. MAC authentication bypass generates a RADIUS request with a MAC address in the calling-station-id (attribute 31) and service-type (attribute 6) with value 10.

To get the device's MAC address, the switch port needs to be in the forwarding state in a VLAN. If the port is not in the forwarding state in a VLAN, unicast traffic cannot enter or exit the switch. Because the switch port is brought up in the native VLAN with learning disabled on the port, the packets are redirected to the supervisor engine. When the supervisor engine sees a new MAC address, it installs a content-addressable memory (CAM) entry with a trap bit that is set to protect the supervisor engine from unnecessary flooding from that MAC address. The supervisor engine does not redirect further packets until the MAC authentication is finished. After a successful authentication, the RADIUS server sends a VLAN, and the port is moved to that VLAN. The trap entry is removed after a successful authentication. The port that is moved to the RADIUS server-specified VLAN behaves like any other switch port. If a MAC authentication fails, the port is moved into the authentication failure VLAN (if that VLAN is configured). (For information on authentication failure VLANs, see the [“Configuring the Authentication Failure VLAN”](#) section on page 40-38.)

## Understanding Reauthentication of MAC Addresses

In the reauthentication mode, a port stays in the RADIUS server-specified VLAN and tries to reauthenticate itself. If the reauthentication is successful, the port stays in the RADIUS server-specified VLAN. If the reauthentication is not successful, the port is either moved back to the authentication failure VLAN (if that VLAN is configured), or the port is moved from its existing VLAN to an administratively configured VLAN. Periodic reauthentication can be attempted for the failed port. The failed port's MAC address CAM entry on the previously authenticated VLAN is removed and the initialization process forces the port to automatically go into the administratively configured VLAN where it attempts to reauthenticate itself. If reauthentication is successful, the port is moved to the RADIUS server-specified VLAN.

The RADIUS server-specified timers can also trigger reauthentication. RADIUS server attributes 27 and 29 control the reauthentication behavior. Attribute 27 (session timeout) specifies the time after which authentication should be tried again, and attribute 29 (termination action) specifies whether the behavior should be one of the following:

- Initialize—The existing session is disrupted until the reauthentication results are available.
- Reauthenticate—The existing session is not disrupted while reauthentication is attempted.

## Understanding MAC Authentication Bypass States

This section describes the following MAC authentication bypass states:

- **Waiting**—In the waiting state, the switch waits to receive the MAC address that needs to be authenticated, learning is disabled, and the idle timer starts. The port is in the forwarding state to receive unicast traffic, and all Layer 2 entries on the port are cleared. The port transitions to the other state if there are other features configured but only after receiving an authentication result (the result could be success or failure). If traffic is not seen, the port remains in the waiting state.
- **Authenticating**—When the switch learns the port's MAC address from a redirected packet, the MAC authentication bypass state machine transitions to authenticating. In this state, the RADIUS request is built and sent to the RADIUS server and the switch waits for the RADIUS server response. If there is a successful authentication, the port moves to the authenticated state where the RADIUS server-specified VLAN is configured on the port, a static CAM entry is installed on the RADIUS server-specified VLAN, and the trap entries on the old VLAN are removed. If authentication fails, the port moves to the AuthFail State. If there is a RADIUS timeout or initialization, the port moves to the waiting state again.
- **Authenticated**—In the authenticated state, the RADIUS-received policy (VLAN) is configured on the port. The port then transitions to the waiting state in case there is an initialization and moves to the authenticating state if it receives a reauthenticate event. In the authenticated state, the trap entry on the port is removed from the old VLAN and the static CAM entry is installed on the new VLAN.
- **AuthFail**—In the AuthFail state, the port waits for “auth-fail-timeout” seconds before moving to the waiting state if no other features are configured. If fallback features are configured (such as web-based proxy authentication, 802.1X, or the authentication failure VLAN), the port moves to those states. A trap still exists in the AuthFail state, so a MAC address cannot authenticate itself again for auth-fail timeout seconds. When a port moves to the waiting state from the AuthFail state, the trap entries are cleared and the port starts the authentication process again.
- **Finished**—The finished state is entered after MAC authentication bypass fails to authenticate a host and if there are other features configured on the port that can potentially grant access (such as web-based proxy authentication, 802.1X, or the authentication failure VLAN). The finished state involves authorizing/bringing up the port and installing any policy required by the other features. For example, if the guest VLAN is configured, the port might be added to the guest VLAN. If web-based proxy authentication is configured, policies might be installed to allow Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and access control entries (ACEs) for HTTP redirection and so on. If other features are not configured, the port roams in the waiting, authenticating, AuthFail, and waiting states in case of an authentication failure or the port stays in the waiting state until it sees traffic.

