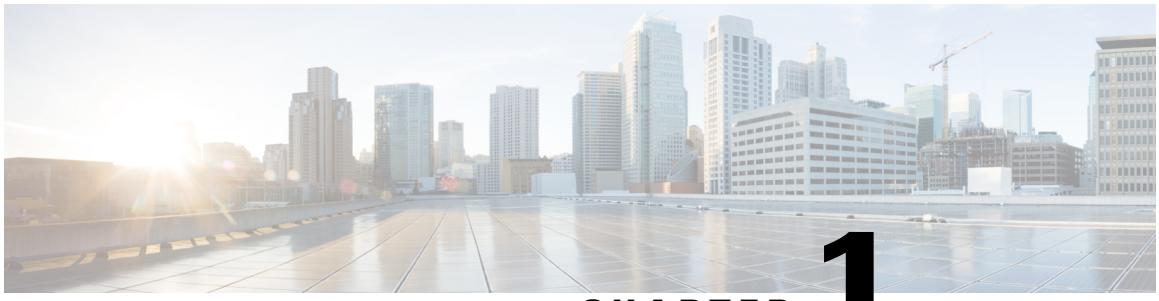
802.1X Authentication Services Configuration Guide, Cisco IOS Release 15E

First Published: 2013-08-06

Last Modified: 2013-08-06

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Configuring IEEE 802.1X Port-Based Authentication

IEEE 802.1X port-based authentication is configured on a device to prevent unauthorized devices (supplicants) from gaining access to the network. The device can combine the function of a router, switch, and access point, depending on the fixed configuration or installed modules. The switch functions are provided by either built-in switch ports or a plug-in module with switch ports. This feature supports both access ports and trunk 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 Configuring IEEE 802.1X Port-Based Authentication

The following tasks must be completed before implementing the IEEE 802.1X Port-Based Authentication feature:

- IEEE 802.1X must be enabled on the device port.
- The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs).
- EAP support must be enabled on the RADIUS server.
- You must configure the IEEE 802.1X supplicant to send an EAP-logoff (Stop) message to the switch when the user logs off. If you do not configure the IEEE 802.1X supplicant, an EAP-logoff message is not sent to the switch and the accompanying accounting Stop message is not sent to the authentication server. See the Microsoft Knowledge Base article at the location http://support.microsoft.com and set the SupplicantMode registry to 3 and the AuthMode registry to 1.
- Authentication, authorization, and accounting (AAA) must be configured on the port for all network-related service requests. The authentication method list must be enabled and specified. A method list describes the sequence and authentication method to be queried to authenticate a user. See the IEEE 802.1X Authenticator feature module for information.
- The port must be successfully authenticated.

The IEEE 802.1X Port-Based Authentication feature is available only on Cisco 89x and 88x series integrated switching routers (ISRs) that support switch ports.

Note Optimal performance is obtained with a connection that has a maximum of eight hosts per port.

The following Cisco ISR-G2 routers are supported:

- 1900
- 2900
- 3900
- 3900e

The following cards or modules support switch ports:

- Enhanced High-speed WAN interface cards (EHWICs) with ACL support:
  - EHWIC-4ESG-P
  - EHWIC-9ESG-P
  - EHWIC-4ESG
  - EHWIC-9ESG

- High-speed WAN interface cards (HWICs) without ACL support:
  - HWIC-4ESW-P
  - HWIC-9ESW-P
  - HWIC-4ESW
  - HWIC-9ES

Note Not all Cisco ISR routers support all the components listed. For information about module compatibility with a specific router platform, see Cisco EtherSwitch Modules Comparison.

To determine whether your router has switch ports that can be configured with the IEEE 802.1X Port-Based Authentication feature, use the **show interfaces switchport** command.

Restrictions for IEEE 802.1X Port-Based Authentication

IEEE 802.1X Port-Based Authentication Configuration Restrictions

- The IEEE 802.1X Port-Based Authentication feature is available only on a switch port.
- If the VLAN to which an IEEE 802.1X port is assigned is shut down, disabled, or removed, the port becomes unauthorized. For example, the port is unauthorized after the access VLAN to which a port is assigned shuts down or is removed.
- When IEEE 802.1X authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- Changes to a VLAN to which an IEEE 802.1X-enabled port is assigned are transparent and do not affect the switch port. For example, a change occurs if a port is assigned to a RADIUS server-assigned VLAN and is then assigned to a different VLAN after reauthentication.
- When IEEE 802.1X authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- This feature does not support standard ACLs on the switch port.
- The IEEE 802.1X protocol is supported only on Layer 2 static-access ports, Layer 2 static-trunk ports, voice VLAN-enabled ports, and Layer 3 routed ports.

Note Ethernet interfaces can be configured either as access ports or as trunk ports with the following specifications:

- An access port can have only one VLAN configured on the interface; it can carry traffic for only one VLAN.
- A trunk port can have two or more VLANs configured on the interface; it can carry traffic for several VLANs simultaneously.

- The IEEE 802.1X protocol is not supported on the following port types:
  - Dynamic-access ports—If you try to enable IEEE 802.1X authentication on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1X authentication is not enabled. If you try to change an IEEE 802.1X-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
  - Dynamic ports—If you try to enable IEEE 802.1X authentication on a dynamic port, an error message appears, and IEEE 802.1X authentication is not enabled. If you try to change the mode of an IEEE 802.1X-enabled port to dynamic, an error message appears, and the port mode is not changed.
  - Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable IEEE 802.1X authentication on a port that is a SPAN or RSPAN destination port. However, IEEE 802.1X authentication is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable IEEE 802.1X authentication on a SPAN or RSPAN source port.

