Configuring MAC Authentication Bypass

Last Updated: July 18, 2011

The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco Identity Based Networking Services (IBNS) and Network Admission Control (NAC) strategy using the client MAC address. The MAC Authentication Bypass feature is applicable to the following network environments:

- Network environments in which a supplicant code is not available for a given client platform.
- Network environments in which the end client configuration is not under administrative control, that is, the IEEE 802.1X requests are not supported on these networks.

Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1X capability or credentials. As a result, devices such as cash registers, fax machines, and printers can be readily authenticated, and network features that are based on authorization policies can be made available.

Before standalone MAB support was available, MAB could be configured only as a failover method for 802.1x authentication. Standalone MAB is independent of 802.1x authentication.

- Finding Feature Information, page 1
- Prerequisites for Configuring MAC Authentication Bypass, page 2
- Information About Configuring MAC Authentication Bypass, page 2
- How to Configure Configuring MAC Authentication Bypass, page 3
- Configuration Examples for Configuring MAC Authentication Bypass, page 10
- Additional References, page 11
- Feature Information for Configuring MAC Authentication Bypass, page 12

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information

about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring MAC Authentication Bypass

IEEE 802.1x--Port-Based Network Access Control

You should understand the concepts of port-based network access control and have an understanding of how to configure port-based network access control on your Cisco platform. See the *Cisco IOS Security Configuration Guide: Securing User Services* , Release 15.0, for more information.

RADIUS and ACLs

You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs). For more information, see the documentation for your Cisco platform and the *Cisco IOS Security Configuration Guide: Securing User Services* , Release 15.0.

The switch must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). For more information, see the *User Guide for Secure ACS Appliance 3.2* .

Information About Configuring MAC Authentication Bypass

- Overview of the Cisco IOS Auth Manager, page 2
- Standalone MAB, page 3

Overview of the Cisco IOS Auth Manager

The capabilities of devices connecting to a given network can be different, thus requiring that the network support different authentication methods and authorization policies. The Cisco IOS Auth Manager handles network authentication requests and enforces authorization policies regardless of authentication method. The Auth Manager maintains operational data for all port-based network connection attempts, authentications, authorizations, and disconnections and, as such, serves as a session manager.

The possible states for Auth Manager sessions are as follows:

- Idle--In the idle state, the authentication session has been initialized, but no methods have yet been run. This is an intermediate state.
- Running--A method is currently running. This is an intermediate state.
- Authc Success--The authentication method has run successfully. This is an intermediate state.
- Authc Failed--The authentication method has failed. This is an intermediate state.
- Authz Success--All features have been successfully applied for this session. This is a terminal state.
- Authz Failed--At least one feature has failed to be applied for this session. This is a terminal state.
- No methods--No method provided a result for this session. This is a terminal state.

Standalone MAB

MAB uses the MAC address of the connecting device to grant or deny network access. To support MAB, the RADIUS authentication server maintains a database of MAC addresses for devices that require access to the network. MAB generates a RADIUS request with a MAC address in the Calling-Station-Id (attribute 31) and Service-Type (attribute 6) with a value of 10. After a successful authentication, the Auth Manager enables various authorization features specified by the authorization policy, such as ACL assignment and VLAN assignment.

How to Configure Configuring MAC Authentication Bypass

- Enabling MAC Authentication Bypass, page 3
- Enabling Standalone MAB, page 4
- Enabling Reauthentication on a Port, page 6
- Specifying the Security Violation Mode, page 8

Enabling MAC Authentication Bypass

Perform this task to enable the MAC Authentication Bypass feature on an 802.1X port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **dot1x mac-auth-bypass** [**eap**]
5. **end**
6. **show dot1x interface** *type slot / port* **details**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type slot* / *port* **Example:** `Router(config)# interface FastEthernet 2/1`	Enters interface configuration mode.
Step 4	**dot1x mac-auth-bypass** [**eap**] **Example:** `Router(config-if)# dot1x mac-auth-bypass`	Enables the MAC Authentication Bypass (MAB) feature on an 802.1X Port.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privilege EXEC mode.
Step 6	**show dot1x interface** *type slot* / *port* **details** **Example:** `Router# show dot1x interface FastEthernet 2/1 details`	Displays the interface configuration and the authenticator instances on the interface.

Enabling Standalone MAB

Ports enabled with the Standalone MAB feature can use the MAC address of connecting devices to grant or deny network access. Perform the steps described in this section to enable standalone MAB on individual ports.

Before you can configure standalone MAB, the switch must be connected to a Cisco Secure ACS server and RADIUS authentication, authorization, and accounting (AAA) must be configured.

Note Standalone MAB can be configured on switched ports only--it cannot be configured on routed ports.

