IEEE 802.1X RADIUS Accounting

The IEEE 802.1X RADIUS Accounting feature is used to relay important events to the RADIUS server (such as the supplicant's connection session). The information in these events is used for security and billing purposes.

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 RADIUS Accounting

The following tasks must be completed before implementing the IEEE 802.1X RADIUS Accounting 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.

- If you plan to implement system-wide accounting, you should also configure IEEE 802.1X accounting. You also need to inform the accounting server of the system reload event when the system is reloaded to ensure that the accounting server is aware that all outstanding IEEE 802.1X sessions on this system are closed.

The RADIUS Accounting 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

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 with RADIUS Accounting

- The IEEE 802.1X with RADIUS Accounting feature is available only on a switch port.

- This feature does not support standard ACLs on the switch port.

Information About IEEE 802.1X with RADIUS Accounting

Relaying of IEEE 802.1X RADIUS Accounting Events

IEEE 802.1X RADIUS accounting relays important events to the RADIUS server (such as the supplicant's connection session). This session is defined as the interval beginning when the supplicant is authorized to use the port and ending when the supplicant stops using the port.

After the supplicant is authenticated, the switch sends accounting-request packets to the RADIUS server, which responds with accounting-response packets to acknowledge the receipt of the request.

A RADIUS accounting-request packet contains one or more Attribute-Value (AV) pairs to report various events and related information to the RADIUS server. The following events are tracked:

- User successfully authenticates.

- User logs off.

- Link-down occurs on an IEEE 802.1X port.

- Reauthentication succeeds.

- Reauthentication fails.

When the port state transitions between authorized and unauthorized, the RADIUS messages are transmitted to the RADIUS server.

The switch does not log any accounting information. Instead, it sends such information to the RADIUS server, which must be configured to log accounting messages.

The following is the IEEE 802.1X RADIUS accounting process:

1 A user connects to a port on the router.

2 Authentication is performed.

3 VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.

4 The router sends a start message to an accounting server.

5 Reauthentication is performed, as necessary.

6 The port sends an interim accounting update to the accounting server that is based on the result of reauthentication.

7 The user disconnects from the port.

8 The router sends a stop message to the accounting server.

The switch port does not log IEEE 802.1X accounting information. Instead, it sends this information to the RADIUS server, which must be configured to log accounting messages.

To configure IEEE 802.1X accounting, you need to perform the following tasks:

Note See the "Enabling 802.1X Accounting" section for more specific configuration information.

- Enable accounting in your RADIUS server.

- Enable IEEE 802.1X accounting on your switch.

- Enable AAA accounting.

Enabling AAA system accounting along with IEEE 802.1X accounting allows system reload events to be sent to the accounting RADIUS server for logging. When the accounting RADIUS server receives notice of a system reload event, the server can infer that all active IEEE 802.1X sessions are appropriately closed.

Because RADIUS uses the unreliable transport protocol UDP, accounting messages may be lost due to poor network conditions. If the switch does not receive the accounting response message from the RADIUS server after a configurable number of retransmissions of an accounting request, the following system message appears:

```
Accounting message %s for session %s failed to receive Accounting Response.
```
When the stop message is not transmitted successfully, a message like the following appears:

```
00:09:55: %RADIUS-3-NOACCOUNTINGRESPONSE: Accounting message Start for session 172.20.50.145
 sam 11/06/03 07:01:16 11000002 failed to receive Accounting Response.
```

Note Use the **debug radius** command or **debug radius accounting** command to enable the %RADIUS-3-NO ACCOUNTING RESPONSE message.

Use the **show radius statistics** command to display the number of RADIUS messages that do not receive the accounting response message.

IEEE 802.1X Accounting Attribute-Value Pairs

The information sent to the RADIUS server is represented in the form of AV pairs. These AV pairs provide data for different applications. (For example, a billing application might require information that is in the Acct-Input-Octets or the Acct-Output-Octets attributes of a RADIUS packet.)

AV pairs are automatically sent by a router that is configured for IEEE 802.1X accounting. Three types of RADIUS accounting packets are sent by a router:

- START—sent when a new user session starts

- INTERIM—sent during an existing session for updates

- STOP—sent when a session terminates

The following table lists the AV pairs and when they are sent by the router.

Note   The Framed-IP-Address AV pair (Attribute 8) is sent only if a valid Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

Note   With CSCtz66183, the Service-Type AV pair (Attribute 6) is not displayed in the Accounting-Request records.

