# IEEE 802.1X Multiple Authentication

The IEEE 802.1X Multiple Authentication feature provides a means of authenticating multiple hosts on a single port. With both 802.1X and non-802.1X devices, multiple hosts can be authenticated using different methods. Each host is individually authenticated before it can gain access to the network resources.

# 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 Multiple 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.

Before you can use the IEEE 802.1X Multiple Authentication feature, the switch must be connected to a Cisco secure Access Control Server and RADIUS authentication, authorization, and accounting (AAA) must be configured for web authentication. ACL download must be enabled.

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 access control lists (ACLs).

The switch must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS).

# Restrictions for IEEE 802.1X Multiple Authentication

- Only one voice VLAN is supported on a multiple authentication port.
- You cannot configure a guest VLAN or an authentication failed VLAN in multiple authentication mode.
- When a port is in multiple authentication mode, the guest VLAN and authentication failed VLAN features do not activate.
- In multiple authentication mode, only multicast EAPOL packets are accepted by the port.
- The web authentication method is not supported on Cisco integrated services routers (ISRs) or Integrated Services Routers Generation 2 (ISR-G2s) in Cisco IOS 15.2(2)T.
- Inactivity aging is not supported on Cisco ISRs or ISR-G2s in multiple authentication mode.
- 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 Multiple Authentication

# Guidelines for Configuring IEEE 802.1X Multiple Authentication

Assign a RADIUS-server-supplied VLAN in multiple authentication mode, under these conditions:

- The host is the first host authorized on the port, and the RADIUS server supplies VLAN information.
- Subsequent hosts are authorized with a VLAN that matches the operational VLAN.

- A host is authorized on the port with no VLAN assignment, and subsequent hosts either have no VLAN assignment, or their VLAN information matches the operational VLAN.

- The first host authorized on the port has a group VLAN assignment, and subsequent hosts either have no VLAN assignment, or their group VLAN matches the group VLAN on the port. Subsequent hosts must use the same VLAN from the VLAN group as the first host. If a VLAN list is used, all hosts are subject to the conditions specified in the VLAN list.

- Only one voice VLAN assignment is supported on a multi-auth port .

- After a VLAN is assigned to a host on the port, subsequent hosts must have matching VLAN information or be denied access to the port.

- You cannot configure a guest VLAN or an auth-fail VLAN in multi-auth mode.

- The behavior of the critical-auth VLAN is not changed for multi-auth mode. When a host tries to authenticate and the server is not reachable, all authorized hosts are reinitialized in the configured VLAN.

# How to Configure IEEE 802.1X Multiple Authentication

## Configuring IEEE 802.1X Multiple Authentication

Beginning in privileged EXEC mode, follow these steps to allow one client on the voice VLAN and multiple authenticated clients on the data VLAN, where each host is individually authenticated.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *interface-id*
5. **access-session host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] *interface-id*
6. **end**
7. **show access-session interface** *interface-id*
8. **copy running-config startup-config**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **radius-server vsa send authentication**<br><br>**Example:**<br>`Device(config)# radius-server vsa send authentication` | Configures the Network Access Server (NAS) to recognize and use vendor-specific attributes. |
| **Step 4** | **interface** *interface-id*<br><br>**Example:** | Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode. |
| **Step 5** | **access-session host-mode** [**multi-auth** \| **multi-domain** \| **multi-host** \| **single-host**] *interface-id*<br><br>**Example:**<br>`Device(config-if)# access-session host-mode multi-auth` | Allows one client on the voice VLAN and multiple authenticated clients on the data VLAN.<br><br>• Each host is individually authenticated. |
| **Step 6** | **end**<br><br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show access-session interface** *interface-id*<br><br>**Example:**<br>`Device# show access-session interface g1/0/23` | Verifies the entries. |
| **Step 8** | **copy running-config startup-config**<br><br>**Example:**<br>`Device# copy running-config startup-config` | Saves entries in the configuration file. |

# Configuration Examples for IEEE 802.1X Multiple Authentication

## Example: Configuring IEEE 802.1X Multiple Authentication

```
aaa new-model
!
!
aaa authentication login CON local
aaa authentication login VTY local
```

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
!
aaa session-id common
!
dot1x system-auth-control
!

interface Gigabitethernet1/1/1
 switchport access vlan 20
 switchport voice vlan 117
 no ip address
 authentication host-mode multi-auth
 authentication order mab
 authentication port-control auto
 mab
 dot1x pae authenticator
end
```

# 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 Command Reference, Cisco IOS Release 12.2(25)SGA*<br><br>• *Catalyst 3750 Switch Command Reference, Cisco IOS Release 12.2(25)SEE* |
| IPSec | • IPsec Management Configuration Guide, Cisco IOS Release 15.2MT<br><br>• Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15.2MT<br><br>• 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 |

**Standards**

| Standard | Title |
|---|---|
| IEEE 802.1X protocol | — |

**MIBs**

| MIB | MIBs Link |
|---|---|
| CISCO–AUTH–FRAMEWORK–MIB<br>CISCO–MAC–AUTH–BYPASS–MIB<br>CISCO–PAE–MIB<br>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:<br><br>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 IEEE 802.1X Multiple 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 1: Feature Information for IEEE 802.1X Multiple Authentication*

| Feature Name | Releases | Feature Information |
|---|---|---|
| IEEE 8021.X Multiple Authentication | Cisco IOS XE 3.2SE<br><br>Cisco IOS XE 3.3SE<br><br>Cisco IOS XE Release 3.6E | The IEEE 802.1X Multiple Authentication feature provides a means of authenticating multiple hosts on a single port. With both 802.1X and non-802.1X devices, multiple hosts can be authenticated using different methods. Each host is individually authenticated before it can gain access to the network resources.<br><br>In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms:<br><br>• Catalyst 3850 Series Switches<br><br>• Cisco 5760 Wireless LAN Controller<br><br>In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms:<br><br>• Catalyst 3650 Series Switches<br><br>• Cisco Catalyst 3850 Series Switches.<br><br>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.<br><br>The following commands were introduced or modified: **authentication host-mode**. |