## Understanding MAC Authentication Bypass Events

This section describes the following MAC authentication bypass events:

- **AuthenticateMac**—This event is posted by the redirected packet processing component when it sees a MAC address on the port. This event is posted to the MAC authentication bypass state machine when it is in the waiting state.
- **Initialize**—This event is triggered by the CLI and can be received in any state. Upon reception of this event, the port is moved to the waiting state and any required cleanup is performed (such as unauthorizing the port, cleaning up any static/trap CAM entries, and so on).
- **Reauthenticate**—This event is received because either a session-timeout expired or because of a CLI trigger (executive command entered from the CLI). This event is accepted only when the port is in the authenticated state; otherwise, it is ignored. If this event is CLI driven, you are informed that the CLI can be accepted only if the port is in the authenticated state.
- **Authentication success**—This event is posted when there is an authentication success from the RADIUS server. This event, which is accepted only when the port is in the authenticating state, transitions the port to the authenticated state.
- **Authentication failure**—This event is posted when there is an authentication failure received from the RADIUS server. This event, which is accepted only when the port is in the authenticating state, transitions the port to the AuthFail state.
- **RADIUS timeout**—This event is received when the RADIUS server is not responding. This event, which is accepted only when the port is in the authenticating state, transitions the port to the waiting state after the maximum number of retries expire and the RADIUS server does not respond.
- **AuthFail timeout**—This event is received when the port is in the AuthFail state because of a RADIUS server authentication failure and there are no other potential features configured to bring the port up. This event transitions the port to the waiting state, and the port starts the authentication process again.
- **Security violation**—This event can be received in any state other than the waiting state. This event is posted if a second MAC address is seen on a port. The action taken for a security violation depends on the global violation mode configured and can either restrict a MAC address or shut down the port.

## MAC Authentication Bypass Configuration Guidelines and Restrictions

This section provides the guidelines and restrictions for configuring MAC authentication bypass:

- **Security violations**—With MAC authentication bypass, only one host is supported per port. If more than one host appears on a port, it is a security violation and the port shuts down. With auxiliary VLAN ports, the one host per-port restriction only applies to hosts on the data VLAN; there is no restriction on the number of hosts on the auxiliary (voice) VLAN.
- **Policy enforcement**—MAC authentication bypass supports all policy enforcement mechanisms that are supported with 802.1X.
- **DHCP snooping**—MAC authentication bypass is independent of DHCP snooping. Until a MAC address successfully authenticates, no traffic is allowed from the MAC address (because of the trap entry), and the traffic that triggers the MAC authentication could be any type of traffic, including DHCP.