Table 1: Accounting AV Pairs

Attribute Number	AV Pair Name	*START*	*INTERIM*	*STOP*
Attribute [1]	User-Name	Always	Always	Always
Attribute [4]	NAS-IP-Address	Always	Always	Always
Attribute [5]	NAS-Port	Always	Always	Always
Attribute [6]	Service-Type	Always	Always	Always
Attribute [8]	Framed-IP-Address	Never	Sometimes	Sometimes 1
Attribute [25]	Class	Always	Always	Always
Attribute [30]	Called-Station-ID	Always	Always	Always
Attribute [31]	Calling-Station-ID	Always	Always	Always
Attribute [40]	Acct-Status-Type	Always	Always	Always
Attribute [41]	Acct-Delay-Time	Always	Always	Always
Attribute [42]	Acct-Input-Octets	Never	Always	Always
Attribute [43]	Acct-Output-Octets	Never	Always	Always
Attribute [44]	Acct-Session-ID	Always	Always	Always
Attribute [45]	Acct-Authentic	Always	Always	Always
Attribute [46]	Acct-Session-Time	Never	Never	Always
Attribute [47]	Acct-Input-Packets	Never	Always	Always

Attribute Number	AV Pair Name	*START*	*INTERIM*	*STOP*
Attribute [48]	Acct-Output-Packets	Never	Always	Always
Attribute [49]	Acct-Terminate-Cause	Never	Never	Always
Attribute [61]	NAS-Port-Type	Always	Always	Always

You can configure the device to send Cisco vendor-specific attributes (VSAs) to the RADIUS server. The following table lists the available Cisco AV pairs.

Note   Before VSAs can be sent in the accounting records you must configure the **radius-server vsa send accounting** command.

Table 2: Cisco Vendor-Specific Attributes

Attribute Number	AV Pair Name	*START*	*INTERIM*	*STOP*
Attribute [26,9,1]	Cisco-Avpair: connect-progress	Always	Always	Always
Attribute [26,9,2]	cisco-nas-port	Always	Always	Always
Attribute [26,9,1]	Cisco-Avpair: disc-cause	Never	Never	Always

You can display the AV pairs that are being sent by the router by entering the **debug radius accounting** privileged EXEC command. For more information about this command, see the *Cisco IOS Debug Command Reference*. For more information about AV pairs, see Cisco IOS RFC 3580, *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*.

How to Use IEEE 802.1X RADIUS Accounting

Enabling 802.1X RADIUS Accounting

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **acct-port** *port-number*
5. **aaa accounting dot1x default start-stop group radius**
6. **aaa accounting system default start-stop group radius**
7. **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	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA globally.

Step 4	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **acct-port** *port-number*
	
	Example:
	`|`
	`Device(config)# radius-server host 172.20.39.46 auth-port 1812 acct-port 1813 key rad123`
		Specifies a RADIUS server host.
		
		• The **auth-port** keyword and *port-number* argument specifies the User Datagram Protocol (UDP) destination port for authentication requests.
		
		• The **acct-port** keyword and *port-number* argument specifies the UDP destination port for accounting requests.

	Command or Action	Purpose

Step 5	**aaa accounting dot1x default start-stop group radius**
	
	Example:
	`|`
	`Device(config)# aaa accounting dot1x default start-stop group radius`
		Provides information about all IEEE 802.1x-related user events.
		
		• The **start-stop** keyword sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
		
		• The **group radius** is the exact name of the character string used to name the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.

Step 6	**aaa accounting system default start-stop group radius**
	
	Example:
	`|`
	`Device(config)# aaa accounting system default start-stop group radius`
		Performs accounting for all system-level events not associated with users, such as reloads.
		Note When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
		
		• The **start-stop** keyword sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
		
		• The **group radius** is the exact name of the character string used to name the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.

Step 7	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuration Example for IEEE 802.1X RADIUS Accounting

Example: Enabling IEEE 802.1X RADIUS Accounting

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server. The first command configures the RADIUS server, specifying port 1812 as the authorization port, 1813 as the UDP port for accounting, and rad123 as the encryption key:

Note You must configure the RADIUS server to perform accounting tasks.

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius-server host 172.20.39.46 auth-port 1812 acct-port 1813 key rad123
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# aaa accounting system default start-stop group radius
Device(config)# end
Device#
```

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 RADIUS Accounting

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 IEEE 802.1X RADIUS Accounting

Feature Name	Releases	Feature Information
IEEE 802.1X RADIUS Accounting	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	This feature is used to relay important events to the RADIUS server (such as the supplicant's connection session). The information in these events is used for security and billing purposes. 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 Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.