IEEE 802.1X Flexible Authentication

The IEEE 802.1X Flexible Authentication feature provides a means of assigning authentication methods to ports and specifying the order in which the methods are executed when an authentication attempt fails. Using this feature, you can control which ports use which authentication methods, and you can control the failover sequencing of methods on those ports.

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.

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 IEEE 802.1X Flexible Authentication

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. For more information, see the *Configuring IEEE 802.1X Port-Based Authentication* module.

Before you can use the IEEE 802.1X Flexible Authentication feature, the switch must be connected to a Cisco secure access control server (ACS) and RADIUS authentication, authorization, and accounting (AAA) must be configured for web authentication. If appropriate, you must enable access control list (ACL) download.

If the authentication order includes the 802.1X port authentication method, you must enable IEEE 802.1X authentication on the switch.

If the authentication order includes web authentication, configure a fallback profile that enables web authentication on the switch and the interface.

RADIUS and ACLs

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

The switch must have a RADIUS configuration and be connected to the Cisco secure ACS. For more information, see the Configuration Guide for *Cisco Secure ACS*.

Restrictions for IEEE 802.1X Flexible Authentication

- The web authentication method cannot fail over to the 802.1X or the MAC Authentication Bypass (MAB) authentication method.

Note No authentication method can follow web authentication in the configuration order. Web authentication must be the last method configured.

- The web authentication method is not supported on Cisco integrated services routers (ISRs) or Integrated Services Routers Generation 2 (ISR-G2s) in Cisco IOS Release 15.2(2)T.
- Layer 2 web authentication is not supported with flexible authentication.
- This feature does not support standard ACLs on the switch port.
- Configuring the same VLAN ID for both access and voice traffic (using the **switchport access vlan** *vlan-id* and the **switchport voice vlan** *vlan-id* commands) will fail if authentication has already been configured on the port.
- Configuring authentication on a port on which you have already configured **switchport access vlan** *vlan-id* and **switchport voice vlan** *vlan-id* will fail if the access VLAN and voice VLAN have been configured with the same VLAN ID.

Information About IEEE 802.1X Flexible Authentication

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:

- 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.
- Idle—In the idle state, the authentication session has been initialized, but no methods have yet been run. This is an intermediate state.
- No methods—No method provided a result for this session. This is a terminal state.
- Running—A method is currently running. This is an intermediate state.

IEEE 802.1X Flexible Authentication Methods

The IEEE 802.1X Flexible Authentication feature supports three authentication methods:

- dot1X—IEEE 802.1X authentication is a Layer 2 authentication method.
- mab—MAC-Authentication Bypass is a Layer 2 authentication method.
- webauth—Web authentication is a Layer 3 authentication method.

IEEE 802.1X Host Mode Authentication

The IEEE 802.1X Flexible Authentication feature supports the following host modes:

- multi-auth—Multiauthentication allows one authentication on a voice VLAN and multiple authentications on the data VLAN.
- multi-domain—Multidomain authentication allows two authentications: one on the voice VLAN and one on the data VLAN.

IEEE 802.1X Authentication Order and Authentication Priority

The IEEE 802.1X Flexible Authentication feature enables authentication order and authentication priority. The **authentication order** command sets the default authentication priority. You can use the **authentication priority** command to override the default authentication priority. For example, you might specify an authentication order of MAB and 802.1X. However, after authorization, you might not want to ignore subsequent 802.1X handshakes. In this case, you can give the 802.1X authentication method a higher priority than the MAB method.

How to Configure IEEE 802.1X Flexible Authentication

Configuring Authentication Order

Authentication order is configured on individual ports to control which ports use which authentication methods.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x system-auth-control**
4. **interface type** *slot/port*
5. **switchport**
6. **switchport mode access**
7. **switchport access vlan** *vlan-id*
8. **mab** [**eap**]
9. **access-session port-control**{**auto**|**force-authorized**|**force unauthorized**}
10. **authentication** *fallback profile*
11. **authentication order**{**dot1x** [**mab** |**webauth**][**webauth**] |**mab** [**dot1x**|**webauth**] [**webauth**] |**webauth**}
12. **dot1x pae authenticator**
13. **end**