Note A port in dynamic mode can negotiate with its neighbor to become a trunk 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) fails 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* fails if the access VLAN and voice VLAN have been configured with the same VLAN ID.
- By default, authentication system messages, MAC authentication by-pass system messages and 802.1x system messages are not displayed. If you need to see these system messages, turn on the logging manually, using the following commands:
  - **authentication logging verbose**
  - **dot1x logging verbose**
  - **mab logging verbose**

Upgrading from a Previous Software Release

In Cisco IOS Release 12.4(11)T, the implementation for IEEE 802.1X authentication changed from the previous releases. When IEEE 802.1X authentication is enabled, information about Port Fast is no longer added to the configuration.

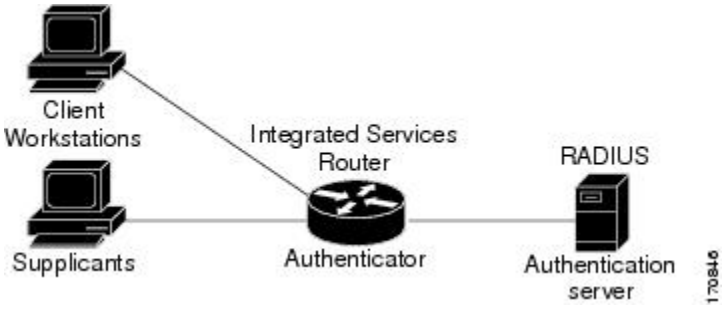
Note To ensure that information about any IEEE 802.1x-related commands that is entered on a port is automaticallly added to the running configuration to address any backward compatibility issues, use the **dot1x pae authenticator** command.

Information About IEEE 802.1X Port-Based Authentication

IEEE 802.1X Device Roles

With IEEE 802.1X authentication, the devices in the network have specific roles as shown in the figure below.

Figure 1: IEEE 802.1X Device Roles



- Supplicant—Device (workstation) that requests access to the LAN and switch services and responds to requests from the router. The workstation must be running IEEE 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The *supplicant* is sometimes called the client.)

  Note To resolve Windows XP network connectivity and IEEE 802.1X authentication issues, read the Microsoft Knowledge Base article at this URL: http://support.microsoft.com/kb/q303597/.

- Authentication server—Device that performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the router whether or not the supplicant is authorized to access the LAN and switch services. The Network Access Device (or ISR router in this instance) transparently passes the authentication messages between the supplicant and the authentication server, and the authentication process is carried out between the supplicant and the authentication server.

The particular EAP method used will be decided between the supplicant and the authentication server (RADIUS server). The RADIUS security system with EAP extensions is available in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client and server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- Authenticator (integrated services router (ISR) or wireless access point)—Router that controls the physical access to the network based on the authentication status of the supplicant. The router acts as an intermediary between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant. The router includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the authenticator receives EAPOL frames and relays them to the authentication server, the EAPOL is stripped and the remaining EAP frame is reencapsulated in the RADIUS format. The EAP frames are not modified during encapsulation, and the authentication server must support EAP within the native frame format. When the authenticator receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

IEEE 802.1X Authentication Initiation and Message Exchange

During IEEE 802.1X authentication, the router or the supplicant can initiate authentication. If you enable authentication on a port by using the **authentication port-control auto** interface configuration command, the router initiates authentication when the link state changes from down to up or periodically if the port remains up and unauthenticated. The router sends an EAP-request/identity frame to the supplicant to request its identity. Upon receipt of the frame, the supplicant responds with an EAP-response/identity frame.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1xport-control** command.

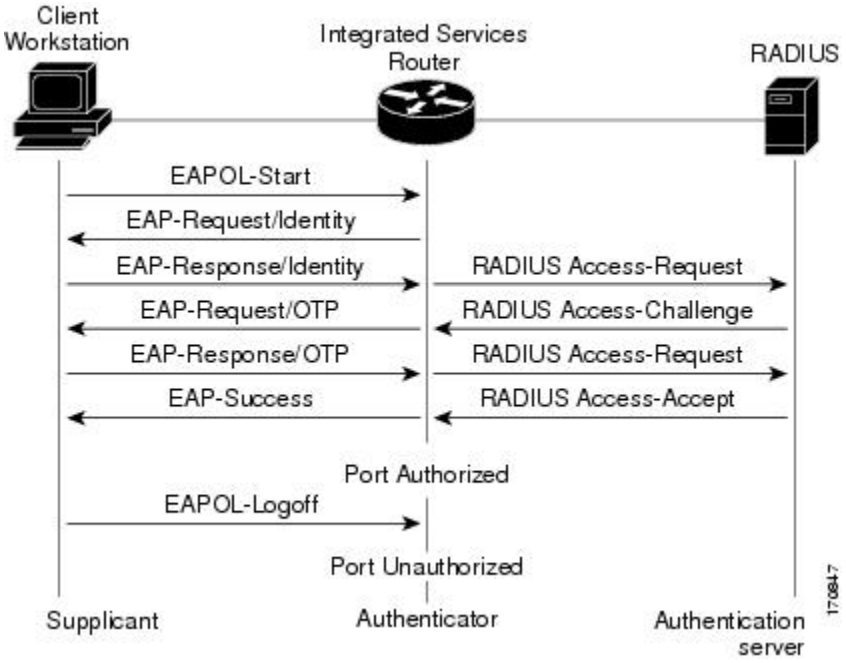
However, if during bootup the supplicant does not receive an EAP-request/identity frame from the router, the supplicant can initiate authentication by sending an EAPOL-start frame, which prompts the router to request the supplicant's identity.