- 802.1X—MAC authentication bypass is an independent feature but when used in combination with 802.1X, acts as a fallback for authenticating MAC addresses. When both MAC authentication bypass and 802.1X are configured on a port, the port tries to authenticate using 802.1X. If the host does not respond to the EAPOL requests, instead of continuing the authentication attempts, the 802.1X port is moved to the MAC authentication bypass state, where the authentication is attempted using MAC authentication bypass.
- Authentication failure VLAN—When 802.1X authentication fails, irrespective of whether MAC authentication bypass is configured, if the authentication failure VLAN is configured, the port is moved to the authentication failure VLAN. The authentication failure VLAN is only for 802.1X authentication failed users and not a generic authentication failure VLAN for MAC authentication bypass. For more information on the authentication failure VLAN, see the [“Configuring the Authentication Failure VLAN” section on page 40-38](#).
- Guest VLAN—The 802.1X guest VLAN and MAC authentication bypass work together but with some changes to the existing guest VLAN behavior. When both the MAC authentication bypass and the guest VLAN are configured and no Extensible Authentication Protocol over LAN (EAPOL) packets are received on a port, the 802.1X state machine is moved to the MAC authentication bypass state where it puts the port to forwarding in the native VLAN and disables learning. If the guest VLAN is not configured, the port remains in the MAC authentication bypass state where it waits for a MAC address on the port. For more information on guest VLANs, see the [“Understanding How 802.1X Authentication for the Guest VLAN Works” section on page 40-9](#).
- Port security—When a new MAC address is redirected, the MAC authentication bypass function sees the MAC address before port security. If the MAC address is successfully authenticated, the port security feature is informed of the newly learned MAC address. In the inband path, the MAC authentication bypass function starts before any port security functions begin.
- Auxiliary VLANs—MAC authentication bypass is supported with auxiliary (voice) VLANs. MAC authentication bypass is restricted to those MAC addresses that appear on the port VLAN only. All IP phone MAC addresses that are learned through Cisco Discovery Protocol (CDP) are allowed on the auxiliary VLAN.
- Dynamic ARP Inspection (DAI)—Works with MAC authentication bypass.
- VLAN Membership Policy Server (VMPS)—MAC authentication bypass and VMPS are mutually exclusive features. The CLI prevents you from configuring both features at the same time.
- LAN port IP—When you configure both MAC authentication bypass and LAN port IP, the MAC authentication bypass function runs first. After authentication, the MAC authentication bypass feature triggers the LAN port IP function. The hosts in the LAN port IP exception list are authenticated using MAC authentication bypass (if configured) before access is provided.
- Web-based proxy authentication— When both MAC authentication bypass and web-based proxy authentication are configured on an interface, MAC authentication bypass starts before the web-based proxy authentication because MAC authentication bypass is a feature in Layer 2. A feature in Layer 2 is always attempted before a feature in Layer 3.
- RADIUS accounting—RADIUS accounting is supported.
- SNMP support—All required set and get calls are exported to SNMP. The SNMP support for MAC authentication bypass is scheduled for a future software release.
- High availability—High availability is supported. The MAC authentication bypass initial state and end state (authorized and unauthorized) of the port are synchronized to the standby supervisor engine. Intermediate states are not synchronized.

# Configuring MAC Authentication Bypass

These sections describe how to configure MAC authentication bypass:

- [Enabling or Disabling MAC Authentication Bypass Globally, page 41-6](#)
- [Enabling or Disabling MAC Authentication Bypass on a Port, page 41-6](#)
- [Initializing the MAC Authentication Bypass State for a Port, page 41-7](#)
- [Reauthenticating the MAC Address for a Port, page 41-7](#)
- [Specifying the Shutdown Timeout Period, page 41-7](#)
- [Specifying the AuthFail Timeout Period, page 41-8](#)
- [Specifying the Reauthentication Timeout Period, page 41-8](#)
- [Enabling or Disabling Reauthentication, page 41-9](#)
- [Specifying the Security Violation Mode, page 41-9](#)
- [Enabling or Disabling MAC Authentication Bypass RADIUS Accounting, page 41-9](#)
- [Configuring a PVLAN on a MAC Authentication Bypass-Enabled Port, page 41-10](#)
- [Configuring MAC Authentication Bypass on a PVLAN Port, page 41-11](#)
- [Displaying MAC Authentication Bypass Information, page 41-11](#)
- [Displaying the MAC Authentication Bypass Global Configuration, page 41-12](#)

## Enabling or Disabling MAC Authentication Bypass Globally

The default is disabled. To enable or disable MAC authentication bypass globally, perform this task in privileged mode:

Task	Command
Enable or disable MAC authentication bypass globally.	<b>set mac-auth-bypass { disable   enable }</b>

This example shows how to enable MAC authentication bypass globally:

```
Console> (enable) set mac-auth-bypass enable
Mac-Auth-Bypass enabled globally.
Console> (enable)
```

## Enabling or Disabling MAC Authentication Bypass on a Port

When you enable or disable MAC authentication bypass on a port, you automatically enable or disable PortFast on the same port. The default is enabled.

