IEEE 802.1X VLAN Assignment

The IEEE 802.1X VLAN Assignment feature is automatically enabled when IEEE 802.1X authentication is configured for an access port, which allows the RADIUS server to send a VLAN assignment to the device port. This assignment configures the device port so that network access can be limited for certain users.

- Prerequisites for IEEE 802.1X VLAN Assignment, on page 1
- Restrictions for IEEE 802.1X VLAN Assignment, on page 2
- Information About IEEE 802.1X VLAN Assignment, on page 3
- How to Configure IEEE 802.1X VLAN Assignment, on page 3
- Configuration Examples for IEEE 802.1X VLAN Assignment, on page 7
- Additional References for IEEE 802.1X Port-Based Authentication, on page 8
- Feature History for IEEE 802.1X VLAN Assignment, on page 8

Prerequisites for IEEE 802.1X VLAN Assignment

The following tasks must be completed before implementing the IEEE 802.1X VLAN Assignment 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 VLAN Assignment feature is available only on Cisco 89x and 88x series integrated switching routers (ISRs) that support switch ports.

The following 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

Restrictions for IEEE 802.1X VLAN Assignment

- The IEEE 802.1X VLAN Assignment feature is available only on a switch port.
- The device port is always assigned to the configured access VLAN when any of the following conditions occurs:
  - No VLAN is supplied by the RADIUS server.
  - The VLAN information from the RADIUS server is not valid.
  - IEEE 802.1X authentication is disabled on the port.
  - The port is in the force authorized, force unauthorized, unauthorized, or shutdown state.

Note An access VLAN is a VLAN assigned to an access port. All packets sent from or received on this port belong to this VLAN.

- Assignment to the configured access VLAN prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error. Examples of configuration errors include the following:
  - A nonexistent or malformed VLAN ID
  - Attempted assignment to a voice VLAN ID
- When IEEE 802.1X authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- If the multihost mode is enabled on an IEEE 802.1X port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.
- If an IEEE 802.1X port is authenticated and put in the RADIUS server-assigned VLAN, any change to the port access VLAN configuration does not take effect.
- This feature does not support standard ACLs on the switch port.

Information About IEEE 802.1X VLAN Assignment

Configuring Authorization

The AAA authorization feature is used to determine what a user can and cannot do. When AAA authorization is enabled, the network access server uses information retrieved from the user profile that is located either in the local user database or on the security server, to configure the user’s session. The user is granted access to a requested service only if the information in the user profile allows it.

IEEE 802.1X Authentication with VLAN Assignment

Device ports support IEEE 802.1X authentication with VLAN assignment. After successful IEEE 802.1X authentication of a port, the RADIUS server sends the VLAN assignment to configure the device port.

The RADIUS server database maintains the username-to-VLAN mappings, assigning the VLAN based on the username of the supplicant connected to the device port.

How to Configure IEEE 802.1X VLAN Assignment

Enabling AAA Authorization for VLAN Assignment

AAA authorization limits the services available to a user. When AAA authorization is enabled, the device uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authorization network radius if-authenticated** **Example:** `Device(config)# aaa authorization network radius if-authenticated`	Configures the device for user RADIUS authorization for all network-related service requests. RADIUS authorization succeeds if the user has authenticated.
Step 5	**aaa authorization exec radius if-authenticated** **Example:** `Device(config)# aaa authorization exec radius if-authenticated`	Configures the device for user RADIUS authorization if the user has privileged EXEC access. RADIUS authorization succeeds if the user has authenticated.
Step 6	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling IEEE 802.1X Authentication and Authorization

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**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.
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	**exit** **Example:** `Device(config-identity-prof)# exit`	Exits dot1x profile configuration mode and returns to global configuration mode.
Step 8	**interface** *type slot/port* **Example:** `Device(config)# interface Gigabitethernet 1/0/1`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 9	**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

	Command or Action	Purpose
		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.
Step 10	**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. • **both**—The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages.
Step 11	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 12	**show dot1x** **Example:** `Device# show dot1x`	Displays whether 802.1X authentication has been configured on the device.

Specifying an Authorized VLAN in the RADIUS Server Database

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the device and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not

suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification.

- You must assign the following vendor-specific tunnel attributes in the RADIUS server database. The RADIUS server must return these attributes to the device:
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID

Attribute [64] must contain the value “VLAN” (type 13). Attribute [65] must contain the value “802” (type 6). Attribute [81] specifies the VLAN name or VLAN ID assigned to the IEEE 802.1X-authenticated user.

Configuration Examples for IEEE 802.1X VLAN Assignment

Example: Enabling AAA Authorization for VLAN Assignment

The following example shows how to enable AAA Authorization for VLAN assignment:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization network radius if-authenticated
Device(config)# aaa authorization exec radius if-authenticated
Device(config)# end
```

Example: Enabling 802.1X Authentication

The following example shows how to enable 802.1X authentication on a device:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius group radius
Device(config)# dot1x system-auth-control
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# dot1x port-control auto
```

The following **show dot1x** command output shows that 802.1X authentication has been configured on a device:

```
Device# show dot1x all

Sysauthcontrol              Enabled
Dot1x Protocol Version            2
Dot1x Info for GigabitEthernet 1/0/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
```

```
ReAuthentication          = Enabled
QuietPeriod               = 600
ServerTimeout             = 60
SuppTimeout               = 30
ReAuthPeriod              = 1800 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 3
TxPeriod                  = 60
RateLimitPeriod           = 60
```

Additional References for IEEE 802.1X Port-Based Authentication

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*

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 History for IEEE 802.1X VLAN Assignment

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Gibraltar 16.11.1	IEEE 802.1X VLAN Assignment	The IEEE 802.1X VLAN Assignment feature is automatically enabled when IEEE 802.1X authentication is configured for an access port, which allows the RADIUS server to send a VLAN assignment to the device port. This assignment configures the device port so that network access can be limited for certain users.

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