Note If IEEE 802.1X authentication is not enabled or supported on the network access device, any EAPOL frames from the supplicant are dropped. If the supplicant does not receive an EAP-request/identity frame after three attempts to start authentication, the supplicant sends frames as if the port is in the authorized state. A port in the authorized state effectively means that the supplicant has been successfully authenticated. For more information, see the *Ports in Authorized and Unauthorized States* module.

When the supplicant supplies its identity, the router begins its role as the intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If the authentication succeeds, the router port becomes authorized. If the authentication fails, authentication can be retried, the port might be assigned to a VLAN that provides limited services, or network access is not granted. For more information, see the *Ports in Authorized and Unauthorized States* module.

The specific exchange of EAP frames depends on the authentication method being used. The figure below shows a message exchange initiated by the supplicant using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 2: Message Exchange



IEEE 802.1X Authentication Process

To configure IEEE 802.1X port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

The AAA process begins with authentication. When IEEE 802.1X port-based authentication is enabled and the device attempting to authenticate is IEEE 802.1x-capable (meaning it supports the supplicant functionality), this event occurs:

- If the supplicant identity is valid and the IEEE 802.1X authentication succeeds, the router grants the supplicant access to the network.

The router reauthenticates a supplicant when this situation occurs:

- Periodic reauthentication is enabled, and the reauthentication timer expires.

You can configure the reauthentication timer to use a router-specific value or to be based on values from the RADIUS server.

After IEEE 802.1X authentication using a RADIUS server is configured, the router uses timers based on the Session-Timeout RADIUS attribute (Attribute [27]) and the Termination-Action RADIUS attribute (Attribute [29]).

The Session-Timeout RADIUS attribute (Attribute [27]) specifies the time after which reauthentication occurs.

The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during reauthentication. The actions can be Initialize or ReAuthenticate. When the Initialize action is set (the attribute value is DEFAULT), the IEEE 802.1x session ends, and connectivity is lost during reauthentication. When the ReAuthenticate action is set (the attribute value is RADIUS-Request), the session is not affected during reauthentication.

You manually reauthenticate the supplicant by entering the **dot1x re-authenticate interface** *interface-name interface-number* privileged EXEC command.

IEEE 802.1X Host Mode

You can configure an IEEE 802.1X port for single-host or for multihost mode. In single-host mode (see the figure IEEE 802.1X Device Roles in the Device Roles section of this module), only one supplicant can be authenticated by the IEEE 802.1X-enabled switch port. The router detects the supplicant by sending an EAPOL frame when the port link state changes to the up state. If a supplicant leaves or is replaced with another supplicant, the router changes the port link state to down, and the port returns to the unauthorized state.

In multihost mode, you can attach multiple hosts to a single IEEE 802.1X-enabled port. In this mode, only one of the attached supplicants must be authorized for all supplicants to be granted network access. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the router denies network access to all of the attached supplicants.

Note Cisco 870 series platforms do not support single-host mode.

IEEE 802.1X Port Authorization States

During IEEE 802.1X authentication, depending on the port state, the router can grant a supplicant access to the network. The port starts in the *unauthorized* state. While in this state, the port that is not configured as a voice VLAN port disallows all ingress traffic except for IEEE 802.1X authentication, Cisco Discovery Protocol (CDP), and STP packets. When a supplicant is successfully authenticated, the port changes to the *authorized* state, allowing all traffic for the supplicant to flow normally. If the port is configured as a voice VLAN port, the port allows VoIP traffic and IEEE 802.1X protocol packets before the supplicant is successfully authenticated.

If a client that does not support IEEE 802.1X authentication connects to an unauthorized IEEE 802.1X port, then the router requests the client's identity. In this situation, if the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an IEEE 802.1X-enabled supplicant connects to a port that is not running the IEEE 802.1X standard, the supplicant initiates the authentication process by sending the EAPOL-start frame. When no response is received, the supplicant sends the request for a fixed number of times. Because no response is received, the supplicant begins sending frames as if the port is in the authorized state.

If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the router can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a supplicant logs off, it sends an EAPOL-logoff message, causing the router port to change to the unauthorized state.

If the link state of a port changes from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

IEEE 802.1X—Conditional Logging

Use the IEEE 802.1X—Conditional Logging feature for troubleshooting. When the Conditional Logging feature is enabled, the router generates debugging messages for packets entering or leaving the router on a specified interface; the router will not generate debugging output for packets entering or leaving through a different interface. You can specify the interfaces explicitly. For example, you may want to see only debugging messages for one interface or subinterface. You can also turn on debugging for all interfaces that meet the configured condition. This feature is useful on dial access servers, which have a large number of ports.

Normally, the router will generate debugging messages for every interface, resulting in a large number of messages. The large number of messages consumes system resources, and can affect your ability to find the specific information you need. By limiting the number of debugging messages, you can receive messages related to only the ports you want to troubleshoot.

For more information on conditional logging and enabling conditionally triggered debugging, see the "Enabling Conditionally Triggered Debugging" section of the "Troubleshooting and Fault Management" chapter in the *Basic System Management Configuration Guide*.

