



IEEE 802.1X Common Session ID

The IEEE 802.1X Common Session ID feature allows a single session identifier to be used for all 802.1X and MAB authenticated sessions. This session ID is used for all reporting purposes such as show commands, MIBs, and RADIUS messages and allows users to distinguish messages for one session from messages for other sessions.

- [Finding Feature Information, page 1](#)
- [Prerequisites for IEEE 802.1X Common Session ID, page 1](#)
- [Restrictions for IEEE 802.1X Common Session ID, page 3](#)
- [Information About IEEE 802.1X Common Session ID, page 3](#)
- [Examples for IEEE 802.1X Common Session ID, page 3](#)
- [Additional References for IEEE 802.1X Port-Based Authentication, page 4](#)
- [Feature Information for IEEE 802.1X Common Session ID, page 5](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IEEE 802.1X Common Session ID

The following tasks must be completed before implementing the IEEE 802.1X Common Session ID 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 Common Session ID 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, use the **show interfaces switchport** command.

Restrictions for IEEE 802.1X Common Session ID

- The IEEE 802.1X Common Session ID feature is available only on a switch port.
- This feature does not support standard ACLs on the switch port.

Information About IEEE 802.1X Common Session ID

IEEE 802.1X Common Session ID Reporting

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD).
- A monotonically increasing unique 32 bit integer.
- The session start time stamp (a 32 bit integer).

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

Examples for IEEE 802.1X Common Session ID

Example: Common Session ID in Authentication Session Output

This example shows how the session ID appears in the output of the **show authentication** command. The session ID in this example is 1600000500000000B288508E5:

```
Switch# show authentication sessions

Interface MAC Address      Method Domain Status      Session ID
Fa4/0/4   0000.0000.0203 mab      DATA    Authz Success 1600000500000000B288508E5
```

Example: Common Session ID in Syslog Output

The following output is an example of how the session ID appears in the syslog output. The session ID in this example is also 1600000500000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 1600000500000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 1600000500000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 1600000500000000B288508E5
```

Additional References for IEEE 802.1X Port-Based Authentication

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	<i>Port Based Network Access Control</i>
RFC 3580	<i>IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines</i>

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 Common Session ID

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 [http://www.cisco.com/cisco/web/featurenavigator](#). An account on Cisco.com is not required.

Table 1: Feature Information for IEEE 802.1X Common Session ID

Feature Name	Releases	Feature Information
IEEE 802.1X Common Session ID	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE	The IEEE 802.1X Common Session ID feature allows a single session identifier to be used for all 802.1X and MAB authenticated sessions. This session ID is used for all reporting purposes such as show commands, MIBs, and RADIUS messages and allows users to distinguish messages for one session from messages for other sessions. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.