To enable or disable MAC authentication bypass on a port, perform this task in privileged mode:

Task	Command
Enable or disable MAC authentication bypass on a port.	<b>set port mac-auth-bypass <i>mod/port</i> { disable   enable }</b>

This example shows how to enable MAC authentication bypass on a port:

```
Console> (enable) set port mac-auth-bypass 3/1 enable
MAC-Auth-Bypass successfully enabled on 3/1.
Console> (enable)
```

## Initializing the MAC Authentication Bypass State for a Port

To initialize the MAC authentication bypass state for a port so that the port can participate in authentication again, perform this task in privileged mode:

Task	Command
Initialize the MAC authentication bypass state for a port so the port can participate in authentication again.	<b>set port mac-auth-bypass <i>mod/port</i> initialize</b>

This example shows how to initialize the MAC authentication bypass state for a port so that the port can participate in authentication again:

```
Console> (enable) set port mac-auth-bypass 3/1 initialize
Mac-Auth-Bypass successfully Initialized 3/1.
Console> (enable)
```

## Reauthenticating the MAC Address for a Port

To reauthenticate the MAC address for a port, perform this task in privileged mode:

Task	Command
Reauthenticate the MAC address for a port.	<b>set port mac-auth-bypass <i>mod/port</i> reauthenticate</b>

This example shows how to reauthenticate the MAC address for a port:

```
Console> (enable) set port mac-auth-bypass 3/1 reauthenticate
Reauthenticating MAC address 00-00-00-00-00-01 on port 3/1 using Mac-Auth-Bypass.
Console> (enable)
```

## Specifying the Shutdown Timeout Period

If there is a security violation on a port, the port shuts down. Use the global **set mac-auth-bypass shutdown-timeout *seconds*** command to specify the time (in seconds) the ports are shut down before they are automatically reenabled. The range is from 30 to 65535 seconds. The default is 60 seconds. If you specify a shutdown timeout period of 0 seconds, the automatic port enable function is disabled and you will have to reenable the ports manually.

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

Task	Command
Specify the shutdown timeout period.	<b>set mac-auth-bypass shutdown-timeout</b> <i>seconds</i>

This example shows how to specify the shutdown timeout period:

```
Console> (enable) set mac-auth-bypass shutdown-timeout 40
Shutdown Timeout set to 40 seconds.
Console> (enable)
```

## Specifying the AuthFail Timeout Period

The global **set mac-auth-bypass auth-fail-timeout** *seconds* command specifies the time (in seconds) that ports wait in the authentication failure (AuthFail) state before trying authentication again. The range is from 5 to 65535 seconds. The default is 60 seconds.

To specify the AuthFail timeout period, perform this task in privileged mode:

Task	Command
Specify the AuthFail timeout period.	<b>set mac-auth-bypass auth-fail-timeout</b> <i>seconds</i>

This example shows how to specify the AuthFail timeout period:

```
Console> (enable) set mac-auth-bypass auth-fail-timeout 60
Authfail Timeout set to 60 seconds.
Console> (enable)
```

## Specifying the Reauthentication Timeout Period

The global **set mac-auth-bypass reauth-timeout** *seconds* command specifies the time (in seconds) that elapse before reauthentication is triggered after global reauthentication is enabled. The range is from 300 to 65535 seconds. The default is 3600 seconds.

To specify the reauthentication timeout period, perform this task in privileged mode:

Task	Command
Specify the reauthentication timeout period.	<b>set mac-auth-bypass reauth-timeout</b> <i>seconds</i>

This example shows how to specify the reauthentication timeout period:

```
Console> (enable) set mac-auth-bypass reauth-timeout 400
Reauth Timeout set to 400 seconds.
Console> (enable)
```

## Enabling or Disabling Reauthentication

Enabling the global **set mac-auth-bypass re-authentication** command returns all MAC authentication bypass values to their defaults. The default is disabled.

To enable or disable MAC authentication bypass reauthentication globally, perform this task in privileged mode:

Task	Command
Enable or disable MAC authentication bypass reauthentication globally.	<b>set mac-auth-bypass reauthentication</b> { <b>disable</b>   <b>enable</b> }

This example shows how to enable MAC authentication bypass reauthentication globally:

```
Console> (enable) set mac-auth-bypass reauthentication enable
Global reauthentication mode enabled.
Console> (enable)
```

## Specifying the Security Violation Mode

If there is a security violation on a port, the port goes into restricted mode or is shut down. In restricted mode, the MAC address that causes the security violation is added as a trap entry into the forwarding table. The default is shutdown.