IEEE 802.1X MIB Support

Cisco IOS Release 12.4(11)T provides support for the following MIBs that provide SNMP access to IEEE 802.1X feature components:

- IEEE8021-PAE-MIB
- Cisco-PAE-MIB

The IEEE8021-PAE-MIB supports reporting of the following information:

- The state of the IEEE 802.1X state machine on a particular port
- Statistics associated with the state of the IEEE 802.1X state machine

The Cisco-PAE-MIB provides SNMP support for the logging and reporting of events, including:

- Port mode
- Guest VLAN number (details the Guest VLAN number configured on a port)
- InGuestVLAN (indicates whether a port is in the Guest VLAN)

How to Configure IEEE 802.1X Port-Based Authentication

Enabling IEEE 802.1X Authentication and Authorization

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*]
5. **dot1x system-auth-control**
6. **identity profile default**
7. **interface** *type slot/port*
8. **access-session port-control** {**auto** | **force-authorized** | **force-unauthorized**}
9. **dot1x pae** [**supplicant** | **authenticator** | **both**]
10. **end**
11. **show dot1x**

DETAILED STEPS

	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	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*] **Example:** `Device(config)# aaa authentication dot1x default group radius`	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.

	Command or Action	Purpose
Step 5	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 6	**identity profile default** **Example:** `Device(config)# identity profile default`	Creates an identity profile and enters dot1x profile configuration mode.
Step 7	**interface** *type slot/port* **Example:** `Device(config-identity-prof)# interface Gigabitethernet 1/0/1`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 8	**access-session port-control** {**auto** | **force-authorized** | **force-unauthorized**} **Example:** `Device(config-if)# access-session port-control auto`	Enables 802.1X port-based authentication on the interface. • **auto—**Enables IEEE 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The Device requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the Device by using the supplicant MAC address. • **force-authorized-—**Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting. • **force-unauthorized—**Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The Device cannot provide authentication services to the supplicant through the port. **Note** Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1xport-control** command.
Step 9	**dot1x pae** [**supplicant** | **authenticator** | **both**] **Example:** `Device(config-if)# dot1x pae authenticator`	Sets the Port Access Entity (PAE) type. • **supplicant—**The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator. • **authenticator-—**The interface acts only as an authenticator and does not respond to any messages meant for a supplicant.

	Command or Action	Purpose
		• **both—**The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages.
Step 10	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 11	**show dot1x** **Example:** `Device# show dot1x`	Displays whether 802.1X authentication has been configured on the device.

Configuring the IEEE 802.1X Host Mode

Note This section describes IEEE 802.1X security features available only on the switch ports.

SUMMARY STEPS

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

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	**radius-server vsa send authentication** **Example:** `Device(config)# radius-server vsa send authentication`	Configures the Network Access Server (NAS) to recognize and use vendor-specific attributes.
Step 4	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 1/2/1`	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**} [**open**] **Example:** `Device(config-if)# access-session host-mode single-host Gigabitethernet 1/2/1`	Allows a single host (client) or multiple hosts on the 802.1X-authorized port. • The **multi-auth** keyword specifies multiple authentications to occur on the 802.1X-authorized port. • The **multi-domain** keyword specifies multi-domain authentication (MDA), which is used to enable authentication of both a host and a voice device, such as an IP phone (Cisco or non-Cisco) on the same switch port. • The **multi-host** keyword specifies multiple hosts on the 802.1X-authorized port. • The **single-host** keyword specifies a single client on the 802.1X-authorized port. • (Optional) The **open** keyword specifies that the port is open; that is, there are no access restrictions.
Step 6	**switchport voice vlan** *vlan-id* **Example:** `Device(config-if)# switchport voice vlan 2`	(Optional) Configures the voice VLAN.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 8	**show authentication interface** *type number* **Example:** `Device# show authentication interface`	Displays your entries.

	Command or Action	Purpose
Step 9	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Enabling IEEE 802.1X SNMP Notifications on Switch Ports

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps dot1x** *notification-type*

DETAILED STEPS

	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	**snmp-server enable traps dot1x** *notification-type* **Example:** `Device(config)# snmp-server enable traps dot1x no-guest-vlan`	Enables SNMP logging and reporting when no Guest VLAN is configured or available.

Configuration Examples for IEEE 802.1x Port-Based Authentication

Example: Enabling IEEE 802.1X and AAA on a Port

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1xport-control** command.

Note Whenever you configure any IEEE 802.1X parameter on a port, a dot1x authenticator is automatically created on the port. As a result, the **dot1x pae authenticator** command appears in the configuration to ensure that IEEE 802.1X authentication still works without manual intervention on legacy configurations. The appearance of the IEEE 802.1X information in the configuration is likely to change in future releases.

The following example shows how to enable IEEE 802.1X and AAA on Fast Ethernet port 2/1 and how to verify the configuration:

Note In this example the Ethernet interface is configured as an access port by using the **switchport mode access** command in interface configuration mode. The Ethernet interface can also be configured as a trunk port using the **switchport mode trunk** command in interface configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# dot1x system-auth-control
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# interface fastethernet2/1
Device(config-if)# switchport mode access
Device(config-if)# authentication port-control auto
Device(config-if)# dot1x pae authenticator
Device(config-if)# end

Device# show dot1x interface fastethernet7/1 details

Dot1x Info for FastEthernet7/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Dot1x Authenticator Client List
-------------------------------
```

```
Supplicant                = 1000.0000.2e00
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED

Authentication Method     = Dot1x
Authorized By             = Authentication Server
Vlan Policy               = N/A
```

Example: Configuring the IEEE 802.1X Host Mode

The following example shows how to enable 802.1X authentication and to allow multiple hosts:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication port-control auto
Device(config-if)# authentication host-mode multihost
Device(config-if)# end
```

Example: Displaying IEEE 802.1X Statistics and Status

- To display IEEE 802.1X statistics for all ports, use the **show dot1x all statistics** command in privileged EXEC configuration mode.
- To display IEEE 802.1X statistics for a specific port, use the **show dot1x status interface** *type number* command in privileged EXEC configuration mode.
- To display the IEEE 802.1X administrative and operational status for the switch, use the **show dot1x all** [**details** | **statistics** | **summary**] command in privileged EXEC configuration mode.
- To display the IEEE 802.1X administrative and operational status for a specific port, use the **show dot1x interface** *type number* command in privileged EXEC configuration mode. For detailed information about the fields in these displays, see the command reference for this release.

