MAC Authentication Bypass

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.

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.

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 *Securing User Services Configuration Guide Library*.

The device 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 MAC Authentication Bypass

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—There were no results for this session. This is a terminal state.

Overview of the Configurable MAB Username and Password

A MAC Authentication Bypass (MAB) operation involves authentication using RADIUS Access-Request packets with both the username and password attributes. By default, the username and the password values are the same and contain the MAC address. The Configurable MAB Username and Password feature enables you to configure both the username and the password attributes in the following scenarios:

- To enable MAB for an existing large database that uses formatted username attributes, the username format in the client MAC needs to be configured. Use the **mab request format attribute 1** command to configure the username format.
- Some databases do not accept authentication if the username and password values are the same. In such instances, the password needs to be configured to ensure that the password is different from the username. Use the **mab request format attribute 2** command to configure the password.

The Configurable MAB Username and Password feature allows interoperability between the Cisco IOS Authentication Manager and the existing MAC databases and RADIUS servers. The password is a global password and hence is the same for all MAB authentications and interfaces. This password is also synchronized across all supervisor devices to achieve high availability.

If the password is not provided or configured, the password uses the same value as the username. The table below describes the formatting of the username and the password:

MAC Address	Username Format (Group Size, Separator)	Username	Password Configured	Password Created
08002b8619de	(1, :) (1, -) (1, .)	0:8:0:0:2:b:8:6:1:9:d:e 0-8-0-0-2-b-8-6-1-9-d-e 0.8.0.0.2.b.8.6.1.9.d.e	None	0:8:0:0:2:b:8:6:1:9:d:e 0-8-0-0-2-b-8-6-1-9-d-e 0.8.0.0.2.b.8.6.1.9.d.e
08002b8619de	(1, :) (1, -) (1, .)	0:8:0:0:2:b:8:6:1:9:d:e 0-8-0-0-2-b-8-6-1-9-d-e 0.8.0.0.2.b.8.6.1.9.d.e	Password	Password
08002b8619de	(2, :) (2, -) (2, .)	08:00:2b:86:19:de 08-00-2b-86-19-de 08.00.2b.86.19.de	None	08:00:2b:86:19:de 08-00-2b-86-19-de 08.00.2b.86.19.de
08002b8619de	(2, :) (2, -) (2, .)	08:00:2b:86:19:de 08-00-2b-86-19-de 08.00.2b.86.19.de	Password	Password
08002b8619de	(4, :) (4, -) (4, .)	0800:2b86:19de 0800-2b86-19de 0800.2b86.19de	None	0800:2b86:19de 0800-2b86-19de 0800.2b86.19de
08002b8619de	(4, :) (4, -) (4, .)	0800:2b86:19de 0800-2b86-19de 0800.2b86.19de	Password	Password
08002b8619de	(12, <not applicable>)	08002b8619de	None	08002b8619de
08002b8619de	(12, <not applicable>)	08002b8619de	Password	Password

How to Configure MAC Authentication Bypass

Enabling MAC Authentication Bypass

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

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot / port* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Enters interface configuration mode.
Step 4	**mab** **Example:** `Device(config-if)# mab`	Enables MAB.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show authentication sessions interface** *type slot / port* **details** **Example:** `Device# show authentication sessions interface gigabitethernet 1/0/1`	Displays the interface configuration and the authenticator instances on the interface.

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.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* / *port* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Device(config-if)# switchport`	Places interface in Layer 2 switched mode.
Step 5	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	**authentication port-control auto** **Example:** `Device(config-if)# authentication port-control auto`	Configures the authorization state of the port.
Step 7	**mab** [**eap**] **Example:** `Device(config-if)# mab`	Enables MAB.
Step 8	**authentication periodic** **Example:** `Device(config-if)# authentication periodic`	Enables reauthentication.
Step 9	**authentication timer reauthenticate** {*seconds* | **server**} **Example:** `Device(config-if)# authentication timer reauthenticate 900`	Configures the time, in seconds, between reauthentication attempts.
Step 10	**end** **Example:**	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	

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.

Procedure

	Command or Action	Purpose
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** *type slot / port* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Device(config-if)# switchport`	Places interface in Layer 2 switched mode.
Step 5	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	**authentication port-control auto** **Example:** `Device(config-if)# authentication port-control auto`	Configures the authorization state of the port.
Step 7	**mab** [**eap**] **Example:**	Enables MAB.

	Command or Action	Purpose
	`Device(config-if)# mab`	
Step 8	**authentication violation** {**protect** | **replace** | **restrict** | **shutdown**} **Example:** `Device(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:** `Device(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:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling Configurable MAB Username and Password

Procedure

	Command or Action	Purpose
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	**mab request format attribute 1 groupsize** {**1** | **2** | **4** | **12**} **separator** {**-** | **:** | **.**} [**lowercase** | **uppercase**] **Example:** `Device(config)# mab request format attribute 1 groupsize 2 separator :`	Configures the username format for MAB requests.
Step 4	**mab request format attribute 2** [**0** | **7**] *password* **Example:** `Device(config)# mab request format attribute 2 password1`	Configures a global password for all MAB requests.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuration Examples for MAC Authentication Bypass

Example: MAC Authentication Bypass Configuration

In the following example, the **mab** command has been configured to enable the MAC Authorization Bypass (MAB) feature on the specified interface. The optional **show authentication sessions** command has been enabled to display the interface configuration and the authentication instances on the interface.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# mab
Device(config-if)# end
Device# show authentication sessions interface gigabitethernet 1/0/1 details
```

Example: Enabling Configurable MAB Username and Password

The following example shows how to configure the username format and password for MAC Authentication Bypass (MAB). In this example, the username format is configured as a group of 12 hexadecimal digits with no separator and the global password as **password1**.

```
Device> enable
Device# configure terminal
Device(config)# mab request format attribute 1 groupsize 2 separator :
Device(config)# mab request format attribute 2 password1
Device(config)# end
```

Additional References for MAC Authentication Bypass

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst Micro Switches)*

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 History for MAC Authentication Bypass

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	Feature Information
Cisco IOS Release 15.2(7)E3k	MAC Authentication Bypass	The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the IBNS and NAC strategy using the client MAC address.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.