To specify the security violation mode globally, perform this task in privileged mode:

Task	Command
Specify the security violation mode globally.	<b>set mac-auth-bypass violation</b> { <b>restrict</b>   <b>shutdown</b> }

This example shows how to specify “restricted” for the security violation mode:

```
Console> (enable) set mac-auth-bypass violation restrict
Mac-Auth-Bypass security violation mode set to restrict.
Console> (enable)
```

## Enabling or Disabling MAC Authentication Bypass RADIUS Accounting

The default is disabled. To enable or disable MAC authentication bypass RADIUS accounting, perform these tasks in privileged mode:

Task	Command
Enable or disable MAC authentication bypass RADIUS accounting.	<b>set mac-auth-bypass</b> <b>radius-accounting</b> { <b>disable</b>   <b>enable</b> }
Verify the MAC authentication bypass RADIUS accounting state.	<b>show mac-auth-bypass config</b>

This example shows how to enable MAC authentication bypass RADIUS accounting:

```
Console> (enable) set mac-auth-bypass radius-accounting enable
Radius Accounting for MacAuth enabled.
Console> (enable)
```

This example shows how to verify the MAC authentication bypass RADIUS accounting state:

```
Console> (enable) show mac-auth-bypass config
Mac-Auth-Bypass Global Config
-----
Mac-Auth-Bypass Status      = Enabled
AuthFail Timeout           = 60
RadiusAccounting           = Enabled
Reauthentication           = Disabled
Reauth Timeout             = 3600
Shutdown Timeout           = 60
Violation mode              = Shutdown
Console> (enable)
```

## Configuring a PVLAN on a MAC Authentication Bypass-Enabled Port

To configure a PVLAN on a MAC authentication bypass-enabled port, perform these tasks in enabled mode:

Task	Command
Configure MAC authentication bypass.	<b>set mac-auth-bypass {enable   disable}</b>
Configure a PVLAN on a MAC authentication bypass-enabled port.	<b>set port mac-auth-bypass mod/port {enable   disable}</b>
Configure the PVLAN on the port.	<b>set pvlan primary vlan secondary vlan mod/port</b>

This example shows how to configure MAC authentication bypass-enabled on PVLAN port 3/13:

```
Console> (enable) set mac-auth-bypass enable
Mac-Auth-Bypass enabled globally.
Console> (enable) set port mac-auth-bypass 3/13 enable
Mac-Auth-Bypass successfully enabled on port(s) 3/13
Console> (enable) show port mac-auth-bypass 3/13
Port  Mac-Auth-Bypass State  MAC Address      Auth-State      Vlan
-----
3/13  Enabled                    00-00-00-00-00-00  waiting         25

Port  Termination action  Session Timeout  Shutdown/Time-Left
-----
3/13  initialize           3600             NO              -

Port  PolicyGroups
-----
3/13  -

Port  Critical Critical-Status
-----
3/13  Enabled -
Console> (enable) set pvlan 12 30 3/13
Host mode set to enable for port 3/13.
BPDU guard set to enable for port 3/13.
Trunk mode set to off for ports 3/13
```

```
Successfully set the following ports to Private Vlan 12,30:
3/13
Console> (enable)
```

## Configuring MAC Authentication Bypass on a PVLAN Port

To configure MAC authentication bypass on a PVLAN port, perform these tasks in enabled mode:

Task	Command
Configure the PVLAN on the port.	<b>set pvlan</b> <i>primary vlan secondary vlan mod/port</i>
Configure MAC authentication bypass.	<b>set mac-auth-bypass</b> {enable   disable}
Configure a PVLAN on a MAC authentication bypass-enabled port.	<b>set port mac-auth-bypass</b> <i>mod/port</i> {enable   disable}

This example shows how to configure MAC authentication bypass-enabled on PVLAN port 3/13:

```
Console> (enable) set pvlan 12 30 3/13
Successfully set the following ports to Private Vlan 12,30:
3/13
Console> (enable) set mac-auth-bypass enable
Mac-Auth-Bypass enabled globally.
Console> (enable) set port mac-auth-bypass 3/13 enable
Mac-Auth-Bypass successfully enabled on port(s) 3/13
Console> (enable)
```

## Displaying MAC Authentication Bypass Information

The **show port mac-auth-bypass** {*mod/port*} command displays the port state (such as authenticating, authenticated, and waiting to learn the source MAC address), and the port's RADIUS server-specified VLAN.