The following example displays **show dot1x all** command output:

```
Device# show dot1x all

Sysauthcontrol                  Enabled
Dot1x Protocol Version     2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Device-871#
```

The following example displays **show dot1x summary** command output:

```
Device# show dot1x all summary

Interface             PAE             Client                          Status
-------------------------------------------------------------------------------
Fa1                   AUTH             000d.bcef.bfdc           AUTHORIZED
```

AdditionalReferencesforIEEE802.1XPort-BasedAuthentication

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

Standards and RFCs

Standard/RFC	Title
IEEE 802.1X	*Port Based Network Access Control*
RFC 3580	*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*

MIBs

MIB	MIBs Link
• 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 Port-Based 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 Port-Based Authentication

Feature Name	Releases	Feature Information
CDP Enhancement —Host Presence TLV	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS 15.2(1)E	

Feature Name	Releases	Feature Information
		This features allows you to ensure that only one client can be connected to the 802.1X-enabled port. The switch detects the client by sending an EAPOL frame when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state. 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 was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E

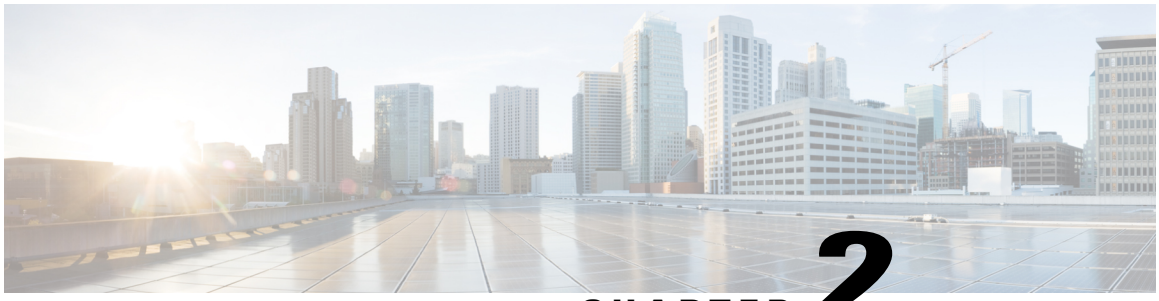
Feature Name	Releases	Feature Information
		• Catalyst 4500E Supervisor Engine 6L-E

Feature Name	Releases	Feature Information
IEEE 802.1X Authenticator	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS 15.2(1)E	This feature was introduced to prevent unauthorized devices (supplicants) from gaining access to the network. 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 was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E • Catalyst 4500E Supervisor Engine 6L-E The following commands were introduced or modified: **aaa accounting**, **dot1x guest-vlan**, **snmp-server enable traps**.

Feature Name	Releases	Feature Information
IEEE 802.1X-Conditional Logging	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS 15.2(1)E	The IEEE 802.1X-Conditional Logging feature is used for troubleshooting interfaces. 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 was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E • Catalyst 4500E Supervisor Engine 6L-E

Feature Name	Releases	Feature Information
IEEE 802.1X MIB Support	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS 15.2(1)E	This feature provides support for the following MIBs: • Cisco-PAE-MIB • IEEE8021-PAE-MIB 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 was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E • Catalyst 4500E Supervisor Engine 6L-E

Feature Name	Releases	Feature Information
IEEE 802.1X Support for Trunk Ports	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS 15.2(1)E	The IEEE 802.1X Support for Trunk Ports feature is used to configure Ethernet interfaces as trunk ports. 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 was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E • Catalyst 4500E Supervisor Engine 6L-E



CHAPTER 2

Network Edge Authentication Topology

The Network Edge Access Topology (NEAT) feature enables extended secure access in areas outside the wiring closet (such as conference rooms). This secure access allows any type of device to authenticate on the port.

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 Network Edge Authentication Topology

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.

The switch must be connected to a Cisco secure ACS and RADIUS authentication, authorization, and accounting (AAA) must be configured for Web authentication. If appropriate, you must enable 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.

Note 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.

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*.

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

Restrictions for Network Edge Authentication Topology

- NEAT is not supported on an EtherChannel port.
- It is recommended that NEAT is only deployed with auto-configuration.
- This feature does not support standard ACLs on the switch port.

Information About Network Edge Authentication Topology

Authenticator and Supplicant Switch with Network Edge Authentication Topology

The NEAT feature enables extended secure access in areas outside the wiring closet (such as conference rooms). NEAT allows you to configure a switch to act as a supplicant to another switch. Thus, with NEAT enabled, the desktop switch can become a supplicant switch and authenticate itself to the access switch.

- 802.1X supplicant switch: You can configure a switch to act as a supplicant to another switch by using the 802.1X supplicant feature. This configuration is helpful in a scenario where, for example, a switch is outside a wiring closet and is connected to an upstream switch through a trunk port. A switch configured with the 802.1X switch supplicant feature authenticates with the upstream switch for secure connectivity. Once the supplicant switch authenticates successfully the port mode changes from access to trunk.

