Standalone MAB Support

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

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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.

Information About Configuring Standalone MAB

Standalone MAB

MAC Authentication Bypass (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 with a Service-Type (attribute 6) 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 Standalone MAB Support

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 Begin

Before you can configure standalone MAB, the device 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 devices with switched ports only; it cannot be configured on devices with routed ports.

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

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**
8. **end**

DETAILED STEPS

	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 FastEthernet2/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Switch(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 a as 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** **Example:** `Device(config-if)# mab`	Enables MAB.
Step 8	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

The following commands can help troubleshoot standalone MAB:

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

Configuration Examples for Standalone MAB Support

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.

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet2/1
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 2
Device(config-if)# authentication port-control auto
Device(config-if)# mab
Device(config-if)# authentication violation shutdown
Device(config-if)# authentication timer restart 30
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate 1200
Device(config-if)# authentication timer inactivity 600
```

Additional References

Related Documents

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

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 Standalone MAB Support

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 Standalone MAB Support

Feature Name	Releases	Feature Information
Standalone MAB Support	12.2(33)SXI 15.2(2)T	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 authentication registrations**, **show authentication sessions**, and **show mab**.