To display MAC authentication bypass information, perform these tasks in normal mode:

Task	Command
Display MAC authentication bypass information for all ports in the switch that have MAC authentication bypass enabled or for a single port.	<b>show port mac-auth-bypass</b> [ <i>mod/port</i> ]
Display MAC authentication bypass information for all ports in the switch that have MAC authentication bypass enabled or for the port with the specified MAC address.	<b>show mac-auth-bypass</b> {all   config   <i>mac_address</i> }

This example shows how to display MAC authentication bypass information for port 5/1:

```
Console> (enable) show port mac-auth-bypass 5/1
Port  Mac-Auth-Bypass State MAC Address      Auth-State      Vlan
-----
5/1   Disabled           -              -                1
```

```

Port Termination action Session Timeout Shutdown/Time-Left
-----
5/1 - 3600 - -
Console> (enable)

```

This example shows how to display MAC authentication bypass information for all ports in the switch that have MAC authentication bypass enabled:

```
Console> (enable) show mac-auth-bypass all
```

```

Port Mac-Auth-Bypass State MAC Address Auth-State Vlan
-----
5/1 Disabled - - 1
5/2 Enabled 00-00-00-00-00-00 waiting 1
5/3 Enabled 00-00-00-00-00-00 waiting 1
5/4 Enabled 00-00-00-00-00-00 waiting 1
5/5 Enabled 00-00-00-00-00-00 waiting 1
5/6 Enabled 00-00-00-00-00-00 waiting 1
5/7 Enabled 00-00-00-00-00-00 waiting 1
5/8 Enabled 00-00-00-00-00-00 waiting 1
.
.
.

```

```

Port Termination action Session Timeout Shutdown/Time-Left
-----
5/1 - 3600 - -
5/2 reauthenticate 3600 NO -
5/3 reauthenticate 3600 NO -
5/4 reauthenticate 3600 NO -
5/5 reauthenticate 3600 NO -
5/6 reauthenticate 3600 NO -
5/7 reauthenticate 3600 NO -
5/8 reauthenticate 3600 NO -
.
.
.
Console> (enable)

```

## Displaying the MAC Authentication Bypass Global Configuration

The **show mac-auth-bypass config** command displays MAC authentication bypass global configuration settings including the timer values, violation mode, global reauthentication mode, and so on.

To display MAC authentication bypass global configuration settings, perform this task in normal mode:

Task	Command
Display MAC authentication bypass global configuration settings.	<b>show mac-auth-bypass {all   config   mac_address}</b>

This example shows how to display MAC authentication bypass global configuration settings:

```

Console> (enable) show mac-auth-bypass config
Mac-Auth-Bypass Global Config
-----
Mac-Auth-Bypass Status = Enabled
AuthFail Timeout = 60
RadiusAccounting = Enabled
Reauthentication = Disabled
Reauth Timeout = 3600

```

```
Shutdown Timeout           = 60
Violation mode             = Shutdown
Console> (enable)
```

## Configuring MAC Authentication Bypass with ACL Assignments

MAC authentication bypass(MAB)-enabled ports support ACL assignments similar to 802.1X-enabled ports. For more information, see [“Configuring 802.1X with ACL Assignments” section on page 40-26](#).

The ACLs must be predefined and committed on the switch. ACL mapping by MAB is a runtime configuration and does not reflect in the NVRAM. The mapping is removed when the MAB static CAM entry is removed or at reauth, if the RADIUS sends a different or no ACL to map.