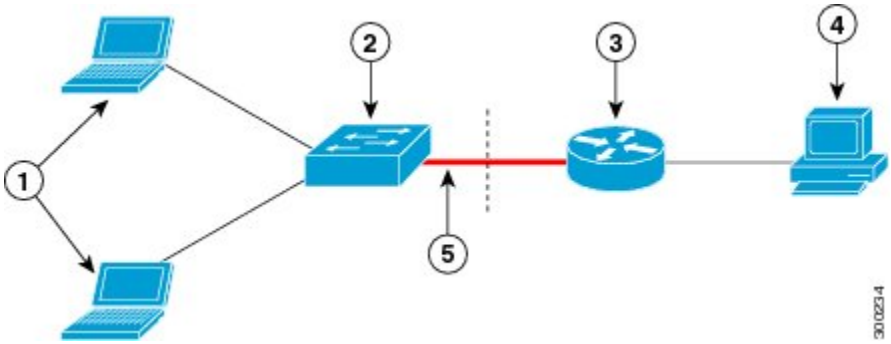
- If the access VLAN is configured on the authenticator, it becomes the native VLAN for the trunk port after successful authentication.

You can enable multidomain authentication (MDA) or multiple-authentication mode on the authenticator interface that connects to one or more supplicant switches. Multihost mode is not supported on the authenticator interface. Additional information about the authenticator can be found in the "IEEE 802.1X Authenticator" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

Use the **dot1x supplicant force-multicast** global configuration command on the supplicant switch for NEAT to work in all host modes.

- Host Authorization: Ensures that only traffic from authorized hosts (connecting to the switch with supplicant) is allowed on the network. The switches use Client Information Signalling Protocol (CISP) to send the MAC addresses connecting to the supplicant switch to the authenticator, as shown in the figure below.
- Auto enablement: Automatically enables trunk configuration on the authenticator switch, allowing user traffic from multiple VLANs coming from supplicant switches. Configure the Cisco Attribute-Value (AV) pair as device-traffic-class=switch at the ACS. (You can configure this under the group or the user settings.)

Figure 3: Authenticator and Supplicant Switch Using CISP



1	Workstations (clients)	2	Supplicant switch (outside wiring closet)
3	ISR G2 as an Authenticator	4	Access control server (ACS)
5	Trunk port		

Guidelines for Configuring Network Edge Access Topology

- You can configure NEAT ports with the same configurations as the other authentication ports. When the supplicant switch authenticates, the port mode is changed from access-based to trunk-based on the switch vendor-specific attributes (VSAs) (device-traffic-class=switch).
- The VSA changes the authenticator switch port mode from access to trunk and enables 802.1X trunk encapsulation and the access VLAN (if any) would be converted to a native trunk VLAN. VSA does not change any of the port configurations on the supplicant.

- To change the host mode and apply a standard port configuration on the authenticator switch port, you can also use Auto Smartports user-defined macros, instead of the switch VSA. This allows you to remove unsupported configurations on the authenticator switch port and to change the port mode from access to trunk. For information, see the *AutoSmartports Configuration Guide*.

Note NEAT does not support redundant links between authenticator and supplicant switches.

How to Configure Network Edge Authentication Topology

Configuring an Authenticator with Network Edge Authentication Topology

SUMMARY STEPS

1. **configure terminal**
2. **cisp enable**
3. **interface** *type slot/port*
4. **switchport mode access**
5. **authentication port-control auto**
6. **dot1x pae authenticator**
7. **end**
8. **show authentication interface** *interface-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**cisp enable** **Example:** `Switch(config)# cisp enable`	Enables CISP.
Step 3	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets the port mode to access.
Step 5	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Sets the port-authentication mode to auto.
Step 6	**dot1x pae authenticator** **Example:** `Switch(config-if)# dot1x pae authenticator`	Configures the interface as a port access entity (PAE) authenticator.
Step 7	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	**show authentication interface** *interface-id* **Example:** `Switch# show authentication interface gigabitethernet0/1`	Verifies your entries.

Configuring a Supplicant Switch with Network Edge Authentication Topology

SUMMARY STEPS

1. **configure terminal**
2. **cisp enable**
3. **dot1x credentials** *profile*
4. **username** *name*
5. **password** *password*
6. **exit**
7. **dot1x supplicant force-multicast**
8. **interface** *type slot/port*
9. **switchport trunk encapsulation dot1q**
10. **switchport mode trunk**
11. **dot1x pae supplicant**
12. **dot1x credentials** *profile-name*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**cisp enable** **Example:** `Switch(config)# cisp enable`	Enables CISP.
Step 3	**dot1x credentials** *profile* **Example:** `Switch(config)# dot1x credentials test`	Creates a 802.1X credential profile. This must be attached to the port that is configured as supplicant.
Step 4	**username** *name* **Example:** `Switch(config-dot1x-creden)# username suppswitch`	Creates a username.