Note If you are unsure whether MAB or MAB EAP is enabled or disabled on the switched port, use t **mab**or **default mab eap** commands in interface configuration mode to configure MAB or MAI default.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
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	**interface** *type slot* / *port* **Example:** `Switch(config)# interface FastEthernet2/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Switch(config-if)# switchport`	Places interface in Layer2-switched mode.
Step 5	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets a nontrunking, nontagged single VLAN Layer 2 interface.

	Command or Action	Purpose
Step 6	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Configures the authorization state of the port.
Step 7	**mab** [**eap**] **Example:** `Switch(config-if)# mab`	Enables MAB.
Step 8	**end** **Example:** `Switch(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

- Troubleshooting Tips, page 6

Troubleshooting Tips

The following commands can help troubleshoot standalone MAB:

- **debug authentication**
- **debug mab all**
- **show authentication registrations**
- **show authentication sessions**
- **show mab**

Enabling Reauthentication on a Port

By default, ports are not automatically reauthenticated. You can enable automatic reauthentication and specify how often reauthentication attempts are made.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication periodic**
9. **authentication timer reauthenticate** {*seconds* | **server**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
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	**interface** *type slot* / *port* **Example:** `Switch(config)# interface FastEthernet2/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Switch(config-if)# switchport`	Places interface in Layer2-switched mode.
Step 5	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets a nontrunking, nontagged single VLAN Layer 2 interface.

	Command or Action	Purpose
Step 6	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Configures the authorization state of the port.
Step 7	**mab** [**eap**] **Example:** `Switch(config-if)# mab`	Enables MAB.
Step 8	**authentication periodic** **Example:** `Switch(config-if)# authentication periodic`	Enables reauthentication.
Step 9	**authentication timer reauthenticate** {*seconds* | **server**} **Example:** `Switch(config-if)# authentication timer reauthenticate 900`	Configures the time, in seconds, between reauthentication attempts.
Step 10	**end** **Example:** `Switch(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Specifying the Security Violation Mode

When there is a security violation on a port, the port can be shut down or traffic can be restricted. By default, the port is shut down. You can configure the period of time for which the port is shut down.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication violation** {**restrict** | **shutdown**}
9. **authentication timer restart** *seconds*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
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	**interface** *type slot* / *port* **Example:** `Switch(config)# interface FastEthernet2/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Switch(config-if)# switchport`	Places interface in Layer2-switched mode.
Step 5	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets a nontrunking, nontagged single VLAN Layer 2 interface.

	Command or Action	Purpose
Step 6	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Configures the authorization state of the port.
Step 7	**mab** [**eap**] **Example:** `Switch(config-if)# mab`	Enables MAB.
Step 8	**authentication violation** {**restrict** | **shutdown**} **Example:** `Switch(config-if)# authentication violation shutdown`	Configures the action to be taken when a security violation occurs on the port.
Step 9	**authentication timer restart** *seconds* **Example:** `Switch(config-if)# authentication timer restart 30`	Configures the period of time, in seconds, after which an attempt is made to authenticate an unauthorized port.
Step 10	**end** **Example:** `Switch(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Configuring MAC Authentication Bypass

- Example Standalone MAB Configuration, page 10

Example Standalone MAB Configuration

The following example shows how to configure standalone MAB on a port. In this example, the client is reauthenticated every 1200 seconds and the connection is dropped after 600 seconds of inactivity.

```
enable
 configure terminal
  interface GigabitEthernet2/1
   switchport
```

```
switchport mode access
switchport access vlan 2
authentication port-control auto
mab
authentication violation shutdown
authentication timer restart 30
authentication periodic
authentication timer reauthenticate 1200
authentication timer inactivity 600
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Authentication commands	*Cisco IOS Security Command Reference*
IEEE 802.1x--Flexible Authentication	*Cisco IOS Security Configuration Guide: Securing User Services*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3580	*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring MAC Authentication Bypass

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Configuring MAC Authentication Bypass

Feature Name	Releases	Feature Information
MAC Authentication Bypass (MAB)	12.1(22)T 12.2(31)SG 12.2(33)SXH15.1(4)M	The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco IBNS and NAC strategy using the client MAC address. In Cisco IOS Release 15.1(4)M support was extended for Integrated Services Router Generation 2 (ISR G2) platforms. The following commands were introduced or modified: **dot1x mac-auth-bypass**, **show dot1x interface**.

Feature Name	Releases	Feature Information
Standalone MAB Support	12.2(33)SXI	This feature grants network access to devices based on MAC address regardless of 802.1x capability or credentials. The following commands were introduced or modified: **authentication periodic**, **authentication port-control**, **authentication timer inactivity**, **authentication timer reauthenticate**, **authentication timer restart**, **authentication violation**, **debug authentication**, **mab**, **show authentication interface**, **show mab**, **show authentication registrations**, **show authentication sessions**.