DETAILED STEPS

	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	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	(Optional) Enables IEEE 802.1x authentication globally on the switch. • Enable IEEE 802.1x authentication if the authentication order includes the **dot1x** authentication method.
Step 4	**interface type** *slot/port* **Example:** `Device(config)# interface Gigabitethernet 1/2/1`	Enters interface configuration mode.
Step 5	**switchport** **Example:** `Device(config-if)# switchport`	Places the interface in Layer 2-switched mode.
Step 6	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
Step 7	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 2`	Sets the VLAN for the port.
Step 8	**mab** [**eap**] **Example:** `Device(config-if)# mab`	(Optional) Enables MAB. • Enable MAB if the authentication order includes the **mab** keyword (see Step 11).
Step 9	**access-session port-control** {**auto**|**force-authorized**|**force unauthorized**} **Example:** `Device(config-if)# access-session port-control auto`	Configures the authorization state of the port.
Step 10	**authentication** *fallback profile* **Example:** `Device(config-if)# authentication fallback web-profile`	Configures the authorization state of the port and enables web authentication. • Enable web authentication if the authentication order includes the **webauth** keyword (see Step 11).

	Command or Action	Purpose
Step 11	**authentication order** {**dot1x** [**mab** |**webauth**][**webauth**] |**mab** [**dot1x**|**webauth**] [**webauth**] |**webauth**} **Example:** `Device(config-if)# authentication order mab dot1x webauth`	Configures the authentication order.
Step 12	**dot1x pae authenticator** **Example:** `Device(config-if)# dot1x pae authenticator`	Enables the port to respond to messages meant for an IEEE 802.1x authenticator.
Step 13	**end** **Example:** `Device(config-if)# end`	Returns to global configuration mode.

Configuring Authentication Priority

Authentication priority is configured to control the fail-over sequencing of methods on individual ports.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *typeslot/port*
4. **authentication priority** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
5. **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.

	Command or Action	Purpose
Step 3	**interface** *typeslot/port* **Example:** `Switch(config)# interface Gigabitethernet 1/2/1`	Enters interface configuration mode.
Step 4	**authentication priority** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**} **Example:** `Switch(config-if)# authentication priority dot1x mab webauth`	Configures authentication priority.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to global configuration mode.

Configuration Examples for IEEE 802.1X Flexible Authentication

Example: Configuring IEEE 802.1X Flexible Authentication

The following example shows the commands used to configure the port in multiple authentication host mode. The order of authentication is 802.1X first, then MAB, and finally web authentication:

```
enable
configure terminal
dot1x system-auth-control

aaa new-model
aaa authentication login default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa session-id common
ip http server

ip admission name webauth-rule proxy http
fallback profile webauth-profile
 ip access-group webauthlist in
 ip admission webauth-rule

interface GigabitEthernet 2/1
 switchport
 switchport mode access
 switchport access vlan 125
 switchport voice vlan 127
 mab
 authentication port-control auto
 authentication fallback webauth-profile
 authentication host-mode multi-auth
 authentication order dot1x mab webauth
 dot1x pae authenticator
```

Additional References

Related Documents

Related Topic	Document Title
Authentication commands	*Cisco IOS Security Command Reference Commands A to C*
IEEE 802.1x commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	• *Catalyst 4500 Series Switch Cisco IOS Command Reference, Release 12.2(25)SGA* • *Catalyst 3750 Switch Command Reference, Cisco IOS Release 12.2(25)SEE*
IPSec	• *IPsec Management Configuration Guide, Cisco IOS Release 15.2MT* • *Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15.2MT* • *Security for VPNs with IPsec Configuration Guide, Cisco IOS Release 15.2MT*
RADIUS	*RADIUS Configuration Guide, Cisco IOS Release 15.2MT*
Standalone MAB support	*Standalone MAB Support*
Port-based network access control	"Configuring IEEE 802.1X Port-Based Authentication"*Configuring IEEE 802.1X Port-Based Authentication* module. module.

Standards and RFCs

Standard/RFC	Title
IEEE 802.1X protocol	—
RFC 3580	IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)

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 releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 IEEE 802.1X Flexible Authentication

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 . An account on Cisco.com is not required.

Table 1: Feature Information for IEEE 802.1X Flexible Authentication

Feature Name	Releases	Feature Information
IEEE 8021.X Flexible Authentication	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE	This feature provides a means of configuring ports with one or more authentication methods and specifying the order in which those authentication methods are attempted. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers. The following commands were introduced or modified: **authentication fallback**, **authentication hostmode**, **authentication order**, **authentication port-control** **authentication priority**, **authentication timer restart**, **debug authentication**, **mab**, **show authentication interface**, **show authentication registrations**, **show authentication sessions**, **showmab**. The following commands were removed or made obsolete: **dot1x fallback**, **dot1x host-mode**, **dot1x port-control**.