	Command or Action	Purpose
Step 5	**password** *password* **Example:** `Switch(config-dot1x-creden)# password secret`	Creates a password for the new username.
Step 6	**exit** **Example:** `Switch(config-dot1x-creden)# exit`	Returns to global configuration mode.
Step 7	**dot1x supplicant force-multicast** **Example:** `Switch(config)# dot1x supplicant force-multicast`	Forces the switch to send only multicast EAPOL packets when it receives either unicast or multicast packets, which allows NEAT to work on the supplicant switch in all host modes.
Step 8	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode.
Step 9	**switchport trunk encapsulation dot1q** **Example:** `Switch(config-if)# switchport trunk encapsulation dot1q`	Sets the port to trunk mode.
Step 10	**switchport mode trunk** **Example:** `Switch(config-if)# switchport mode trunk`	Configures the interface as a VLAN trunk port.
Step 11	**dot1x pae supplicant** **Example:** `Switch(config-if)# dot1x pae supplicant`	Configures the interface as a port access entity (PAE) supplicant.
Step 12	**dot1x credentials** *profile-name* **Example:** `Switch(config-if)# dot1x credentials test`	Attaches the 802.1X credentials profile to the interface.

	Command or Action	Purpose
Step 13	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for Network Edge Authentication Topology

Example: Configuring an Authenticator with NEAT

The following example shows how to configure a switch as an 802.1X authenticator:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
```

Example: Configuring a Supplicant Switch with NEAT

This example shows how to configure a switch as a supplicant:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
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*

Standards and RFCs

Standard/RFC	Title
IEEE 802.1X	*Port Based Network Access Control*

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

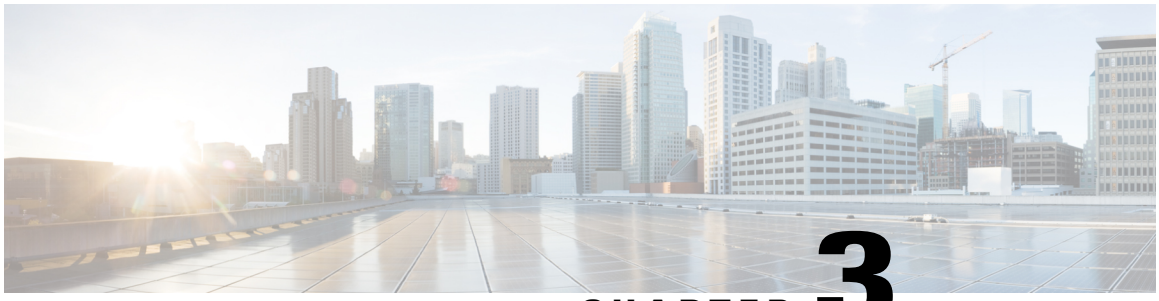
Feature Information for Network Edge Authentication Topology

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 2: Feature Information for NEAT

Feature Name	Releases	Feature Information
NEAT (Network Edge Authentication Topology)	Cisco IOS 15.2(1)E	The NEAT feature enables extended secure access in areas outside the wiring closet (such as conference rooms). This secure access allows any type of device to authenticate on the port.



CHAPTER 3

VLAN RADIUS Attributes in Access Requests

The VLAN RADIUS Attributes in Access Requests feature enhances the security for access switches with the use of VLAN RADIUS attributes (VLAN name and ID) in the access requests and with an extended VLAN name length of 128 characters.

This module describes how to create an attribute filter-list and how to bind an attribute filter-list with authentication and accounting requests.

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.

Restrictions for VLAN RADIUS Attributes in Access Requests

- Dynamic VLAN assignment to critical authentication (inaccessible authentication bypass or AAA fail policy) VLAN is not supported.

- If the RADIUS server becomes unavailable during an 802.1x authentication exchange, the current exchange times out, and the switch uses critical access control lists (ACLs) during the next authentication attempt.
- In a scenario when the VLAN RADIUS Attributes in Access Requests feature is enabled on a Catalyst 4000 series switch, reloading the switch with an image that does not support the feature may lead to a crash. To recover the switch, erase the vlan.dat file by issuing the `erase cat4000_flash:` command. Once the vlan.dat file is erased, reboot the switch with the intended image.

Information About VLAN RADIUS Attributes in Access Requests

VLAN RADIUS attributes

Authentication prevents unauthorized devices (clients) from gaining access to the network by using different methods to define how users are authorized and authenticated for network access. To enhance security, you can limit network access for certain users by using VLAN assignment. Information available in the access-request packets sent to the authentication server (AAA or RADIUS server) validates the identity of the user and defines if a user can be allowed to access the network.

The VLAN RADIUS Attributes in Access Requests feature supports authentication using IEEE 802.1X, MAC authentication bypass (MAB), and web-based authentication (webauth). The default order for authentication methods is 802.1X, and then MAB, then web-based authentication. If required, you can change the order or disable any of these methods.

- If MAC authentication bypass is enabled, the network device relays the client's MAC address to the AAA server for authorization. If the client's MAC address is valid, the authorization succeeds and the network device grants the client access to the network.
- If web-based authentication is enabled, the network device sends an HTTP login page to the client. The network device relays the client's username and password to the AAA server for authorization. If the login succeeds, the network device grants the client access to the network.

While performing authentications, the VLAN RADIUS attributes (name and ID of the VLAN) assigned to the hosting port is included in the RADIUS access requests and accounting requests. The VLAN RADIUS Attributes in Access Requests feature supports VLAN names accommodating 128-character strings.

With the use of VLAN RADIUS attributes in authentication requests, clients are authorized based on existing VLAN segmented networks. The existing VLAN provisioning is used as an indication of the location.

Based on RFC 2868 (RADIUS Attributes for Tunnel Protocol Support), support is provided for standard RADIUS attributes that exist for specifying the tunnel-type, medium and identifier.

- Tunnel-Type (IEFT #64) = VLAN
- Tunnel-Medium-Type (IEFT #65) = 802 (6)
- Tunnel-Private-Group-ID (IEFT #81) = [tag, string]

Note The Tunnel-Private-Group-ID includes the VLAN ID or name and accommodates a string length of up to 253 characters.

How to Configure VLAN RADIUS Attributes in Access Requests

Configuring VLAN RADIUS Attributes in Access Requests

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-session attributes filter-list list** *list-name*
4. **vlan-id**
5. **exit**
6. **access-session accounting attributes filter-spec include list** *list-name*
7. **access-session authentication attributes filter-spec include list** *list-name*
8. **end**

DETAILED STEPS

	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	**access-session attributes filter-list list** *list-name* **Example:** `Device(config)# access-session attributes filter-list list mylist`	Adds access-session protocol data to accounting and authentication records and enters common filter list configuration mode. The **filter-list** keyword configures a sensor protocol filter list to accounting and authentication records.
Step 4	**vlan-id** **Example:** `Device(config-com-filter-list)# vlan-id`	Includes the VLAN ID for the attribute.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-com-filter-list)# exit`	Exits common filter list configuration mode and returns to global configuration mode.
Step 6	**access-session accounting attributes filter-spec include list** *list-name* **Example:** `Device(config)# access-session accounting attributes filter-spec include list mylist`	Configures a sensor protocol filter specification, and binds an attribute filter list with accounting records.
Step 7	**access-session authentication attributes filter-spec include list** *list-name* **Example:** `Device(config)# access-session authentication attributes filter-spec include list mylist`	Configures a sensor protocol filter specification, and binds an attribute filter list with authentication records.
Step 8	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying VLAN RADIUS Attributes in Access Requests

SUMMARY STEPS

1. **enable**
2. **debug radius**
3. **show authentication sessions interface**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **debug radius**

Displays the RADIUS attributes.

Example:

```
Device# debug radius

19:01:33: RADIUS:  Tunnel-Private-Group[81]  5   01:"20"
19:01:33: RADIUS:  Tunnel-Type         [64]  6   01:VLAN     [13]
19:01:33: RADIUS:  Tunnel-Medium-Type  [65]  6   01:ALL_802  [6]
19:01:33: RADIUS:  Tunnel-Private-Group[81]  131
02:"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
19:01:33: RADIUS:  Tunnel-Type         [64]  6   02:VLAN     [13]
19:01:33: RADIUS:  Tunnel-Medium-Type  [65]  6   02:ALL_802  [6]
19:01:33: RADIUS:  NAS-IP-Address      [4]   6   192.168.1.6
```

Step 3 **show authentication sessions interface**

Displays the detailed authentication session output for a specific interface.

Example:

```
Device# show authentication sessions interface GigabitEthernet3/0/2 details

            Interface:  GigabitEthernet3/0/2
          MAC Address:  xxxx.xxxx.xxxx
         IPv6 Address:  Unknown
         IPv4 Address:  192.0.2.1
            User-Name:  cisco1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  CXXXXXX0000XXXXXXX
      Acct Session ID:  Unknown
               Handle:  0xDX0XXXX
       Current Policy:  POLICY_Gi3/0/2

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecure

Server Policies:
            SGT Value:  5


Method status list:
       Method           State
       dot1x            Authc Success

----------------------------------------
            Interface:  GigabitEthernet3/0/2
          MAC Address:  yyyy.yyyy.yyyy
         IPv6 Address:  Unknown
         IPv4 Address:  203.0.113.1
            User-Name:  cisco2
```

```
               Status:  Authorized
               Domain:  VOICE
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  CXXXXXX000
     Acct Session ID:  Unknown
               Handle:  0xDX0XXXX
      Current Policy:  POLICY_Gi3/0/2

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure

     Security Status:  Link Unsecure

Server Policies:
          Vlan Group:  Vlan: 11
           SGT Value:  5

Method status list:
       Method           State
       dot1x            Authc Success
```

Configuration Examples for VLAN RADIUS Attributes in Access Requests

Example: Configuring VLAN RADIUS Attributes in Access Requests

```
Device> enable
Device# configure terminal
Device(config)# access-session attributes filter-list list test-vlan-extension
Device(config-com-filter-list)# vlan-id
Device(config-com-filter-list)# exit
Device(config)# access-session accounting attributes filter-spec include list mylist
Device(config)# access-session authentication attributes filter-spec include list mylist
Device(config)# end
```

Additional References for VLAN RADIUS Attributes in Access Requests

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
802.1x Authentication with VLAN Assignment	"Configuring IEEE 802.1x Port-Based Authentication" chapter in *Catalyst 3750-X and 3560-X Switch Software Configuration Guide*
Configuring IEEE 802.1X authentication for access ports	"IEEE 802.1X VLAN Assignment" chapter in *802.1X Authentication Services Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*
RFC 2869	*RADIUS Extensions*
RFC 4675	*RADIUS Attributes for Virtual LAN and Priority Support*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for VLAN RADIUS Attributes in Access Requests

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 3: Feature Information for VLAN RADIUS Attributes in Access Requests

Feature Name	Releases	Feature Information
VLAN RADIUS Attributes in Access Requests	Cisco IOS 15.2(3)E	The VLAN RADIUS Attributes in Access Requests feature enhances the security for access switches with the use of VLAN RADIUS attributes (VLAN name and ID) in the access requests and with an extended VLAN name length of 128 characters. The following commands were introduced or modified: **access-session attributes filter-list** *list*, **access-session accounting attributes filter-spec include** *list*, and **access-session authentication attributes filter-spec include** *list*.