## Configuring MAC Authentication Bypass with QoS ACLs

MAC authentication bypass-enabled ports support ACLs sent by RADIUS and QoS policies-based authentication similar to QoS policies on 802.1X-enabled ports. For more information, see [“Configuring 802.1X with QoS ACLs” section on page 40-29](#).

When configuring MAB with QoS ACLs, follow these guidelines:

- The QoS ACLs must be predefined and committed on the switch.
- If more than one QoS ACL of the same attribute type (*invacl*, *outvacl*, or *inpacl*) is sent to the MAB port, only the first ACL for an attribute type is configured.
- The minimum acceptable reauthentication timeout for MAB has been reduced to 30 from 300 seconds. The default is 30 seconds.
- Dynamically applied QoS ACLs cannot be removed using commands. They are automatically removed when MAB initializes.

This example shows how to display the QoS ACLs information for a MAB-enabled port:

```
Console (enable)> show port mac-auth-bypass 3/13
Port  Mac-Auth-Bypass State MAC Address          Auth-State      Vlan
-----
3/13  Enabled              00-11-22-33-01-87 authenticated    391

Port  Termination action Session Timeout Shutdown/Time-Left
-----
3/13  initialize           3600           NO              -

Port  PolicyGroups
-----
3/13  -

Port  Security ACL                      Sec ACL Type    QoS ACL Type
-----
3/13  my_security_pacl                   Pacl             Vacl

Port  QoS Ingress Policy                  QoS Egress Policy
-----
3/13  my_qos_invacl                      my_qos_outvacl

Port  Critical Critical-Status
-----
3/13  Disabled -
```

# Configuring Agentless Hosts for NAC Auditing with MAB



## Note

Catalyst 6500 series software release 8.7(1) and later releases support NAC auditing for agentless hosts with MAC authentication bypass enabled. This feature is not supported on Supervisor Engine 2 and for agentless hosts with 802.1X enabled on other supervisor engines.

These sections describe how to audit agentless hosts with MAC authentication bypass enabled:

- [NAC Agentless Hosts Auditing Overview, page 41-14](#)
- [Configuring the Switch, page 41-14](#)
- [Configuring the Cisco Secure ACS Server, page 41-15](#)
- [Installing and Configuring the NAC Audit Server, page 41-16](#)
- [Displaying the Agentless Host Posture Tokens, page 41-16](#)
- [Interaction of Agentless Host Audit with Security Features, page 41-17](#)

## NAC Agentless Hosts Auditing Overview

Network Admission Control (NAC) enables the posture of an endpoint device to check for compliance with the security policy before the device accesses the protected areas of a network. NAC allows the host posture to be determined using either the Posture Agent (PA), or using the audit server for agentless hosts if the PA is not installed on the host.

Several methods in NAC allow network access to hosts that cannot perform authentication because of the lack of posture agent. Agentless hosts are such as printers, scanners, and hosts with unsupported operating systems. One method is to use an external audit server with agentless hosts connected to MAC authentication bypass-enabled NAD ports. To determine the posture, the MAC address must be registered, and shared profiles and admission policies must be created on a centralized ACS server.

Audit servers have the ability to probe and scan the clientless devices for security compliance, vulnerabilities, and threats. The result of the audit sever can influence access servers to make host specific network access policy decisions rather than enforce a common restrictive policy for all nonresponsive hosts.

## Configuring the Switch

For the NAC audit server to determine the posture of agentless hosts, perform these tasks in privileged mode:

	Task	Command
Step 1	Enable MAC authentication bypass globally on the switch.	<b>set mac-auth-bypass enable</b>
Step 2	Enable MAC authentication bypass reauthentication on the switch.	<b>set mac-auth-bypass reauthentication enable</b>
Step 3	Enable MAC authentication bypass on a per-port basis.	<b>set port mac-auth-bypass <i>mod/port</i> enable</b>

When configuring the switch, follow these guidelines:

- The switch must have a RADIUS configuration and be connected to the Cisco Secure ACS server.
- If the audit configuration is removed from the network access profile (NAP) of MAB, the port needs to be reinitialized.
- The session-timeout value must be greater than the time required for the DACL to download all the ACLs and it must be determined based on other audit requirements.

## Configuring the Cisco Secure ACS Server

For auditing agentless hosts, the switch must be connected to a Cisco Secure ACS server and a third-party NAC audit server such as Qualys. When the audit server is installed and running, configure the audit server information on the ACS server. Cisco Secure ACS server 4.1 or later is required for this feature to function properly.

To configure the ACS server with NAC agentless hosts and NAC audit server information, perform these steps:

- 
- Step 1** Import the NAC audit vendor trusted root CA to the certificate store on ACS by using the **CSUtil** tool.
  - Step 2** Import an audit device-type attribute file for the NAC audit server by using **CSUtil**.
  - Step 3** Import NAC attribute-value pairs for the audit vendor by using **CSUtil**.
  - Step 4** Enable posture validation on the ACS.
  - Step 5** Configure the external audit server on ACS using the external posture validation audit server setup page on the ACS.
  - Step 6** Define shared profile components.
  - Step 7** Configure network access profile (NAP) authorization policy.



---

**Note** In the NAP profile, configure MAB, specify the audit server, DACL or shared RAC policies to be applied for the various posture tokens, and the fail open policy to be applied when the audit server cannot communicate with the host.

---

- Step 8** Configure the hosts to be audited, and device-type retrieval and mapping for audit vendors who have a device attribute in the RADIUS dictionary using the external audit server posture validation setup page on the ACS.
- Step 9** Set up a device group policy on the ACS.

For more information about auditing agentless hosts, and detailed steps to complete each of these tasks, refer to the following documents:

- *Configuration Guide for CISCO Secure ACS*
- *NAC Framework Configuration Guide*
- *NAC Audit Vendor Configuration Guide*

## Installing and Configuring the NAC Audit Server

For information regarding installing and configuring the NAC audit server, refer to the NAC Audit vendor documentation shipped with the audit server. Ensure that the audit server is physically connected to the switch before you install and configure it.

## Displaying the Agentless Host Posture Tokens

The agentless host is evaluated on the number of vulnerabilities found and their severity levels. This vulnerability information is taken from the cached audit report, and the posture token is determined by the evaluation method settings on the NAC audit server.

The agentless host can hold any of the following posture agents:

- **Infected**—When at least one Severity 5 vulnerability is detected. Infected host audit reports are cached and expire after 5 minutes.
- **Quarantine**—When at least one Severity 4 vulnerability is detected. Quarantine host audit reports are cached and expire after 10 minutes.
- **Check-up**—When at least one Severity 3 vulnerability is detected. Check-up host audit reports are cached and expire after 1 hour.
- **Healthy**—When no severity 5, 4, or 3 vulnerabilities are detected. Healthy host audit reports are cached and expire after 24 hours.
- **Unknown**—When nonexistent and dead hosts do not respond to probes. Unknown host audit reports are cached and expire after 12 hours.



### Note

There will be a delay in traffic because of auditing and the host would hold a transition posture token during such delay.

This example shows how to display the posture tokens of a MAC authentication bypass-enabled port:

```

Console> (enable) show port mac-auth-bypass 6/25
Port  Mac-Auth-Bypass State   MAC Address  Auth-State  Vlan
-----
6/25  Disabled              -            -           5

Port  Termination action  Session Timeout  Shutdown/Time-Left
-----
6/25  -                    3600             NO          -

Port  PolicyGroups
-----
6/25  -

Port  Critical      Critical-Status
-----
6/25  Disabled      -

Port  Session-id
-----
6/25  000015a90000099a000019ba000003e1

Port  Posture -Token  Url-Redirect
-----
6/25  Healthy        http://10.76.255.100:2002

```

## Interaction of Agentless Host Audit with Security Features

This section describes the behavior of NAC audit with other security features:

- 802.1X—When ACS audits a 802.1X-authenticated port, it checks for the MAB configuration. ACS audits the port only if MAB is enabled, otherwise it considers the port to be part of a guest VLAN.
- MAB—Regardless of how MAB is triggered, audit runs unless MAB fails.
- Layer 3 features—Not affected by MAB-enabled agentless host audit.
- Critical-Auth—Because there is no RADIUS server, no interaction is possible and the old posture (if any) is maintained.
- PVLAN—No effect.

